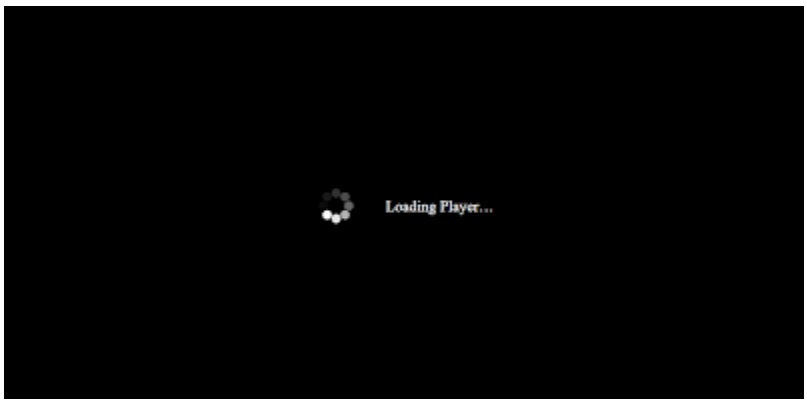
Exposing the Internet-Connected Infrastructure of the Cybercriminals Behind the Flashpoint Intel Web Site Compromise - An OSINT Analysis



We've decided to provide actionable intelligence on the Internet-connected infrastructure behind the Flashpoint Intel Web site compromise with the idea to assist U.S Law Enforcement and the security industry on its way to properly track down and monitor the cybercriminals behind these campaigns.

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

ermoyen.tk
monetizer-return.com
oussercondition.tk
superlzpre.com
mobusi.com
unanimous.live
newsfeed.support
minently.com
destinywall.org
plutonium.icu

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

156.154.113.36
195.20.45.35
104.219.248.19
47.245.10.59
172.64.137.10
138.68.113.179
172.64.165.16

162.222.213.197
10.10.34.35
99.198.108.198
91.195.240.103
198.143.165.221
217.13.124.118
156.154.175.30
198.54.117.210
146.112.61.107
37.230.116.105
198.54.117.216
23.202.231.167
217.13.124.95
23.217.138.108
195.20.41.119
205.147.93.131
162.222.213.199
172.64.93.139
89.255.252.29
104.28.24.233
172.64.85.195
172.64.88.234
185.28.71.53
172.64.94.225
176.123.9.53
198.54.117.212
198.54.117.217

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

www.ecommsupreme.com
botticelli.mobusi.com
www.geardevice.com
mari.mobusi.com
embla.mobusi.com
bria.homeaidsupply.su
piggy.homefirstvalue.su
rftwu.in.vg
iqbal.mytabletcompany.su
adsl-99-191-2-214.edu.tv
cf.arimw.tk
first.staroffer.xyz

uqdgj.tk
targeted.2makeyourday.online
app.premiumtraffc.com
www.americantrade.co
thepresident2016web.tech
macadam.mobusi.com
gamestream.club
battle.mobusi.com
singaporedatingclub.com
kbngpfpse.www.9666hh.com
radiologyjob.info
npupx.www.9azz.com
nbbqg.www.xy2046.com
y8euu.tk
ehcp.5i0j1.tk
free.3arbweb.com
au.bidpd.tk
c.stibium.xyz
oe2npdujm6bgdvil4dvubpjhgi.1.0.igrsocdkqdvgzle4rdnvfvod2a.srw1c3w.dns0.org
www.thepepeserna.com
bz.ocmulgeesite.com
www.leadvestors.com
www.miuxyoga.com
www.rhnc.us
www.olenloistava.com
jmqcf.www.9888hh.com
afkary.alshimaamahmoud.com
gbf.www.9azz.com
lin.campaignlink.xyz
mx1.goto.dialog.support
hostmaster.keepitorganized.bid
web.a.ebscohost.com.ezproxy.eiyaaa.com
direct.urgency.newpost.support
www.zgirls-hack.10l0.com
devtest.qm2727.com
ntmail.usis.com
pdf-54673.brightonclimatechange.org
home.alma-da.org
general.newsfeed.support
publicholidays.ph
www.hk3sp8.space
www.cliqueiachei.com.br

