DNSの徹底調査でBlackNet RATの履歴を追跡

目次

要旨

COVID-19の大流行中に初めて発見され、同ウイルスの効果的な治療法を提供するスパムメッセージを通じて配布されたBlackNet RATは、世界的な危機を生き延びたようです。このリモートアクセス型トロイの木馬（RAT）の運用者は、その後も悪質な活動を続けています。BlackNetボットネットは、2023年第1四半期のトップ・ボットネットの1つに挙げられました。

BlackNet RATが稼働していた3年間を通じて、複数の研究者がこのマルウェアを分析し、レポートを発表してきました。Alienvault OTXのコントリビューターは、この脅威に関連する何千ものセキュリティ侵害インジケーター（IoC）を収集しました。

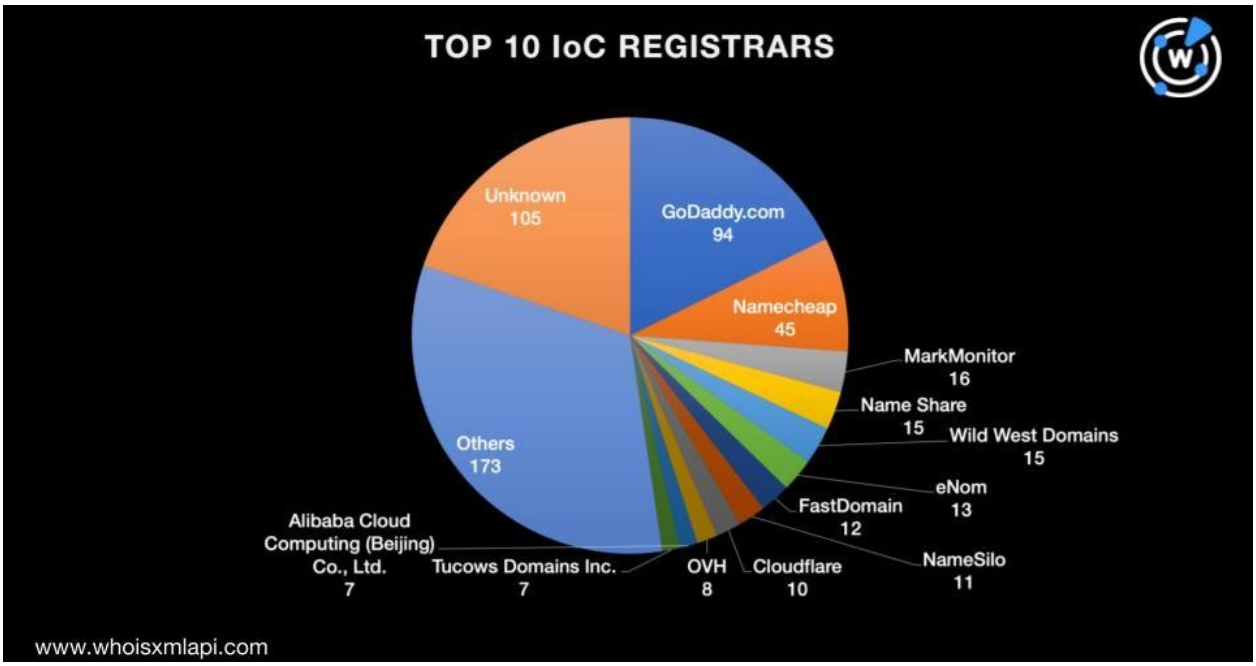
WhoisXML API の研究チームは、54個のIPアドレスと531個のドメイン名からなるその公開IoCリストを拡張するべく、DNSインテリジェンスを活用して未報告のアーティファクトの特定を試みました。その結果、以下が判明しました。

- 未公開の244個のIPアドレスへの名前解決。マルウェアチェックによりそのうち33個には悪意があることを確認
- 共通のメールアドレスを使用している697個のドメイン名。マルウェア一括チェックにより、そのうち3個は悪意あるドメイン名と確認
- 共通のIPアドレスを使っている5,232個のドメイン名。マルウェアの一括チェックにより、そのうち9個に悪意があることが判明

