Rogue Bulletproof Hosts May Still Be Alive and Kicking as DNS Intel Shows

Table of Contents

Executive Report

Rogue bulletproof hosts are part and parcel of the cybercriminal market that is hidden deep underground. Without means to easily evade detection, attribution, and incarceration, many of today's cybercriminals would not be able to continue their malicious operations.

In our constant bid to make the Internet more transparent and safer, our threat researcher Dancho Danchev recently collated 308 domains believed to belong to rogue bulletproof hosting service providers, which the WhoisXML API research team expanded to identify potentially connected web properties.

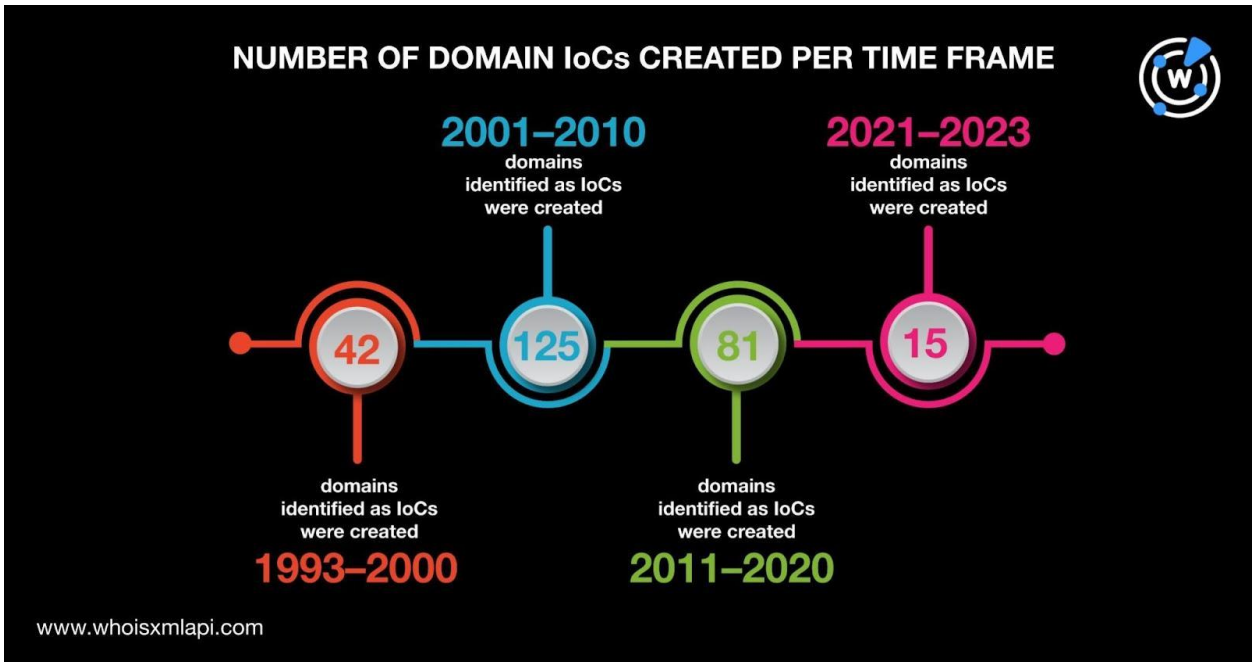
Our DNS deep dive into the threat led to the discovery of:

- 138 public email addresses found in the historical WHOIS records of the domains identified as indicators of compromise (IoCs)
- 1,103 email-connected domains, 10 of which turned out to be malicious based on a bulk malware check
- 4,028 IP-connected domains, seven of which turned out to be malicious based on a bulk malware check