www.codinghim.com
www.hsen.net
shexiangleyuan.cn
mancoronavis24.com
mailwww-promo-web35-login.mindef.gov.sg
3anvs.kangbingdu.com.cn
optsynch.com
talk1170an-inactiveelb.kik.com
celeryleek.com
jm60nmk2or-1nlodfq831bl5w-wtm.sg1.dailymotion.com
datalab.dialog.support
mastera.cluster.notify.support
twitarded.rntx.win
monitor.click.dialog.support
downloadpdf360709.speakyoursoul.org
www.2016election.procon.org
textject.com
scandal.newsfeed.support
faststap.com
www.rusdialog.ru
fixes.boothradiology.com
cinecalidad.tv
ftp.drbrowndmd.com
www.wjhtsy.com
ssp.kimia.mobi
nice.hackerone.com
relay.oxb2.com
smayt.com
www.buttepianoacademy.com
nnoncerprsident.tk
www.preguntopolis.com
manage.dremain.tk
www.thetrustedcentralcontentingperfect.win
widgets.egestion.tk
www.agilefranchiselab.com
www.pythonscript.org
ccm.myramed.in
dv8flxaq.com
historicrentals.com
5fgfc.tk
img13.porngo.com
chinanet-230.tk

www.mhthemes.com
shop.nkoecvg.tk
238.as589.tk
outlook.nvoyerdbut.tk
videos.dremain.tk
www.trafficmap.de
643e3fed5f44ab187dc9b510ed10cd8c.lswcdn.net
www.roykeycreo.com
a307cd38a362d22a0ba922170f4329ba.lswcdn.net

Sample malicious MD5s known to have been involved in the campaign include:

c488a85f4fab76a640db654ac73cbefc
6ec96570247729ecd22670e3fa707276

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

46.20.4.188
5.135.0.194
212.92.39.34
212.92.39.33
212.92.39.35
184.173.90.90
47.245.8.67
13.32.193.81
54.192.82.117
205.251.219.107
52.222.171.227
91.195.240.136
172.64.165.16
162.222.213.197
10.10.34.35
99.198.108.198
67.227.226.240
91.195.240.103
198.143.165.221
217.13.124.118
156.154.175.30
198.54.117.210
146.112.61.107
37.48.105.98
37.230.116.105
185.28.70.32

8.248.0.22
178.162.217.175
67.27.162.122
8.240.48.122
8.238.113.250
205.147.93.131
162.222.213.199
104.26.3.88
172.64.93.139
104.26.2.88
89.255.252.29
172.67.72.14
104.28.24.233
89.255.250.54
172.64.85.195
172.64.88.234
185.28.71.53
172.64.94.225
66.152.109.75
176.123.9.53
124.232.132.94
198.54.117.212
183.224.40.24
195.20.45.35
89.255.249.55
88.150.240.195
104.219.248.19
4.27.17.252
80.233.134.249
47.245.10.59
208.69.32.164
172.64.137.10
138.68.113.179
154.195.91.125
104.24.96.65
108.186.177.125
172.67.195.34
107.172.111.24
172.67.155.13
38.54.238.125
104.28.7.7
156.154.113.36

198.54.117.217
198.54.117.216
68.65.122.150
23.202.231.167
217.13.124.95
23.217.138.108
195.20.41.119
172.64.136.10
104.21.84.40
104.21.21.171
104.27.179.119
172.67.186.21
104.27.178.119
195.20.52.182
104.27.183.84
93.189.113.39
36.86.63.182
23.200.237.225
23.60.91.225
43.249.37.245
198.54.117.197
89.255.249.53
198.54.117.200
209.58.153.10
198.54.117.199
89.255.250.53
198.54.117.198
213.227.130.48
198.105.254.11
89.255.250.69
89.255.249.102
172.64.92.178
103.139.42.59
50.63.202.65
217.13.124.96
89.255.249.68
54.190.245.8
89.255.248.53
184.168.221.47
89.255.248.55
185.237.224.163
34.98.99.30

172.64.81.120
172.64.81.118
172.64.84.141
172.64.81.98
104.27.132.235
104.24.113.235
72.52.179.175
104.21.89.78
185.181.104.82
104.24.119.86
104.20.8.8
89.255.249.54
104.24.118.86
172.64.80.203
172.64.90.173

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