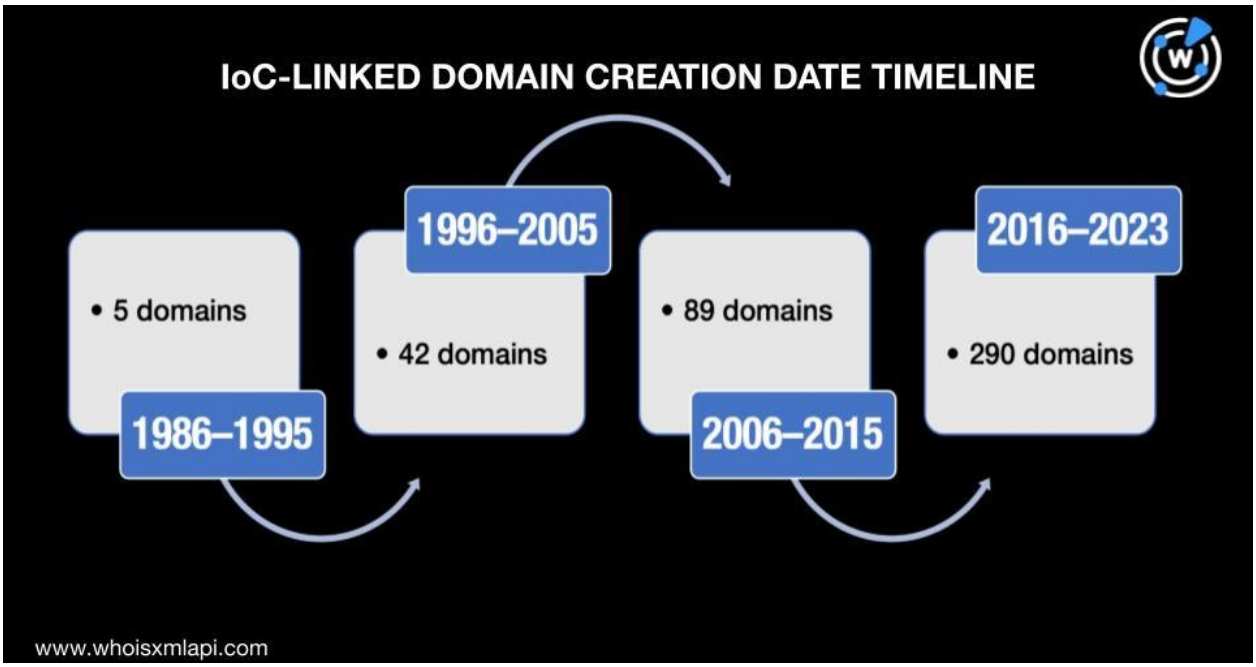
IoCに関するDNSの事実

まず、Alienvault OTXのリストにある合計585個のIoCを詳しく調べることから調査を開始しました。IoCとされた531個のドメイン名（以下「ドメインIoC」）をBulk WHOIS Lookupで検索したところ、次の結果が得られました。

- レジストラの上位はGoDaddy.com（94個のドメインIoCを管理）を筆頭に、Namecheap（45個）、MarkMonitor（16個）、Name Share（15個）、Wild West Domains（15個）、eNom（13個）、FastDomain（12個）, NameSilo（11個）、Cloudflare（10個）、OVH（8個）、Alibaba Cloud Computing (Beijing)（7個）、Tucows Domains（7個）でした。合計105個のドメインIoCではレジストラ情報を公開しておらず、残りの173個は58の別のレジストラに分散して管理されていました。



