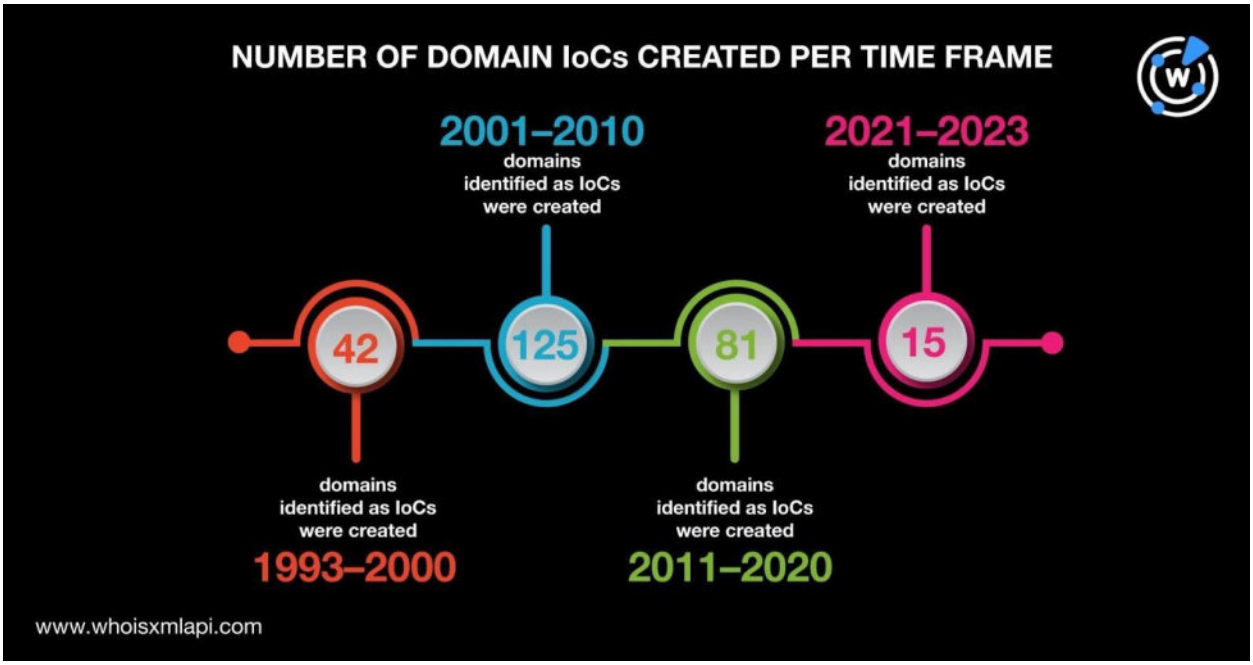
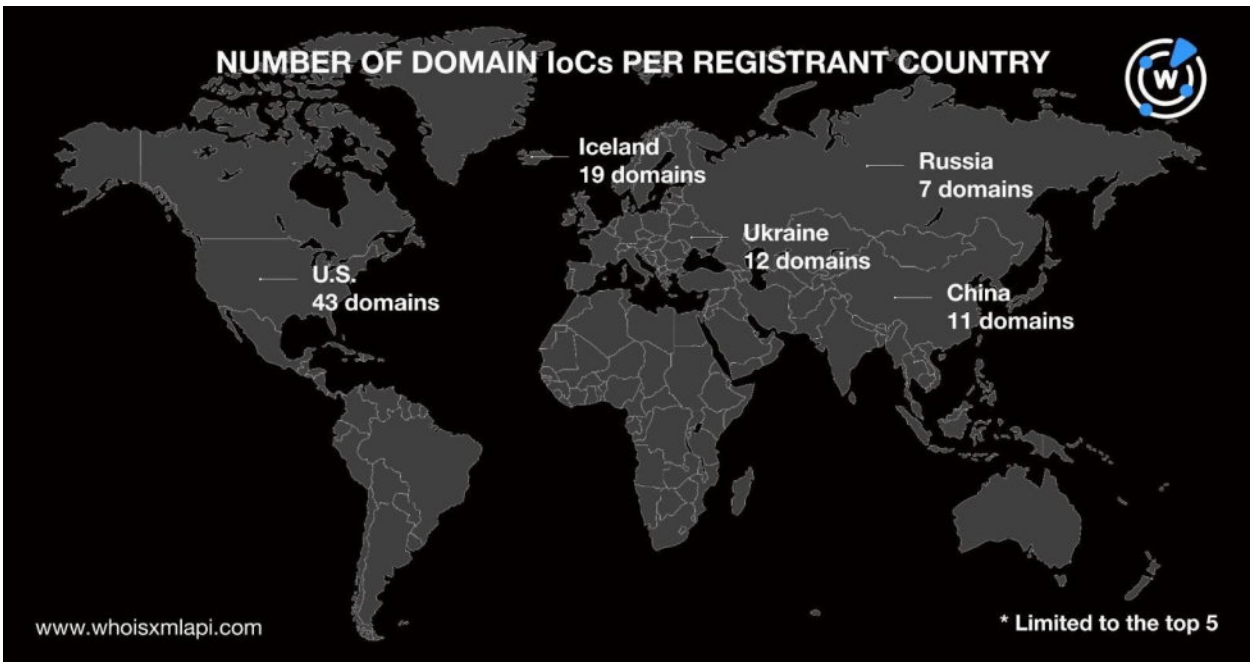


