Exposing a Domain Portfolio of Cybercrime-Friendly Forum Communities - An OSINT Analysis

We've decided to share an exclusive list of cybercrime-friendly forum communities which we obtained using Technical Collection and actually enrich it using WhoisXML API's vast real-time and historical WHOIS database for the purpose of assisting U.S Law Enforcement and the security community on its way to properly track down monitor and prosecute the cybercriminals behind these communities.

Sample list of currently active cybercrime-friendly forum communities includes:
zblock.co
zismo.biz
zone-academie.com
zs-squad.com
zevkli.org
zacodim.ru
zarabyte.com
zarbat.org
zion-network.co.uk
zyberph.com
undercover.su
underground.org.mx
zugriff.cc
zhacker.net
zhk.su
zillionere.com
ultuifii.info
underc0de.org
union-district.cc
unionpay.pro
underground.ws

ugworld.biz
ultimatenetwork.ru
undersecurity.net
undetecter.org
unoriginalforums.com
uniquecrew.net
unity-soft.org
underplace.biz
undersec.info
universalforums.co.cc
unleashedcrime.se
v-carder.com
v-carder.ws
untouchable.cc
upx8.com
unityfinxomxhf73.onion
unityforum.xyz
uw-team.org
uxt.ooo
val1d.cc
val1d.net
v-h.su
v3nen0.com
usernames.org
usoppn66bwsh3oot.onion
v4u.vn
vakanalar.com
vbspiders.com
vctools.net
vavilon.cc
vazonez.com
v3rmillion.net
v4-team.com
vbhacker.net
vbiv.bid
verifiedvendors.biz
veryleaks.cz
vdfno1.com
vendors.su
vb4arb.com
verified.re
verified2ebdpvms.onion

vietmatrix.net
viettrojan.org
vfu.cc
vhacking.com
vendorsbay.club
verified.lu
vhs-team.com
victory-turk.org
visi0nnaire.com
vlmi.io
vietzilla.com
vigilante.tech
vhbgroup.net
vhcteam.net
viprasys.org
virtualhackers.net
vor.nz
vortex-team.org
vlmi.su
vncno1.com
vip-hackerz.com
viphackforums.net
void.to
voidcore.ru
w3challs.com
waraxe.us
vpnpinas.xyz
vulnes.cc
vnhack.us
vnw.cc
w-1-w.com
w0rm.io
webcracking.com
webcriminal.ru
wardom.com.tr
wardriving-forum.de
vvvvvvvv766nz273.onion
vydepedev7nxcsxt.onion
web-attack.ru
webacard.com
wesecret.in
white-obnal.ru

webmasters.ru
webtoch.com
warez.red
wasm.ru
wehave.info
werb-ung.su

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

198.105.244.37
10.99.176.246
10.99.94.241
198.105.254.37
172.67.156.183
37.157.245.59
104.28.6.39
184.168.221.48
104.18.44.103
89.163.252.5
89.163.128.245
18.144.60.3
197.232.37.254
61.230.154.31
104.18.53.84
66.171.0.48
68.65.120.200
37.48.65.150
37.9.175.156
37.9.175.21
198.54.117.14
74.125.224.72
166.78.238.48
198.105.254.63
213.186.33.24
8.5.1.44
111.90.158.203
172.64.81.242
91.235.116.232
50.63.202.89
109.201.135.44
128.199.60.202
64.74.223.48

94.124.85.18
50.63.202.95
103.224.212.220
204.152.214.28
23.235.198.21
162.210.195.122
64.74.223.36
78.41.204.26
8.5.1.51
164.88.183.97
154.92.53.106
104.27.144.120
185.107.56.207
141.8.226.14
176.9.1.8
8.19.117.10
104.28.28.117
144.76.245.146
74.220.207.146
146.112.245.197
58.82.243.9
208.73.211.169
162.241.219.155
209.99.64.18
91.195.240.101
136.243.218.18
51.254.45.68
89.42.211.237
45.15.129.19
94.229.72.123
44.238.216.24
45.130.41.73
208.115.105.38
188.165.28.187
66.147.244.131
72.52.178.23
87.236.19.12
5.254.113.36
87.236.16.206
162.144.106.16
207.244.67.172
141.8.230.53