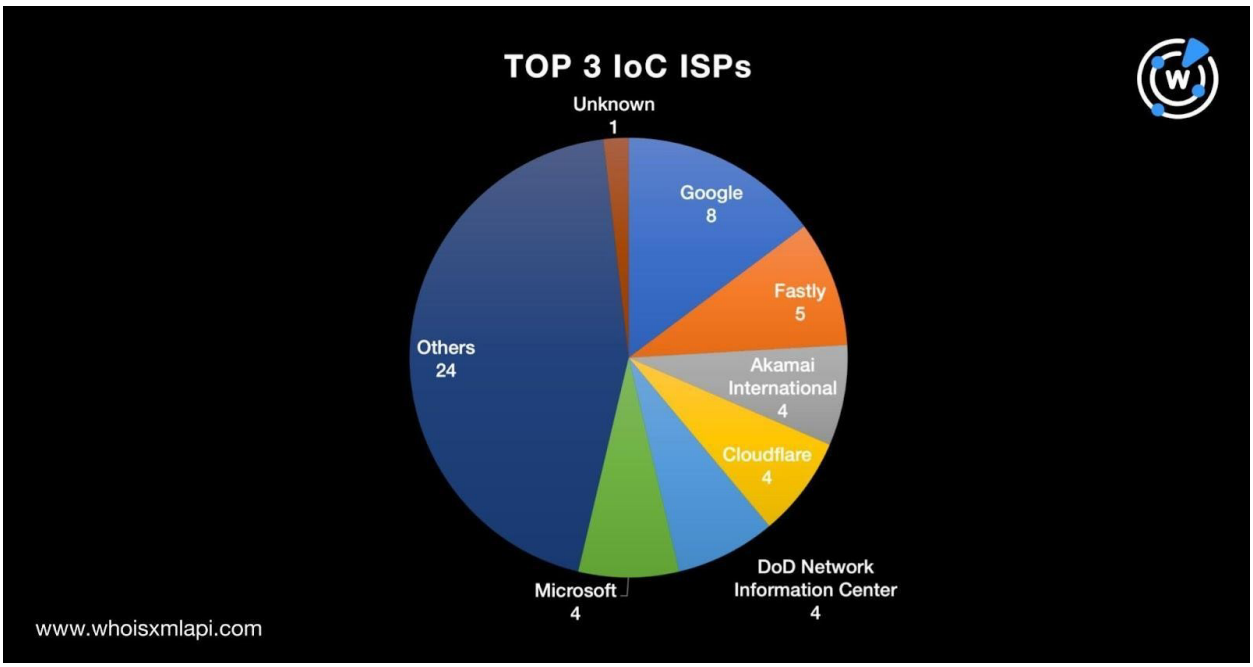
- ドメインIoCが新規登録されたタイミングは、1986年から2023年の間という広範囲にわたっていました。このことから、BlackNet RATの運用者はマルウェアを仕込んだページをホストするドメイン名の年齢を特に考慮していなかったと推測できます。ただし、105個のドメインIoCは、WHOIS上で新規登録日を確認できませんでした。



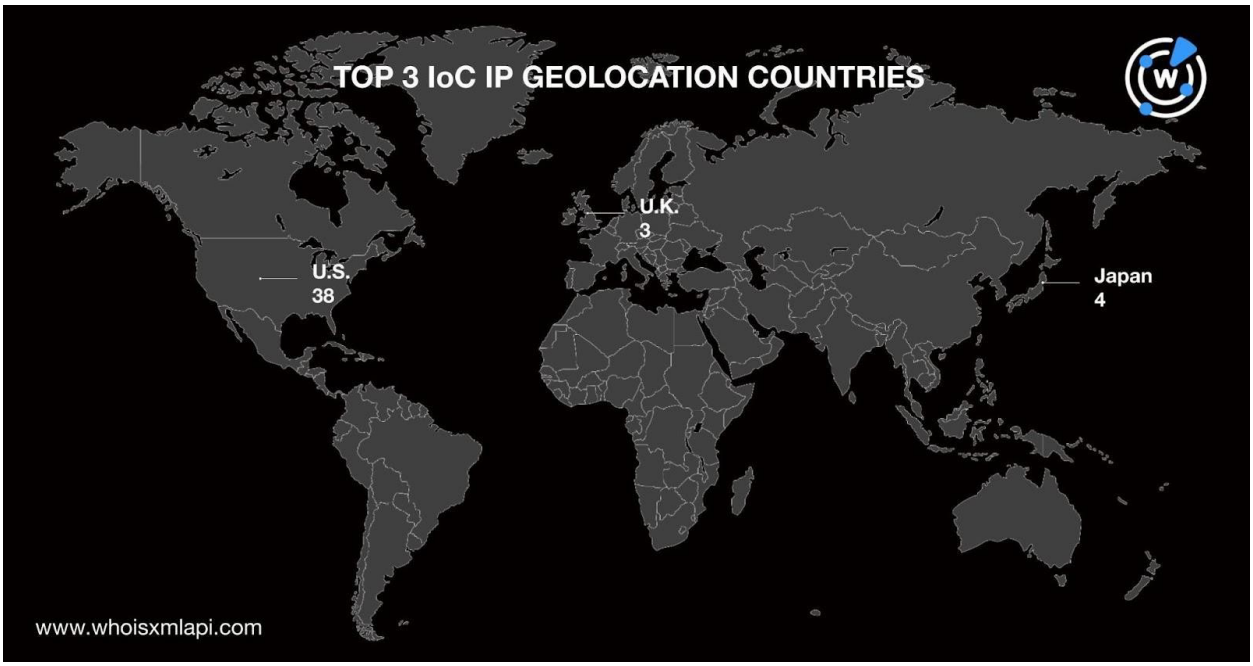
- ドメインIoCの登録国として最も多かったのは、米国（258個）、アイスランド（34個）および英国（17個）でした。他方、125個のドメインIoCは、登録者の国の情報を公開していませんでした。そして、残りの97個のドメインIoCの登録国は別の34カ国に分散していました。