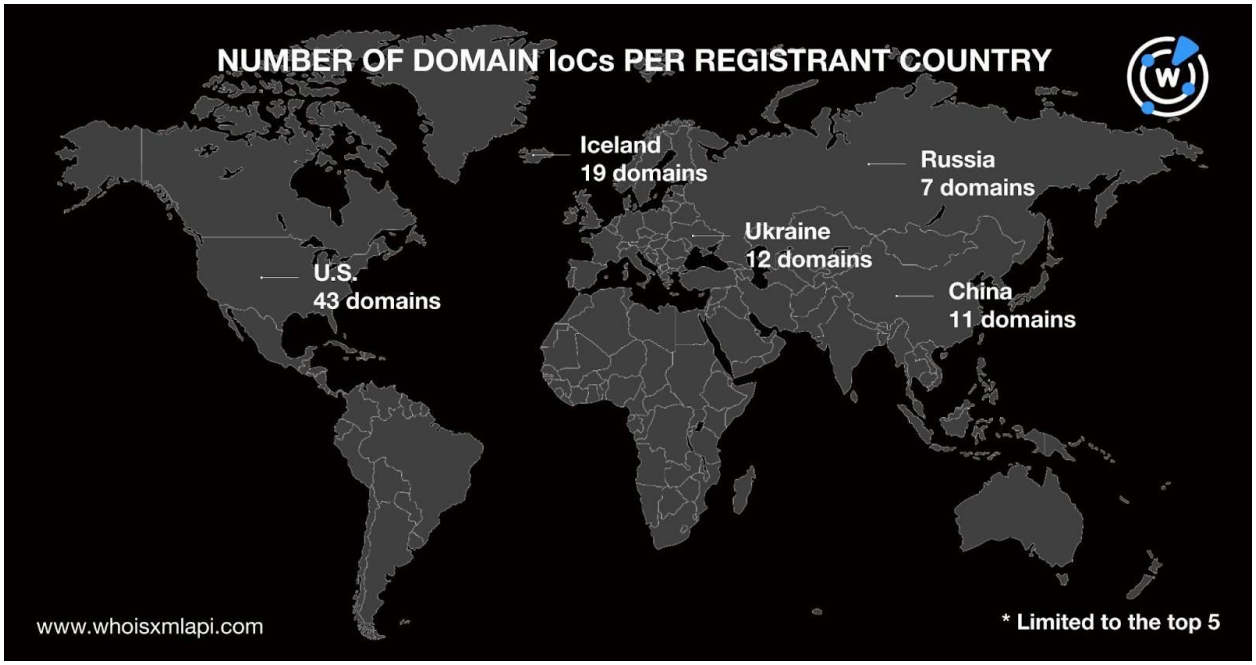
DNS Revelations about the IoCs

As the first step in our in-depth analysis of the rogue bulletproof hosting services, we subjected the 308 domains identified as IoCs to a bulk WHOIS lookup that led to these discoveries:

- A total of 263 domains had public creation dates in their current WHOIS records. 2010 (21 domains), 2012 (19 domains), 2013 (18 domains), 2000 (16 domains), and 2014 (15 domains) were the top 5 creation years. The remaining creation years accounted for 174 domains, while forty-five domains did not have public creation dates.



- Only 183 domains had public registrant country information in their current WHOIS records. The U.S. (43 domains), Iceland (19 domains), Ukraine (12 domains), China (11 domains), and Russia (seven domains) were the top 5 registrant countries. The remaining 91 domains were registered in 39 other countries. A total of 125 domains did not have public registrant country data.



A closer look at the 308 domains identified as IoCs also enabled us to identify text strings closely related to bulletproof hosting services, such as:

- **host**
- **net**
- **web**
- **server**
- **vps**
- **cloud**
- **data**
- **ddos**
- **site**
- **bulletproof**

The string **host** was the most commonly used (82 domains), followed by **net** (53 domains) and **web** (16 domains). Note that more than one text string could be present in some of the domains, such as in bulletproof-web[.]ru.

DNS Deep Dive Findings

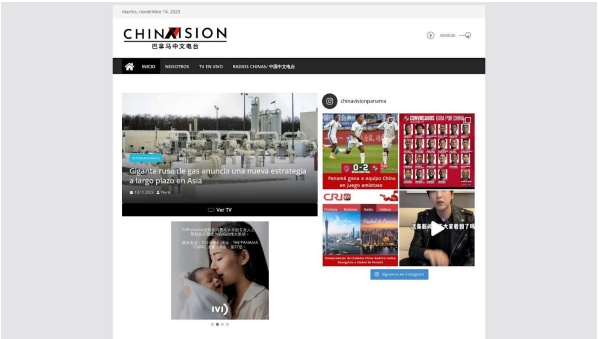
To find all potentially connected web properties, we first subjected the domains identified as IoCs to WHOIS history lookups, which led us to uncover 808 email addresses that appeared anywhere in their historical WHOIS records.

