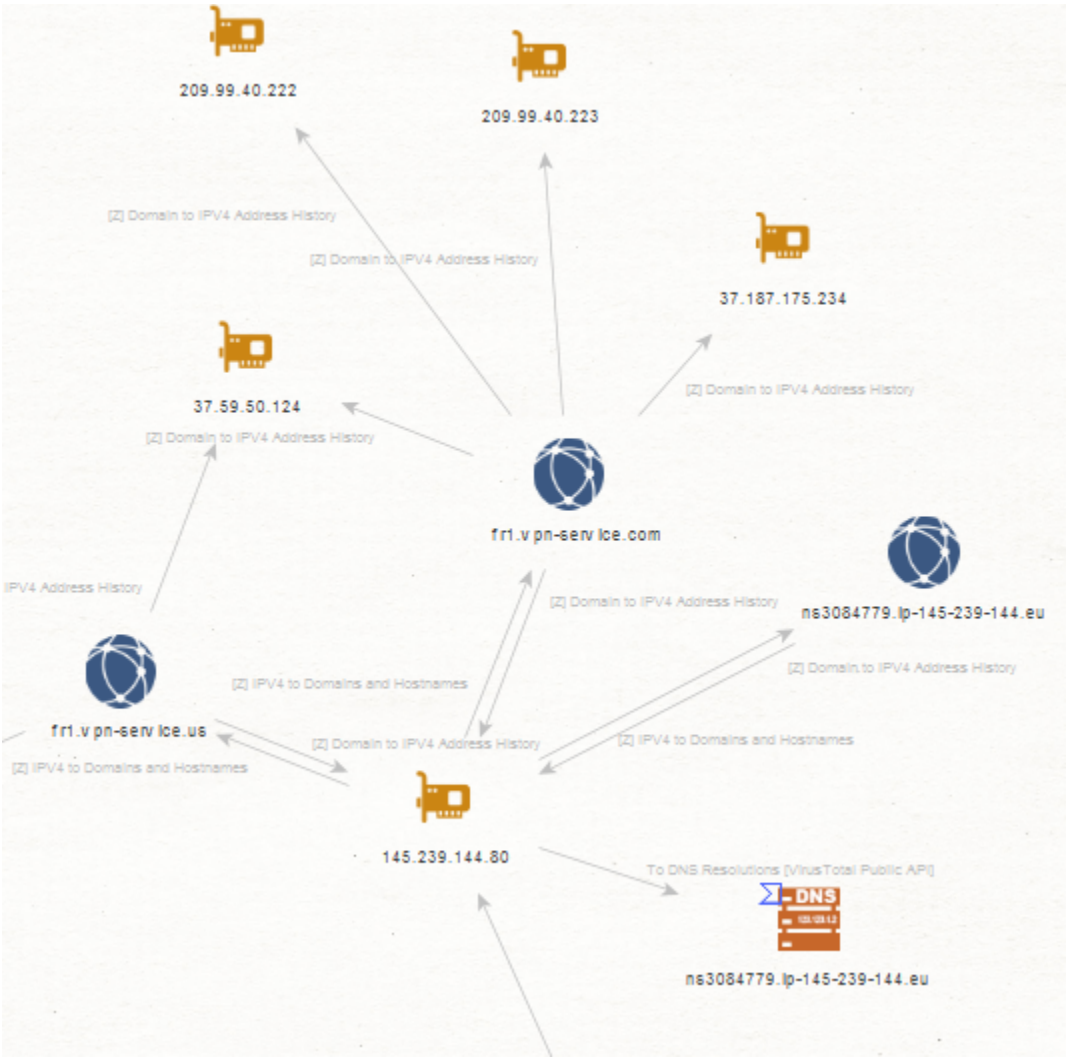
00. Profiling the Guccifer 2.0 Rogue Enterprise - An Analysis



We've decided to take a deeper look inside the Gucciffer 2.0 rogue online enterprise using public sources and the company's vast real-time and historical WHOIS database on our way to offer and provide as much actionable intelligence on the rogue actor for the purpose of assisting U.S Law Enforcement and the security industry on their way to properly attribute and track down the malicious and rogue cyber threat actor.