次に、IoCとして特定された54個のIPアドレス（以下「IPアドレスIoC」）を[Bulk IP Geolocation Lookup](#)にかけたところ、以下が判明しました。

- インターネットサービスプロバイダー（ISP）のトップはGoogleで、8個のIPアドレスIoCを管理していました。2位は Fastlyで5個、3位を分け合ったのはAkamai International、Cloudflare、DoD Network Information CenterおよびMicrosoftで、それぞれ4個を管理していました。



- 最多である38個のIPアドレスIoCのジオロケーションは米国を指していました。これは、米国で最も多くのドメインIoCが登録されていたことと符号しています。IPアドレスIoCの地理的位置として米国の次に多かったのは、日本（4個）と英国（3個）でした。残りの9個のIPアドレスIoCは、他の6カ国に分散していました。



IoCリスト拡張分析でわかったこと

次に、未報告の関連アーティファクトを見つけ出すため、Alienvault OTXで公開されているIoCリストの拡張を試みました。

まず、531個のドメインIoCをWHOIS History Searchで調べたところ、495個のドメインIoCの過去のWHOISレコードに登録者のメールアドレスが公開の状態で残っていました。

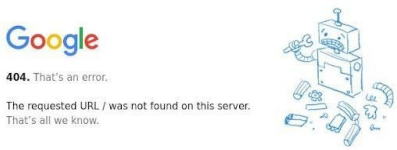
それらのメールアドレスをキーワードとしてReverse WHOIS Searchで検索した結果、共通のメールアドレスを使用しているドメイン名が697個検出されました。マルウェアの一括チェックにより、そのうち3個は悪意あるドメイン名に分類されました。3個のうちの1個、go-bitly[.]comは空白のページに繋がりましたが、著名なURL短縮サービスのブランド名「Bitly」をドメイン名の文字列に含んでいます。このドメイン名をWHOIS Lookupにかけたところ、WHOISレコードではBitlyへの帰属を確認できませんでした。

次に、531個のドメインIoCをDNS Lookupで検索してみました。その結果、IoCリストに含まれていない244個のIPアドレスが検出されました。そして、マルウェアチェックによりそのうち33個は悪意あるものと判定されました。

さらに、合計298個のIPアドレス（54個のIPアドレスIoCと上記の検索で検出された244個のIPアドレス）についてReverse IP Lookupを実行しました。その結果、152個は専用ホストらしいことがわかりました。それらは、IoCリストに含まれていない合計5,232個のドメイン名をホストしていました。マルウェア一括チェックの結果、そのうち9個のドメイン名には悪意があることが確認されました。

Screenshot Lookupにより、その悪意あるドメイン名のうち2個はアクティブなコンテンツをホストし続けていたことが判明しました。

共通のIPアドレスにホストされていた悪意あるドメイン名
pairdevice[.]gleのスクリーンショット



共通のIPアドレスにホストされていた悪意あるドメイン名
wyshop056[.]comのスクリーンショット

—

今回当社で行ったBlackNet RATのIoCリスト拡張分析により、潜在的な関連アーティファクトが6,173個新たに検出されました。そのうち45個（33個のIPアドレスと12個のドメイン名）は、悪意あるウェブプロパティでした。

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

Alienvault OTXが収集したBlackNet RATのIoC

- 87[.]62[.]96[.]246
- 23[.]67[.]33[.]24
- 199[.]184[.]215[.]11
- 163[.]172[.]184[.]32
- 116[.]203[.]50[.]182
- 148[.]113[.]162[.]135
- 108[.]181[.]62[.]185
- 104[.]124[.]1[.]33
- 35[.]172[.]94[.]1
- 34[.]102[.]136[.]180
- 182[.]22[.]25[.]124
- 172[.]67[.]187[.]204
- 172[.]67[.]177[.]211
- 104[.]21[.]91[.]185
- 104[.]21[.]84[.]71
- 100[.]24[.]208[.]97
- 50[.]87[.]249[.]29
- 162[.]0[.]223[.]226
- 156[.]231[.]25[.]88
- 29[.]1[.]1[.]169
- 2[.]19[.]96[.]163
- 74[.]217[.]253[.]92
- 67[.]199[.]248[.]13
- 67[.]199[.]248[.]12
- 216[.]58[.]204[.]132
- 172[.]217[.]169[.]68
- 151[.]101[.]120[.]133
- 131[.]253[.]33[.]203
- 107[.]21[.]218[.]43
- 68[.]169[.]217[.]172
- 33[.]28[.]101[.]95
- 26[.]37[.]247[.]52
- 212[.]161[.]61[.]168
- 212[.]143[.]182[.]52
- 210[.]31[.]213[.]23
- 21[.]173[.]189[.]20
- 20[.]99[.]184[.]37
- 20[.]80[.]129[.]13
- 142[.]251[.]33[.]68
- 142[.]250[.]217[.]100
- 142[.]250[.]200[.]36
- 133[.]109[.]199[.]185