A total of 138 email addresses were public (unredacted or could be attributed to specific individuals or organizations). They were also used to register 1–50 domains each only

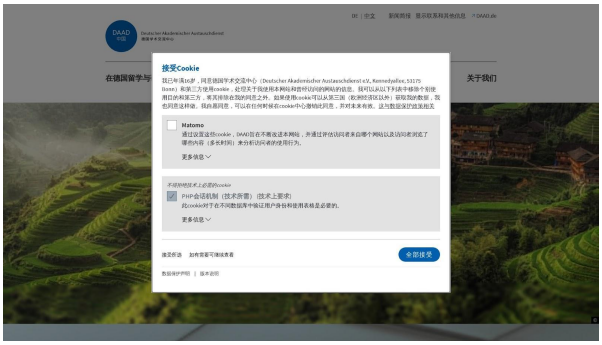
according to reverse WHOIS lookups. Altogether, the 138 public email addresses appeared in the current WHOIS records of 1,103 domains after duplicates and the IoCs were filtered out.

A bulk malware check for the 1,103 email-connected domains revealed that 10 of them were classified as malicious. Four of the 10 malicious domains remained accessible as of this writing based on screenshot lookups, three of which are shown below.

chgcorp[.]com



chinavision1180am[.]com



daad[.]org[.]cn

Next, we subjected the 308 domains identified as IoCs to DNS lookups and found that they resolved to 517 IP addresses after IPv6 addresses and duplicates were filtered out.

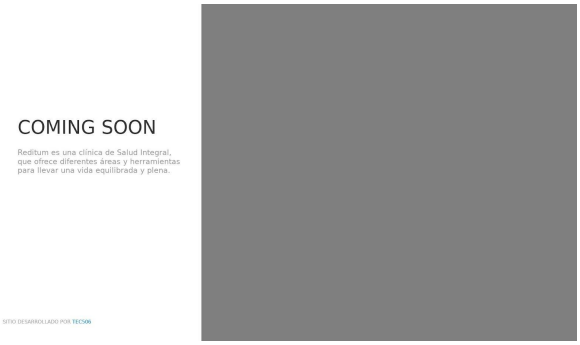
Reverse IP lookups for the 517 IP addresses showed that only 249 of them were seemingly private (only hosted 1–299 domains each). Fourteen of the 249 potentially private IP addresses turned out to be malicious based on malware checks.

Altogether, the 249 seemingly dedicated IP addresses hosted 4,028 domains after duplicates, the IoCs, and email-connected domains were filtered out. A bulk malware check for the IP-connected domains showed that seven of them were malicious and remained accessible as of this writing, six of which are shown below.

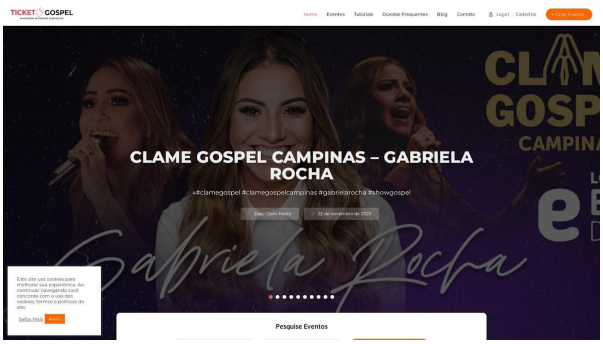
amygdala[.]rs[.]ba

cmc[.]dz

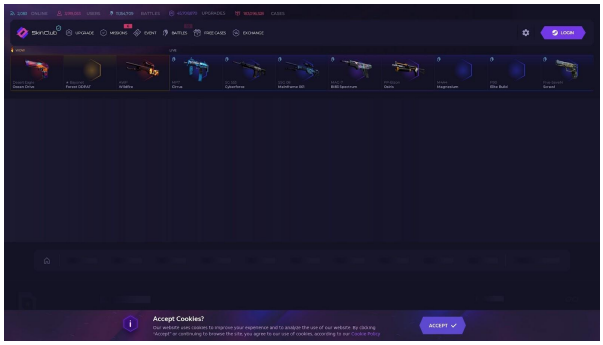
profitablesurvey[.]online



reditum[.]net



ticketgospel[.]com[.]br



usaskin[.]club

—

Our IoC expansion analysis showed signs that bulletproof hosts and their infrastructure may still remain up and running as evidenced by the 6,456 potentially connected web properties we uncovered, comprising 808 email addresses; 1,103 email-connected domains; 517 IP addresses; and 4,028 IP-connected domains. It is also worth noting that 31 of them (10 email connected domains, 14 IP addresses, and seven IP-connected domains) were already classified as malicious.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts and IoCs