108.61.213.61
104.31.148.69
188.166.241.217
52.4.209.250
52.0.7.30
104.18.41.103
194.67.71.6
173.194.220.121
104.24.102.141
104.24.103.141
62.149.128.75
62.149.128.203
62.149.128.200
194.67.71.4
194.58.56.32
104.21.36.232
146.112.250.221
62.149.128.166
144.172.89.21
13.56.228.54
178.216.250.190
178.33.232.39
71.6.196.237
146.112.240.241
62.210.15.17
92.222.93.237
51.255.20.179
18.119.154.66
52.204.216.132
195.20.55.161
104.27.8.39
34.207.156.39
104.27.171.205
104.28.2.115
54.209.32.212
3.130.253.23
185.27.134.219
107.181.174.185
54.80.72.81
104.28.21.62
54.164.198.60
52.7.6.73

3.223.115.185
172.67.152.182
52.73.115.80
54.84.126.162
52.86.6.113
54.156.152.109
5.196.111.155
198.58.118.167
198.54.117.211
141.8.226.58
104.21.57.252
104.21.66.210
178.63.126.195
104.27.129.122
104.27.128.122
18.215.128.143
54.157.151.17
54.157.178.147
104.20.155.101
104.31.68.111
104.20.156.101
183.181.98.150
185.62.189.15
162.159.250.138
104.18.46.22
104.28.13.131
192.124.249.11
104.28.26.29
185.12.108.125
127.0.0.10
104.18.47.22
50.63.202.53
104.24.127.77
104.27.128.99
104.27.156.149
104.27.129.99
104.28.15.81
104.28.14.81
108.162.192.222
146.112.61.104
192.64.119.20
145.239.211.56

91.134.249.212
148.251.7.40
144.76.168.46
31.31.196.42
195.20.47.24
192.70.198.184
104.24.96.49
208.67.216.25
23.235.210.43
178.248.239.176
104.24.97.49
52.72.80.1
81.27.243.178

Sample personally identifiable email address accounts known to have been involved in the related campaigns includes:

tisinekinsisi889@rambler.ru
metan@live.ru
akurnuzova@bk.ru
kops123@list.ru
kirill56036@yandex.ru
coinodeals.com@whoisproxy.ru
XAKEROFF.NET@regprivate.ru
LEGALNO.NET@regprivate.ru
xaknet.org@regprivate.ru
ivanovsergeidomen@rambler.ru
roller75s@bk.ru
mail@ashatrov.ru
margelovmail@mail.ru
binms@list.ru
bilzerian247.com@whoisproxy.ru
dj_kolyan_rich@mail.ru
thecardingforum.com@whoisproxy.ru
p1095@ya.ru
rysik78@yandex.ru
loveplanet1-evoteam@yandex.ru
mr.controller@list.ru
kolobov063@yandex.ru
CARDERLIFE.COM@regprivate.ru
CARDERLAND.COM@regprivate.ru
dima181998@yandex.ru
zukko_shop@mail.ru

carderland.com@regprivate.ru
money.34@mail.ru
termitnet@mail.ru
avpro4em@mail.ru
nekit.lavr.99@mail.ru
carderforum.net@whoisproxy.ru
nelsman@ya.ru
carder.site@regprivate.ru
ilia@krukover.ru
neonovaya.company@yandex.ru
BITSHACKING.COM@regprivate.ru
root@crypters.ru
volosovik@inbox.ru
crim3time-world.net@whoisproxy.ru
inntensev@yandex.ru
cardersgroup.com@whoisproxy.ru
c2bit.xyz@whoisproxy.ru
nesternko43@mail.ru
kuzmenkov9898@mail.ru
keytv@rambler.ru
pr.zhdanov@inbox.ru
king-hack.xyz@regprivate.ru
olezhka_smirnov_69@internet.ru
ivan19541@bk.ru
mursel_007@mail.ru
msoc@bk.ru
govac8@list.ru
itsuper.info@regprivate.ru
ufolabs.net@regprivate.ru
minakin741@mail.ru
intactdev@mail.ru
arti_zorro@mail.ru
stardumps24.com@whoisproxy.ru
ga.special@mail.ru
Flex1337@bk.ru
csucclub@ya.ru
xakzona.com@yandex.ru
rif009@bk.ru
vlmi.su@yandex.ru
l33t.su@allperson.ru
l33t.su@allregistrantName.ru
klochkov.aleks78@mail.ru