- 133[.]108[.]199[.]185
- 12[.]179[.]89[.]13
- 106[.]89[.]54[.]20
- 103[.]125[.]250[.]142
- 20[.]99[.]133[.]109
- 185[.]199[.]111[.]133
- 185[.]199[.]110[.]133
- 185[.]199[.]109[.]133
- 185[.]199[.]108[.]133
- 23[.]216[.]147[.]64
- 165[.]160[.]15[.]20
- 165[.]160[.]13[.]20
- msn[.]com
- muid18c0382ad3a0666729fb2bb9d2ec67bdmicrosoft[.]com
- muid01e26509e61469f30347769ae75868b1msn[.]com
- 863712738031059121muid18c0382ad3a0666729fb2bb9d2ec67bdmicrosoft[.]com
- 1137592638999383310591 21muid01e26509e61469f30347769ae75868b1msn[.]com
- 102545380876831137592638999383310591 21usrlocmsn[.]com
- facebook[.]com
- httpsmetro-tmo[.]com
- turtlepeak[.]co
- trysmalltalkagency[.]com
- tryclik[.]com
- swagbybrilliant[.]com
- psychologycompass[.]co
- onlinebusinessaccountant[.]com
- logsforhire[.]com
- ggleadgen[.]com
- buildmydashboards[.]com
- kbcbrussels[.]be
- wynnsustainability[.]com
- withsecure[.]com
- tikkie-onlinenl[.]me
- tejastoyota[.]com
- scottishwidows[.]co[.]uk
- pngtree[.]net
- permanente[.]org
- onlinevervangen[.]info
- napletonsautopark[.]com
- mcgrathhyundaicr[.]com
- mallsbrasilplural[.]com[.]br
- gullotoyota[.]com
- genialgestao[.]com[.]br
- garagedoorsma[.]com
- fairfaxmazda[.]com
- eliolv[.]com
- boleromatti[.]be
- bettingpartners[.]com
- luxurycasino[.]com
- moderate[.]ml
- high[.]ml
- ukcasinoclub[.]eu
- ubinary[.]com
- ragingbullcasino[.]com
- powerplaypoints[.]com
- toolbar[.]google
- vspxhale[.]us
- vizius[.]us
- ulit[.]us
- theaccesspath[.]us
- seriousseeds[.]us
- retailbrilliance[.]us
- referenceratings[.]us
- rebelradiolive[.]com
- qydc[.]us
- queensyoungdemocraticparty[.]us
- queensydc[.]us
- queensldp[.]us
- queenslatinodemocraticparty[.]us
- projectarrowhead[.]us
- osourceglobal[.]org
- northpoleroute[.]com
- neod[.]us