Domains Belonging to Bulletproof Hosting Service Providers Identified as IoCs

- 1984hosting[.]com
- 2sync[.]co
- 2X4[.]ru
- 3nt[.]com
- abusehosting[.]ru
- admintek[.]net
- advania[.]com
- afranet[.]com
- agava[.]ru
- albahost[.]net
- alexhost[.]com
- altushost[.]com
- anders[.]ru
- anonymoushosting[.]in
- antiddos[.]biz
- area6[.]ru
- artmotion[.]eu
- asiapacific-it[.]com
- asiapacifichosting[.]com
- atlax[.]com
- availo[.]se
- avk-com[.]ru
- bacloud[.]com
- bahnhof[.]net
- balkanvps[.]com
- beotel[.]net
- berihoster[.]ru
- besthosting[.]ua
- blazingfast[.]io
- blueangelhost[.]com
- borneo[.]kg
- bulletproof-web[.]ru
- bullhost[.]co
- ccihosting[.]com
- cinipac[.]com
- citynethost[.]com
- cloud[.]volia[.]com
- cloudlite[.]ru
- colocall[.]net
- comsats[.]net[.]pk
- continent8[.]com
- crservers[.]com
- ctyun[.]cn
- cubexsweatherly[.]com
- curacaowebhosting[.]com
- cyberbunker[.]com
- cyberfuel[.]com
- datacenter[.]ir

- datahouse[.]ru
- dataplugs[.]com
- dedicado[.]com[.]uy
- deltahost[.]com
- deltalis[.]com
- deltasystem[.]cl
- dis[.]telecom[.]kz
- dmzhost[.]c
- doclerweb[.]com
- dreamwebhosting[.]net
- ecatel[.]co[.]uk
- eccsolutions[.]net
- ecodissident[.]net
- ekvia[.]com
- elkupi[.]com
- elvsoft[.]com
- en[.]datasource[.]ch
- en[.]hostsolutions[.]ro
- en[.]ukrtelecom[.]ua
- en[.]uplink[.]hu
- eng[.]deninet[.]net
- eodatacenter[.]com
- eranet[.]com
- eserver[.]ru
- evoluso[.]com
- exmasters[.]com
- fastvds[.]ru
- finalhosting[.]cz
- firstbyte[.]ru
- firstvds[.]ru
- flokinet[.]is
- freehost[.]com[.]ua
- galkahost[.]com
- geekhost[.]pro
- gemenii[.]ro
- glesys[.]com
- global[.]ba
- globatel[.]org
- gmhost[.]hosting
- goodnet[.]com[.]ua
- grandhost[.]cc
- habangnet[.]com
- hc[.]ru
- heberjahiz[.]com
- hidemyhost[.]com
- hktechnology[.]com
- host[.]al
- hostalot[.]ru
- hoster[.]ru
- hosthink[.]net
- hosting[.]nic[.]ru
- hosting[.]reg[.]com
- hosting[.]tel[.]ru
- hosting[.]tongacable[.]net
- hosting[.]turk[.]net
- hosting[.]ua
- hostingserve[.]rs
- hostkey[.]com
- hostname[.]cl
- hostoweb[.]com
- hostparatuvida[.]com
- hostsailor[.]com
- hts[.]ru
- hub[.]org
- icyevolution[.]com
- idhost[.]kz
- ihc[.]ru
- ihor[.]ru
- infiumhost[.]com
- infobox[.]ru
- infomaniak[.]ch
- innovahosting[.]net
- insacom[.]cl
- internetport[.]com
- internetsolutions[.]hk
- iprosrv[.]com
- ironservers[.]cl
- ispcompania[.]com
- ispserver[.]com
- ititch[.]com