Related domains known to have been involved in the campaign include:

220140.vpn-security.us
dnsseed.emzy.de

305636.vpn-security.us
240435.vpn-security.us
x9.seed.bitcoinstats.com
x9.seed.bitcoin.sprovoost.nl
241901.vpn-security.us
542163.vpn-security.us
www.sandiegoforless.com
705763.vpn-security.us
411580.vpn-security.us
legolanddiscoverycenter.com
amadoresbrasileiros10.com
idlehearts.com
284651.vpn-security.us
www813.weezie.shantakatie.com
424745.vpn-security.us
004d0f1b.ewoodbussiness.info
00440759.ewoodbussiness.info
us1.vpn-service.com
es1.vpn-service.us
00086b0f.ewoodbussiness.info
us1.vpn-service.us
vpn-security.us
166965.vpn-security.us
us2.vpn-service.us
ns2.vpn-service.us
265769.vpn-security.us
004a07b2.ewoodbussiness.info
449236.vpn-security.us
admin.vpn-service.us
vpn-service.com
vgn.myanmarkup.net
nl2.vpn-service.us
www2.bestekleinwagen.com
303553.vpn-security.us
483630.vpn-security.us
428072.vpn-security.us
252747.vpn-security.us
43e163d6577106bb8ed303dd21c816fbc7a9b08314fb32c5a100e054.6.vfrtg.com
637230.vpn-security.us
846724.vpn-security.us
635225.vpn-security.us
vpn-service.us

383079.vpn-security.us
656219.vpn-security.us
ns3.vpn-service.us
admin.vpn-service.com
www.vpn-service.com
105408.vpn-security.us
218479.vpn-security.us
ns3.vpn-service.com
970279.vpn-security.us
580469.vpn-security.us
345829.vpn-security.us
178869.vpn-security.us
sc-monster.ru
fr1.vpn-service.com
gamesmaincraft.ru
www.landofart.ru
ns3084779.ip-145-239-144.eu
mail.gamesballs.ru
fr1.vpn-service.us
fantera.ru

Related personally identifiable email address accounts known to have been involved in the campaign include:

info@vpn-service.us
vpn_support@mail.ru
sec.service@mail.ru

Related responding IPs known to have been involved in the campaign include:

94.242.216.3
208.91.197.46
95.211.141.199
94.242.216.42
198.27.123.181
5.79.68.108
185.17.145.14
5.79.71.86
193.161.87.107
37.48.92.139
217.29.57.221
217.29.56.151

188.114.96.4
217.29.56.146
5.196.41.152
185.242.87.112
95.211.168.139
176.74.218.33
94.242.216.66
64.32.8.67
144.76.222.230
208.76.52.162
199.71.233.234
198.57.247.207
212.117.164.35
172.241.112.89
95.215.60.159
91.194.90.89
223.16.30.175
87.236.221.27
95.215.61.174
103.107.237.198
95.130.9.198
145.14.47.79
45.9.251.188
204.82.127.34
188.114.97.28
204.91.241.130
172.64.92.67
172.64.81.25
21.71.43.220
8.221.126.143
185.181.104.82
200.217.156.62
6.138.125.7
193.58.251.1
4.200.104.101
4.124.105.53
4.103.66.158
194.58.56.105
195.191.251.20
194.58.56.50
118.75.56.101
171.38.203.61

85.212.25.167
114.105.218.235
124.119.209.129
209.99.40.219
108.44.216.229
37.36.4.11
37.59.50.124
80.134.30.123
37.187.175.234
79.252.63.114
209.99.40.223
77.189.12.110
193.161.87.105
209.99.40.222
13.248.196.204
23.239.97.219
194.85.61.76
104.239.213.7
72.52.4.90
184.168.221.62
72.52.4.119
185.53.178.7
108.59.5.84
185.242.86.23
145.239.144.80
194.58.56.231
95.211.141.195
81.171.31.14
34.234.89.0
192.162.24.172
188.165.242.45
198.57.247.233
212.32.234.134
104.16.54.111
13.107.213.35
141.255.167.110
54.193.126.19

Related organizations known to have been involved in the campaign include:

Elite VPN Service
Security and Host Ltd

VPN Services Inc.

We'll continue monitoring the campaign and will post updates as soon as new developments take place.