- mylegalcollaborative[.]us
- mentalillnesssucksinstitute[.]us
- mariaelamine[.]com
- manyarticles[.]info
- jdrftalent[.]org
- fasttrackfund[.]com
- europeananticellulitetreatment[.]com
- earthbondproperty[.]com
- designscapital[.]com
- cosmosoftventures[.]com
- britishbusinessfunding[.]co
- bayouselfmedia[.]com
- bayislistings[.]com
- arunisharma[.]com
- aptracking1[.]com
- anipetkingdom[.]com
- yellowstonepharmacy[.]com
- xn--telemedicna-5xb[.]lv
- trocadero[.]ie
- rollesgraciejiujitsu[.]com
- nesmaui[.]com
- ganevents[.]com
- ceoaccel[.]com
- buildonhope[.]org
- brateneconst[.]com
- vizualintelligenceconsulting[.]com
- sixves[.]com
- mezf-rthr[.]com
- maudsix[.]com
- g20rx6[.]xyz
- aviewed[.]com
- yurtdisilink[.]online
- whatcom[.]cfd
- testingmuch[.]xyz
- spartanpremiacoes[.]com
- otrap[.]link
- junaidstutorials[.]com
- hinfo[.]com
- goodwaveinnovativesolutions[.]com
- getmedia-pro[.]com
- duluthpackblog[.]com
- darfiq[.]com
- communitycareenhancement[.]org
- clareador[.]site
- cagestoreshop[.]com
- bb44zz[.]com
- azdcloud[.]com
- 7curiousrituals[.]com
- valuebuildersystem[.]com
- uc2b[.]net
- tyeunderwood[.]realtor
- tiffanybruington[.]realtor
- suewyllie[.]com
- stemmleplumbing[.]com
- smiley-roofing[.]com
- sk-lh[.]com
- sharonplc[.]store
- roblong[.]realtor
- renishawilliams[.]realtor
- neurobytes[.]tech
- nataliemoore[.]realtor
- melissahibbert[.]realtor
- mediacollege[.]site
- lubea[.]website
- layerfive[.]com
- laginawynn[.]realtor
- kwanzoo[.]com
- kimheather[.]realtor
- kevenhernandez[.]realtor
- juliemuniz[.]realtor
- jaipur[.]ie
- isabelleswindowdesignvestal[.]com
- fotosbel[.]store
- dreampropertieswithregina[.]realtor
- dekart[.]com
- davidball[.]realtor
- cavmfg[.]com
- call32logistics[.]com
- benjohnson[.]realtor
- bcae[.]us

- aurelio[.]realtor
- attesterecharge[.]fr
- ashelby[.]realtor
- skilledup[.]life
- inversegamer[.]com
- 19slottica[.]online
- wjpso[.]bond
- wixmoreltd[.]com
- werkzeug-sale[.]com
- usdtpool[.]website
- uhbbysli[.]shop
- ubbgntof[.]top
- tyhgb[.]online
- tiyubb51[.]com
- spxstars[.]net
- redtube[.]express
- pornvid2[.]live
- onocnaconri[.]tk
- obsyhwx[.]xyz
- nhacaiuytinlk[.]com
- nanobot-tools[.]com
- mostbetcasinos-slots[.]top
- micnosoftupdates[.]com
- mexicocityhotels377176[.]life
- lotosports[.]bet
- livessy[.]com
- lanaudierequalifie[.]life
- krypton-services[.]com
- kieranryates[.]xyz
- johnnyquach[.]com
- haveagency[.]com
- hailzing[.]com
- erotiklove[.]xyz
- d4057[.]top
- bytesblitz[.]com
- auiviser[.]beauty
- askthehouse[.]com
- 785859[.]com
- 52gpcai[.]com
- whereinvienna[.]com
- verinfos[.]com
- siraat[.]sa
- prettymay[.]net
- nakedcomms[.]com
- mycookbook[.]org
- maison-kayser-usa[.]com
- luminafrica[.]com
- labelsprinter[.]com
- iphwn[.]org
- greencookbook[.]org
- gongbiart[.]com
- gillmanbarracks[.]com
- crazyaboutgreens[.]com
- crazyaboutbeans[.]com
- asianart[.]blog
- wpad[.]beauty
- mex33[.]info
- insuranceblog[.]xyz
- contex33[.]xyz
- bomberzilla[.]com
- tmobile[.]com
- kbclease[.]lu
- bolero[.]be
- usrlocmsn[.]com
- u002dmobile[.]com
- suidmmicrosoft[.]com
- suidmicrosoft[.]com
- noformmicrosoft[.]com
- muid33acff0dec5d6e8c0355ec9eed d96f0fmsn[.]com
- muid0f6dcaebb21a6ea53a29d978b 3566fd8microsoft[.]com
- 416627915631059089muid0f6dcae bb21a6ea53a29d978b3566fd8micro soft[.]com
- 1microsoft[.]com
- 13755141701854063105908 9muid33acff0dec5d6e8c0355ec9eedd96f0f msn[.]com