- itldc[.]com
- itools[.]mn
- ixam-hosting[.]com
- justhost[.]in[.]ua
- katzglobal[.]com
- knownsrv[.]com
- koddos[.]com
- kowloonhosting[.]com
- kras[.]host
- kriweb[.]com
- laceibanetsociety[.]com
- lankapartnerhost[.]com
- latinoserver[.]com
- lfait[.]com
- libertyvps[.]net
- libyanspider[.]com
- licosys[.]com
- linkdatacenter[.]net
- localhost[.]tn
- lolekhosted[.]net
- ltt[.]ly
- lunarvps[.]com
- lunarvps[.]comorangewebsite[.]com
- m247[.]roen
- magicnet[.]md
- masterhost[.]ru
- mcloud[.]rs
- melbicom[.]net
- memvds[.]ru
- mikrovps[.]com
- mirohost[.]net
- mtel[.]ba
- mycloud[.]by
- nashirnet[.]net
- natro[.]com
- neoserver[.]ru
- netassist[.]ua
- netbrella[.]net
- netengi[.]com
- netplace[.]ru
- networksdelmanana[.]com
- nexlinx[.]net[.]pk
- nexus[.]pk
- nidahost[.]com
- nine[.]ch
- ninet[.]rs
- nonamehosts[.]com
- NovoGara[.]com
- nplusone[.]ma
- nsc[.]ba
- oblaci[.]rs
- offshorededi[.]com
- offshoreracks[.]com
- ohp[.]ua
- ok[.]is
- online[.]tm
- orangewebsite[.]com
- ouriran[.]com
- overleaf[.]com
- pachosting[.]hk
- panamaserver[.]com
- parsonline[.]com
- parspack[.]com
- pavietnam[.]vn
- pin[.]se
- pirateshosting[.]net
- planetahost[.]ru
- plus[.]hr
- pndc[.]ir
- portlane[.]com
- powerhost[.]cl
- privatelayer[.]com
- pro-managed[.]com
- proen[.]co
- proen[.]co[.]th
- profivps[.]hu
- prq[.]se
- ps[.]kz
- ptclcloud[.]com[.]pk
- pttrs[.]net

- pw-service[.]com
- qsscloud[.]ba
- rackend[.]com
- racklodge[.]com
- racknation[.]cr
- radore[.]com
- rapidcompute[.]com
- rayadatacenter[.]com
- renter[.]ru
- rockhoster[.]com
- ru-tld[.]ruen
- rusonyx[.]ru
- rx-name[.]ua
- sadecehosting[.]com
- securehost[.]com
- selectel[.]com
- semele[.]com[.]tr
- seohosting[.]com[.]tr
- server[.]ua
- serverastra[.]com
- serverhk[.]org
- serverhosting[.]my
- serveria[.]com
- servidores[.]gamerlive[.]cl
- shinjiru[.]com
- simplecloud[.]ru
- sinohosting[.]net
- smart-hosting[.]ro
- solarcom[.]ch
- sologigabit[.]com
- space[.]kz
- starrydns[.]net
- sunnyvision[.]com
- superhosting[.]net
- swedehost[.]net
- swedendedicated[.]com
- synwebhost[.]org
- syt[.]com
- t4[.]cr
- takewyn[.]com
- tchile[.]com
- tehnodom[.]com
- tele-asia[.]net
- teleklik[.]ba
- thnic[.]co
- thnic[.]co[.]th
- thost[.]ru
- tilaa[.]com
- time4vps[.]eu
- timeweb[.]com
- tomtel[.]ru
- tophost[.]mden
- trabia[.]com
- trvps[.]net
- tucha[.]ua
- uanode[.]net
- uar[.]net
- udasha[.]com
- ukraine[.]com[.]ua
- ukrdc[.]net
- ukrnames[.]com
- ultratechhost[.]com
- underhost[.]com
- unit-is[.]com
- uniteddc[.]net[.]ua
- urdn[.]com[.]ua
- valuehost[.]ru
- vds64[.]com
- vdsinside[.]com
- vhoster[.]net
- victoriagroup[.]me
- vinahost[.]vn
- vinastar[.]net
- virtono[.]com
- virtualpark[.]hu
- vit[.]com[.]tr
- voxility[.]com
- vps[.]ag
- vpsbg[.]eu
- vpsgod[.]com

- vscale[.]io
- vstoike[.]ru
- warez-host[.]com
- wavecom[.]ee
- web-server[.]eu
- webcare360[.]com
- webhost[.]tn
- webonic[.]hu
- webservices[.]dz
- webuzo[.]net
- weservit[.]nl
- wrzhost[.]com
- xenyohosting[.]com
- xeonbd[.]com
- xethost[.]com
- xhostfire[.]com
- xservers[.]ro
- yourserver[.]se
- zgh[.]cl
- zomro[.]com