- 現在のWHOISレコードに登録者の国が公開されているドメインIoCはわずか183個。登録国のトップ5は、米国（43個）、アイスランド（19個）、ウクライナ（12個）、中国（11個）、ロシア（7個）。残りの91個は他の39カ国で登録。合計125個は国のデータが非公開。



308個のドメインIoCをさらに詳しく調べたところ、防弾ホスティングサービスと密接に関連する以下のような文字列を特定できました：

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

最も多く使われていたのは**host**（82ドメイン）で、これに**net**（53ドメイン）、**web**（16ドメイン）が続きます。bulletproof-web[.]ruのように、複数の関連文字列が含まれたドメイン名もありました。

DNSの詳細分析でわかったこと

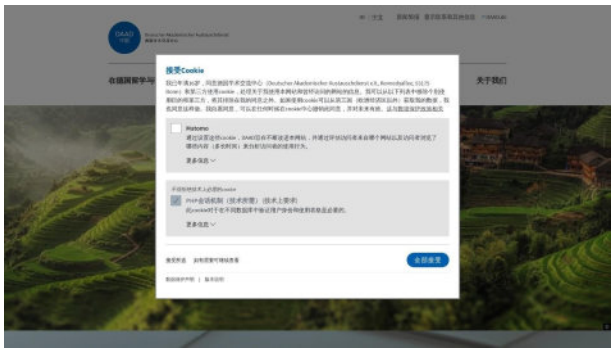
関連性のある全てのウェブプロパティを洗い出すため、ドメインIoCをWHOIS History Lookupで検索してみました。すると、ドメインIoCの過去のWHOISレコードに表示される合計808個のメールアドレスが検出されました。

138個のメールアドレスは公開（非公開化されていない、または特定の個人または組織への帰属が確認できる）のものでした。また、Reverse WHOIS Lookupで検索したところ、それぞれのメールアドレスを使って登録されたドメイン名の数は、1〜50個にとどまりました。重複とIoCを取り除いた結果として、138個の公開メールアドレスがドメイン名1,103個の現行のWHOISレコードに表示されることがわかりました。

その1,103個のドメイン名のマルウェア一括チェックを行ったところ、10個は悪意あるドメイン名に分類されました。Screenshot Lookupを実行した結果、4個の悪意あるドメイン名は本稿執筆時点でアクセス可能でした。そのうち3個のスクリーンショットを以下に示します。

chgcorp[.]com

chinavision1180am[.]com



daad[.]org[.]cn

次に、308個のドメインIoCについてDNS Lookupを実行しました。その結果、それらのドメイン名が名前解決するIPアドレスが、IPv6アドレスと重複を取り除いた後の状態で517個検出されました。