archakovv95@mail.ru
blackhat.ooo@whoisproxy.ru
alex_mobi@mail.ru
mr.matino@list.ru
dbinar@mail.ru
ferdin75@mail.ru
voronve@mail.ru
6@404666.ru
FPTEAM-HACK.COM@regprivate.ru
shopworld@samsebehosting.ru
root@montan.ru
buy@spice-online.ru
fpteam-hack.com@regprivate.ru
asiris.as@yandex.ru
msplus-soft@yandex.ru
domain@volsite.ru
petrosyan.nikita2017@yandex.ru
cccvvvfffrrr@mail.ru
info@1dn.ru
cardingx.com@whoisproxy.ru
dotfix.org@regprivate.ru
gaelspb@gmail.com,svobodu@mail.ru
forregrudomain@yandex.ru
malianov.vova@yandex.ru
onyxia2015@yandex.ru
awento@mail.ru
webnullinfo@yandex.ru
vadimka.9987@mail.ru
HACKINGMAFIA.COM@regprivate.ru
eanez@bk.ru
pshacks-crew.com@regprivate.ru
blackbiz.info@regprivate.ru
mark0incs@bk.ru
adeev.01@mail.ru
lapyaps@yandex.ru
showmessage@mail.ru
crdpro@rambler.ru
teifilpeodifulor670@rambler.ru
HQCOMBO.COM@regprivate.ru
trast34@mail.ru
THEBLACKDECK.NET@regprivate.ru
burenkov.denis1994@mail.ru

wiktrov@yandex.ru
THEBLACKDECK.NET@regprivate.ru
dravemor@mail.ru
dark-zeit@mail.ru
bit-team@mail.ru
hack_evil@mail.ru
dendroidov@ya.ru
flaxz-carter@ro.ru
closeclub.pro1@yandex.ru
closeclub.pro@yandex.ru
ivan.fedorov777@mail.ru
carders.me@allperson.ru
carding.info@whoisproxy.ru
carders.info@mail.ru
altenen.com@whoisproxy.ru
snoozopreswilighdres793@rambler.ru
savinevgeniyahdl@mail.ru
kasl-veter@rambler.ru
dfergosan@mail.ru
blackwebforum.net@whoisproxy.ru
ruslanabrykova@rambler.ru
mr.rock1@bk.ru
yulechka.terenteva.79@mail.ru
marketingoffdirekt@yandex.ru
0daysu@mail.ru
lamamarket@bk.ru
marketzone@bk.ru
jast.game@yandex.ru
raptor.cntoz@yahoo.com
_3xp1r3_@9.cn
lvdarong@yahoo.com.cn
agt.smith@w.cn
support@joz.cn
kefu@now.cn
domainerfze@gmail.com
rubyverified@gmail.com
th3xploiterz@gmail.com
mraddictionking@gmail.com
tonywholt@gmail.com
anthonywayneholt@gmail.com
wehidden@gmail.com
sugianto.iis84@gmail.com

rlee1918@gmail.com
maxbrockman453@gmail.com
almutem.alsyrie1@gmail.com
erofolio@gmail.com
simowebmaster123@gmail.com
kurdcoo@gmail.com
shahoffline@gmail.com
acquirethisname@gmail.com
pcdunyasipc@gmail.com
porchesterpartners@gmail.com
rickyguynn99@gmail.com
domainlookupdbs@gmail.com
surabayablackhat@gmail.com
darehost@gmail.com
itzNickM@gmail.com
swagmaxxima@gmail.com
shailendrasial@gmail.com
souljanboy@gmail.com
tmdpainting@gmail.com
castleofae@gmail.com
willmsonashlery@gmail.com

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