Sample Public Email Addresses Used to Register 1–50 Domains Only

- aba*****@mail[.]ru
- *****@nashirnet[.]net
- *****@azar-a[.]net
- *****@iws[.]co
- *****@space[.]kz
- *****@spinter[.]net
- afranetsol*****@yahoo[.]com
- AGR*****@syt[.]com
- altan*****@itools[.]mn
- as*****@estrella7[.]com
- BI*****@enelis[.]ru
- bi*****@selectel[.]ru
- bisne*****@bisnes[.]com
- co*****@ebs[.]dz
- cse*****@gmail[.]com
- cus*****@dotroll[.]com
- customers*****@cyberfuel[.]com
- denis[.]l*****@yandex[.]ru
- *****@krasmama[.]ru
- dmitriy[.]zeml*****@gmail[.]com
- *****@natro[.]com
- dns*****@mail[.]link[.]net
- dns*****@turk[.]net
- domain[.]ma*****@xeonbd[.]com
- d*****@deninet[.]hu
- d*****@globatel[.]ru
- d*****@ispserver[.]com
- d*****@licosys[.]com
- d*****@radcom[.]co[.]ir
- d*****@radore[.]com
- d*****@rh[.]com[.]tr
- d*****@websprava[.]cz
- domainn*****@yahoo[.]com
- doma*****@parsonline[.]net
- do*****@altushost[.]com
- do*****@atlax[.]com
- do*****@cycom[.]com[.]hk
- do*****@dreamweb[.]rs
- DO*****@linkdatacenter[.]net
- do*****@racklodge[.]com
- doma*****@yahoo[.]com
- domain*****@katzglobal[.]com
- d*****@volia[.]net
- eco[.]a*****@mail[.]ru
- *****@grupogms[.]com
- *****@tnet[.]hk
- *****@felipecruz[.]com
- *****@uar[.]net
- *****@ok[.]is
- hadi[.]*****@email[.]ly

Sample Email-Connected Domains

- 0es3hosting[.]com
- 104[.]152[.]45[.]195
- 1domain[.]com[.]ua
- 24by7telugu[.]com
- 24krs[.]net
- 2f7[.]us
- 410bakery[.]com
- 4play[.]com[.]tr
- 57goldenluckinvestment[.]com
- 5stars[.]hosting
- 808848[.]com
- 82[.]221[.]129[.]44
- 82[.]221[.]141[.]108
- absmalaysia[.]com
- accesoriospanama[.]com
- acem[.]or[.]cr
- activeair[.]ca
- adibnews[.]com
- advertisementbd[.]com
- advokati-blagojevic[.]com
- adwo[.]vip
- aec-pro[.]com
- aerosvitegypt[.]com
- afranet[.]net
- afrique-alu[.]dz
- agencyleonard[.]com
- agneux1840[.]com
- agro-temp[.]com[.]ua
- agrovelasquez[.]com
- ahil[.]ir
- air-pro[.]cn
- airmansinformationmanual[.]com
- aitmenov-mektebi[.]kz
- ajdari[.]us
- albadregypt[.]com
- alelconsulting[.]com
- alfa-mtc[.]com
- algerieferries[.]dz
- allverk[.]is
- altushosting[.]us
- alyassintrade[.]com
- amazing[.]ly
- amrich[.]com[.]hk
- an[.]mk
- antishock-tm[.]com
- appid[.]tn
- appinvest-club[.]com
- appzar[.]mobi
- arch-hardware-solution[.]com
- areaxxx[.]info
- argentina-logistics[.]com
- arianexir[.]com
- arinadavidova[.]com
- ariston-tunisie[.]tn
- ars-tours[.]com
- artgrandinvestment[.]com
- artniture[.]com
- arts[.]tn
- arturryno[.]bid
- arturryno[.]info
- arturryno[.]webcam
- asiacurry[.]com
- asiafood[.]hk
- asiahostingnews[.]com
- asiapacificads[.]com
- asiapacificservers[.]com
- asiapromocodes[.]com
- asiesvoip[.]com
- assetvn[.]net
- astc[.]com[.]hk
- at-t[.]us
- ata-services[.]com[.]hk
- atom-company[.]com
- autohho[.]net
- autohost[.]cloud
- autohydrogen[.]net
- automobileinsurance[.]cheap
- avanzada[.]cr
- averclear[.]com
- avin-co[.]org