その517個のIPアドレスをReverse IP Lookupで検索したところ、専用と思われるアドレスはそのうち249個にとどまりました（各アドレスでホストしていたドメイン名は1〜299個）。マルウェアチェックにより、その249個のうち14個は悪意あるIPアドレスであることが判明しました。

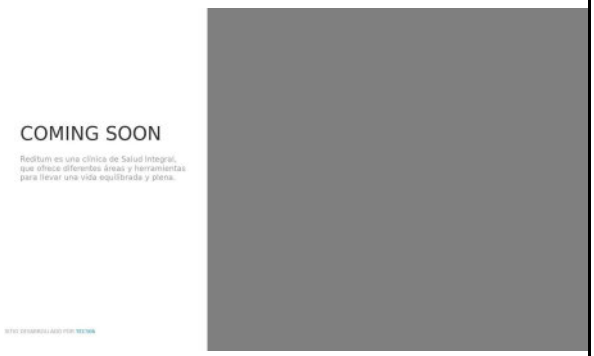
重複、IoC、共通のIPアドレスを使っているドメイン名をフィルタリングした結果、専用らしい249個のIPアドレスは合計で4,028個のドメイン名をホストしていることがわかりました。その4,028個のドメイン名をマルウェア一括チェックにかけたところ、7個は本稿執筆時点でアクセス可能な悪意あるドメイン名でした。そのうち6個のスクリーンショットを以下に示します。

amygdala[.]rs[.]ba

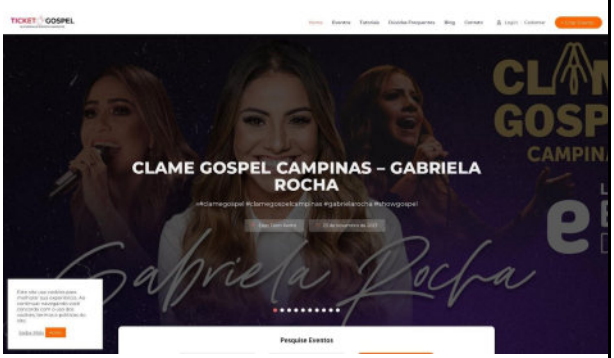
cmc[.]dz

Incorrect URL, try again

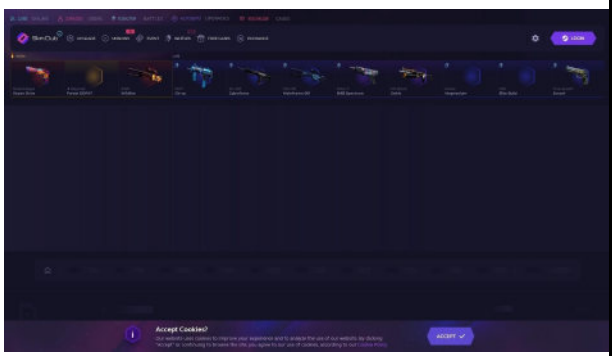
profitablesurvey[.]online



reditum[.]net



ticketgospel[.]com[.]br



usaskin[.]club

—

IoCを出発点とした今回の分析で、防弾ホスティングとそのインフラは現在も稼働しているらしいことが明らかになりました。というのも、関連性の疑われるウェブプロパティが合計6,456個（共通のメールアドレスを使用しているドメイン名1,103個、IPアドレス517個、共通のIPアドレスを使用しているドメイン名4,028個）検出されたためです。そして、そのうち31個（共通のメールアドレスを使用しているドメイン名10個、IPアドレス14個、共通のIPアドレスを使用しているドメイン名7個）は、すでに悪意あるプロパティに分類済みのものでした。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

IoCと特定された防弾ホスティングサービスのドメイン名

- 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

ドメイン名1～50個の登録に使用された公開メールアドレスの例

- 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

共通のメールアドレスを使用していたドメイン名の例

- 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

共通のメールアドレスを使用していた悪意あるドメイン名の例

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

専用IPアドレスの例

- 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

悪意ある専用IPアドレスの例

- 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

共通のIPアドレスを使用していたドメイン名の例

- 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

共通のIPアドレスを使用していた悪意あるドメイン名の例

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