- 102514074679043113755141700291563105908 9usrlocmsn[.]com
- business-report-service[.]pro
- business-report-security[.]pro
- business-acc[.]pro
- maciejszwabe[.]com
- nopify[.]pro
- mellowads[.]com
- adfoc[.]us
- womanspring[.]net
- womanindustry[.]net
- watermaster[.]net
- waterlanguage[.]net
- waterindustry[.]net
- verifypurchase[.]online
- ubercpm[.]com
- thoughtwonder[.]net
- thoughtspring[.]net
- thoughtmaster[.]net
- summermaster[.]net
- stillspring[.]net
- solisdq[.]info
- smokeindustry[.]net
- shrturl[.]site
- reshemporium[.]com
- qq4004[.]com
- prettyguard[.]net
- peak-valleyadvertising[.]com
- partymaster[.]net
- partyindustry[.]net
- paidonlinesites[.]com
- outsidebanker[.]net
- organicdiscover[.]com
- occulusblu[.]com
- mybodysaver[.]com
- movementfence[.]net
- movementbanker[.]net
- mimortgageexpert[.]com
- membermaster[.]net
- joneshondaservice[.]com
- iqpt[.]info
- ifaucet[.]net
- hearty[.]me
- goldfishka12[.]net
- gaigoilaocai[.]com
- freshspring[.]net
- freshbasket[.]net
- followsuccess[.]net
- followmaster[.]net
- followbasket[.]net
- fightdiscover[.]net
- experiencelanguage[.]net
- experiencebefore[.]net
- doublespring[.]net
- doctorfound[.]net
- desiresuccess[.]net
- desirebefore[.]net
- cummingsforum[.]com
- cuadorcoast[.]com
- crowdsuccess[.]net
- crowdspring[.]net
- crowdbanker[.]net
- craftbychristians[.]com
- cpmgo[.]com
- coinurl[.]com
- buildingsuccess[.]net
- brokenspring[.]net
- briative[.]com
- binaryaffiliates[.]com
- beginsuccess[.]net
- apps4fans[.]net
- alreadyfound[.]net
- alreadycontinue[.]net
- unpkg[.]com
- ipinfo[.]io
- googletagmanager[.]com
- adobe[.]com
- 3dadobe[.]com
- yahoo[.]com
- tapad[.]com

- t-mobile[.]com
- snapchat[.]com
- sc-static[.]net
- krxd[.]net
- ispot[.]tv
- doubleclick[.]net
- demdex[.]net
- bluekai[.]com
- bing[.]com
- amazon-adsystem[.]com
- adroll[.]com
- metropcs[.]mobi
- urlscan[.]io
- twitter[.]com
- metrobyt-mobile[.]com
- logourlscan[.]io
- business-report-security[.]online
- widerreach[.]org
- widerreach[.]info
- widerreach[.]biz
- tdautoinsurance[.]us
- tdautoinsurance[.]info
- sipavibart[.]us
- royalchin[.]com
- nopify[.]us
- knoxs[.]ink
- knowthalassemia[.]org
- knowthalassemia[.]info
- grove[.]mov
- epostbnk-m[.]cloud
- easyfries[.]com
- business-report-service[.]online
- business-report-security[.]info
- azd3152[.]us
- assurancesaxa[.]fr
- archden[.]link
- zitly[.]net
- twitterintegration[.]com
- tesco-mobile[.]com
- roksit[.]net
- getweathertite[.]com
- gramfort[.]net
- dns0[.]org
- sheelds[.]link
- factana[.]com
- aura[.]services
- tomoncle[.]online
- nbupaymentsvendorcerts[.]com
- jeonnamtour[.]kr
- zfx-asia[.]com
- nw18[.]com
- molotov[.]tv
- mangiro[.]com
- thekittypad[.]com
- securitystud[.]io
- neyapan[.]xyz
- neolur[.]xyz
- libex[.]co
- jamieol[.]com
- gx3fdn[.]org
- eventix[.]link
- bukacinci[.]xyz
- adec[.]co
- gunowners[.]me
- ggpoker[.]com
- dxpr[.]es
- dreampathdx[.]info
- tossnews[.]net
- supportpage[.]us
- rebirth[.]events
- ocl23[.]com
- jackpotcitycasino[.]info
- business-report-meta[.]pro
- business-policy-manage[.]pro
- business-manage-support[.]pro
- wrsassocinc[.]com
- systech-na[.]com
- productdevelopmentmktngco[.]com
- petergangelos[.]com
- martindougp[.]com