- avionika[.]com
- b335[.]us
- bahai[.]cr
- bahnhof[.]fi
- bantechk[.]com
- baovelamsondong[.]com
- barralaman[.]tn
- batar-pvc[.]com
- battesimo[.]love
- baypetco-egypt[.]com
- beefars[.]com[.]hk
- bestmeeting[.]love
- bestzikarepellent[.]com
- bilgebahisci[.]org
- bilgesoyak[.]com
- billeros[.]com
- bimeh-omidafarin[.]com
- bimehomidafarin[.]com
- bimehsaratan[.]com
- bimesaratan[.]com

Sample Malicious Email-Connected Domains

- 82[.]221[.]129[.]44
- chgcorp[.]com
- chinavision1180am[.]com
- confirms-apple[.]com
- daad[.]org[.]cn
- dcvolia[.]com

Sample Private IP Addresses

- 103[.]11[.]103[.]133
- 103[.]16[.]228[.]34
- 103[.]44[.]163[.]3
- 104[.]18[.]11[.]172
- 104[.]18[.]12[.]172
- 104[.]18[.]42[.]53
- 104[.]20[.]160[.]46
- 104[.]20[.]161[.]46
- 104[.]22[.]12[.]15
- 104[.]22[.]13[.]15
- 104[.]22[.]32[.]78
- 104[.]22[.]33[.]78
- 104[.]22[.]44[.]146
- 104[.]22[.]45[.]146
- 104[.]22[.]62[.]80
- 104[.]22[.]63[.]80
- 104[.]253[.]113[.]155
- 104[.]26[.]0[.]78
- 104[.]26[.]1[.]78
- 104[.]26[.]10[.]223
- 104[.]26[.]11[.]223
- 104[.]26[.]12[.]203
- 104[.]26[.]12[.]47
- 104[.]26[.]12[.]65
- 104[.]26[.]12[.]96
- 104[.]26[.]13[.]203
- 104[.]26[.]13[.]47
- 104[.]26[.]13[.]65
- 104[.]26[.]13[.]96
- 104[.]26[.]2[.]205
- 104[.]26[.]3[.]205
- 104[.]26[.]6[.]175
- 104[.]26[.]7[.]175
- 104[.]26[.]8[.]95
- 104[.]26[.]9[.]95
- 112[.]213[.]82[.]66
- 116[.]202[.]187[.]30
- 116[.]203[.]145[.]230
- 131[.]108[.]208[.]40
- 135[.]181[.]180[.]253
- 138[.]201[.]19[.]68
- 138[.]204[.]228[.]22
- 138[.]255[.]101[.]205
- 139[.]59[.]252[.]123

- 144[.]76[.]159[.]151
- 147[.]78[.]117[.]13
- 15[.]222[.]152[.]144
- 150[.]129[.]35[.]28
- 154[.]70[.]207[.]38
- 154[.]73[.]92[.]52

Sample Malicious Private IP Addresses

- 104[.]26[.]1[.]78
- 104[.]26[.]12[.]65
- 172[.]67[.]72[.]99
- 185[.]112[.]145[.]81
- 185[.]178[.]208[.]183
- 185[.]65[.]123[.]230
- 185[.]65[.]148[.]89
- 194[.]0[.]200[.]202

