Exposing Anonymous International - A Currently Active Domains Portfolio with Actionable IoCs (Indicators of Compromise) - An OSINT Analysis

We've decided to take a deeper look inside the Internet-connected infrastructure of Anonymous International for the purpose of assisting U.S Law Enforcement and the security community on its way to properly monitor and track down the cybercriminals behind these campaigns.

Sample related malicious and rogue and fraudulent domains known to have been involved in the campaign include:
hxxp://anonireland.com
hxxp://anonsweden.se
hxxp://anonymous-austria.com
hxxp://anonymous-japan.org
hxxp://anonymous-mexico.com
hxxp://anonymousargentina.com
hxxp://anonymousgreece.org
hxxp://anonymoushonduras.org
hxxp://anonymousperu.org
hxxp://anonymousvideo.eu

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

abran.celano@yahoo.com

chmod@freed0m4all.net
mexicoanonymous@gmail.com
themadhair@yahoo.co.uk

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

200.58.119.215
200.58.112.27
198.105.254.11
104.239.213.7
82.221.136.24
101.99.75.22
23.54.81.90
23.217.138.108
184.51.121.16
23.38.108.16
46.30.212.240
173.201.193.148
62.115.252.145
74.125.20.121
46.30.213.53
216.58.216.147
172.217.1.179
172.217.11.179
172.217.3.211
172.217.22.83
64.233.160.121
216.58.192.147
184.168.221.89
104.28.29.10
104.31.129.77
50.63.202.65
198.105.244.11
104.31.128.77
81.4.127.203
75.126.101.240
185.247.225.40
205.164.14.72
82.221.100.58
185.206.144.149
92.222.93.233
213.186.33.4

172.64.83.42
92.222.93.198
104.28.27.175

Related domains known to have been involved in the campaign include:
anonireland.org
anonireland.com
anonymoushonduras.org
argentinalibre.org
anonymousperu.org
f4all.org
anonymous-mexico.com
freed0m4all.info

Related IPs known to have been involved in the campaign include:
62.115.252.145
23.54.81.90
184.51.121.16
23.38.108.16
173.201.193.148
23.202.231.167
31.204.65.25
104.28.1.97
69.172.201.218
69.64.147.10
81.4.127.203
75.126.101.240
104.28.0.97
172.217.22.83
64.233.160.121
216.58.192.147
184.168.221.89
34.98.99.30
104.28.30.40
192.64.119.108
50.63.202.65
217.70.184.38
104.31.128.77
195.154.104.178
104.28.29.10
104.31.129.77
185.181.104.82

198.105.244.11
91.195.240.126

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

109.163.226.229
109.163.234.41
81.4.127.203
75.126.101.240
91.195.240.94
173.245.60.49
104.28.28.93
104.28.29.93
81.4.127.180
5.199.161.66
141.101.116.76
216.239.32.21
216.239.38.21
216.239.34.21
216.239.36.21
1.3.3.7
88.221.134.169
104.102.249.65
104.102.249.43
184.50.238.217
104.28.29.10
23.215.104.203
104.28.28.10
23.215.104.194
104.31.128.77
104.85.248.80
104.123.198.51
88.221.134.219
2.16.177.41
184.50.238.187
46.252.207.1
104.123.198.27
46.30.211.245
46.30.213.53
46.30.213.38
94.46.54.240
46.30.211.60

46.30.212.240
82.221.136.24
111.90.133.131
101.99.75.22
111.90.133.122
82.221.136.4
172.67.222.201
104.28.26.175
172.67.179.250
185.224.137.110
104.21.75.111
213.186.33.4
87.98.255.4
79.124.59.123
104.28.27.175
185.247.225.40
185.100.84.54
185.100.84.201
185.100.85.11
185.247.225.7

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