Sample IP-Connected Domains

- 023baby[.]nl
- 029adom[.]com
- 040hosting[.]eu
- 100[.]237[.]77[.]178[.]finalhosting[.]cz
- 100tb[.]cz
- 100trucks[.]com
- 105452627-272246173[.]slunecny[.]net
- 107[.]237[.]77[.]178[.]finalhosting[.]cz
- 108[.]237[.]77[.]178[.]finalhosting[.]cz
- 10xgen[.]com
- 111[.]237[.]77[.]178[.]finalhosting[.]cz
- 123herba[.]com
- 123pelangi[.]org
- 126[.]237[.]77[.]178[.]finalhosting[.]cz
- 1310[.]kz
- 134[.]2446[.]finalhosting[.]cz
- 138[.]237[.]77[.]178[.]finalhosting[.]cz
- 1418-chemindesdames[.]fr
- 144[.]237[.]77[.]178[.]finalhosting[.]cz
- 147training[.]com
- 157[.]237[.]77[.]178[.]finalhosting[.]cz
- 159[.]237[.]77[.]178[.]finalhosting[.]cz
- 166[.]225[.]41245-167-46[.]finalhosting[.]cz
- 16e7196b97[.]claro[.]com[.]sv[.]finalhosting[.]cz
- 170[.]237[.]77[.]178[.]finalhosting[.]cz
- 177-106-135-207[.]xd-dynamic[.]algarnetsuper[.]com[.]br[.]finalhosting[.]cz
- 177-63-226-74[.]dsl[.]telesp[.]net[.]br[.]finalhosting[.]cz
- 177[.]237[.]77[.]178[.]finalhosting[.]cz
- 178[.]237[.]77[.]178[.]finalhosting[.]cz
- 179[.]237[.]77[.]178[.]finalhosting[.]cz
- 183[.]237[.]77[.]178[.]finalhosting[.]cz
- 186[.]237[.]77[.]178[.]finalhosting[.]cz
- 187[.]237[.]77[.]178[.]finalhosting[.]cz
- 1888157188-1200936036[.]nejlevnejsi-pripojeni-k-internetu[.]cz
- 189[.]237[.]77[.]178[.]finalhosting[.]cz
- 18p[.]fun
- 19[.]138[.]73[.]200[.]cab[.]prima[.]net[.]ar[.]finalhosting[.]cz
- 198[.]28[.]48[.]77[.]finalhosting[.]cz
- 1c[.]rocks
- 1cloudlab[.]eu
- 1h8[.]9t4[.]net
- 200[.]237[.]77[.]178[.]finalhosting[.]cz
- 2016go[.]com
- 203[.]157[.]67-46[.]finalhosting[.]cz
- 203[.]237[.]77[.]178[.]finalhosting[.]cz
- 209[.]237[.]77[.]178[.]finalhosting[.]cz
- 216[.]rev6[.]finalhosting[.]cz
- 218[.]237[.]77[.]178[.]finalhosting[.]cz

- 219[.]237[.]77[.]178[.]finalhosting[.]cz
- 223[.]237[.]77[.]178[.]finalhosting[.]cz
- 227[.]237[.]77[.]178[.]finalhosting[.]cz
- 228[.]113[.]220[.]91[.]hostidadns[.]com[.]finalhosting[.]cz
- 228[.]237[.]77[.]178[.]finalhosting[.]cz
- 229[.]237[.]77[.]178[.]finalhosting[.]cz
- 22april[.]org
- 23[.]131[.]73[.]200[.]cab[.]prima[.]net[.]ar[.]finalhosting[.]cz
- 233[.]237[.]77[.]178[.]finalhosting[.]cz
- 234[.]237[.]77[.]178[.]finalhosting[.]cz
- 234pd[.]com
- 237[.]237[.]77[.]178[.]finalhosting[.]cz
- 238[.]237[.]77[.]178[.]finalhosting[.]cz
- 239[.]237[.]77[.]178[.]finalhosting[.]cz
- 242[.]237[.]77[.]178[.]finalhosting[.]cz
- 245[.]237[.]77[.]178[.]finalhosting[.]cz
- 247livesupport[.]biz
- 249[.]28[.]48[.]77[.]finalhosting[.]cz
- 24bbboom[.]com
- 25[.]237[.]77[.]178[.]finalhosting[.]cz
- 253[.]237[.]77[.]178[.]finalhosting[.]cz
- 30min[.]cz
- 30minut[.]cz
- 310902179-942570408[.]pripojeni-k-internetu[.]cz
- 333am[.]tv
- 34[.]237[.]77[.]178[.]finalhosting[.]cz
- 3632252[.]ru
- 3dp[.]kz
- 3e[.]ru
- 3ixam[.]com
- 3l07q[.]9t4[.]net
- 3tdent[.]com
- 3velimited[.]com
- 41005[.]77[.]178[.]finalhosting[.]cz
- 429men[.]com
- 439520266-1710348667[.]nejlevnejsi-pripojeni-k-internetu[.]cz
- 4617988[.]net
- 4allprograms[.]me
- 4calendars[.]co[.]uk
- 4colorprint[.]com
- 4home[.]co[.]za
- 4vd[.]kz
- 4vengineering[.]ba
- 50states[.]com
- 520madison[.]com
- 5cloudhost[.]com
- 5cloudhost[.]net
- 600141203-31501151[.]pripojeni-k-internetu[.]cz
- 69gradernord[.]se
- 6kz[.]1h8[.]9t4[.]net
- 6xteam[.]com
- 77[.]237[.]77[.]178[.]finalhosting[.]cz

Sample Malicious IP-Connected Domains

- amygdala[.]rs[.]ba
- cmc[.]dz
- profitablesurvey[.]online
- reditum[.]net