- kleinshallmarkcards[.]com
- hynetics[.]com
- gtoops[.]com
- georgiaconservancyinc[.]com
- davislaurajesq[.]com
- ctmailco[.]com
- chuckdenmark[.]com
- christanscorner[.]com
- chamberofcommrcepierrearea[.]com
- ccmetalfabricationsinc[.]com
- businessproductsincorporated[.]com
- brooksbrowninsuranceagency[.]com
- bblmasoc[.]com
- appliedphotographics[.]com
- 4databasedesign[.]com
- windowsupdate[.]com
- powerof[.]pub
- nr-data[.]net
- microsoft[.]com
- hgah[.]pub
- google[.]com
- githubusercontent[.]com
- disallowedcertstl[.]cab
- bitly[.]com
- bit[.]ly
- watertips[.]info
- twitter-account[.]com
- tdbankgo[.]com
- siemensmedical[.]com
- sergiotavarez[.]com
- rxweb-prd[.]com
- rolexcollection[.]site
- rolex-water[.]shop
- rolex-want[.]shop
- rolex-swim[.]shop
- rolex-room[.]shop
- rolex-magie[.]shop
- rolex-from[.]shop
- rolex-free[.]shop
- mifacturabait[.]com[.]mx
- metro-tmo[.]com
- httpsaffordablemovers[.]biz
- ftuapps[.]com
- frostsecurity[.]net
- e-pitchforks[.]com
- digestiplus[.]com[.]au
- digestiplus[.]com
- dginfini[.]com
- dealerflex[.]link
- data2decisions[.]kz
- cumbrefinancieraegade[.]com
- countrykitchen[.]com
- cottagedouble[.]com
- complanutrigro[.]com
- complan[.]nz
- complan[.]asia
- business-portal[.]site
- business-portal[.]guru
- business-manage-support[.]online
- business-manage-support[.]info
- bankofamerica[.]org[.]gg
- artboard[.]me
- 3mauto[.]us
- 2xist[.]biz
- westside-solutions[.]com
- waughscustoms[.]com
- smcdltd[.]com
- rockymountainroofers[.]com
- qualitymachinerysystems[.]co
- nowenvironmental[.]com
- njwashout[.]com
- movetek[.]com
- mmlighting[.]com
- medicsusa[.]com
- jjairductcleaning[.]com
- gtsbus[.]com
- flcoolingac[.]com
- dmrclinics[.]org
- coolamericaair[.]com

- bransonconstructiontx[.]com
- blankind[.]com
- asicorporate[.]com
- switchdifferent[.]com
- sigops-france[.]fr
- omesa[.]io
- mopolo[.]fr
- mettray[.]com
- melenchonouimais[.]fr
- mahmoudemad[.]com
- jaskula[.]fr
- ipception[.]fr
- ipception[.]com
- hfdb[.]io
- csemver[.]org
- chandanrai[.]com
- bokeng[.]top
- vobelixora[.]com
- throbscalpelaffirm[.]com
- tacticpoignantsteeple[.]com
- situationhostilitymemorable[.]com
- scornfulabsorbploy[.]com
- privatdns[.]buzz
- pampasdobrasil[.]com
- nachamu7[.]com
- lihi1[.]cc
- grumbletonight[.]com
- fivestarscale[.]com
- buymacaron[.]com
- 10percent[.]ai
- try-to[.]win
- sillilight[.]com
- mo-sadeghi[.]ir
- ldyshop[.]com
- joshuajenkinslaw[.]com
- intermouette[.]com
- hamburgertime[.]org
- google[.]re
- google[.]com[.]gp
- asiaism[.]com
- 3ffiyg[.]live
- bamurindustries[.]com
- indextv[.]org
- salaros[.]com
- gxy-ypy[.]top
- githack[.]com
- angelcrochet[.]com
- tdmyappweb[.]com
- siemens[.]sa
- scaffolddesign[.]net
- experianaperture[.]io
- canonsolutions[.]sa
- canonsaudiarabia[.]sa
- xn--e1arb1a1f07c[.]com
- vertbaudet[.]com[.]sa
- valvoline[.]com[.]sa
- uueasy[.]com
- tipaltipi[.]us
- tipaltipi[.]org
- skroutznewbalance[.]com
- rolextokyo[.]com
- rolexabc[.]com
- raileurope[.]com[.]sa
- powerresponsive[.]com
- northtrustees[.]com
- myups[.]biz
- mysterylessons[.]org
- mysteryeducation[.]org
- myhomeo[.]store
- myhomeo[.]site
- myhomeo[.]org
- louisvuitton[.]com[.]sa
- loewsgifts[.]com
- linuxjournal[.]it
- delarue[.]money
- certinia[.]us
- canonksa[.]sa
- canonksa[.]com[.]sa
- albunorm[.]com[.]sa

共通のメールアドレスを使用していたドメイン名の例

- 10percent[.]ai
- 19slottica[.]online
- 1microsoft[.]com
- 2xist[.]biz
- 3dadobe[.]com
- 3ffiyg[.]live
- 3mauto[.]us
- 4databasedesign[.]com
- 52gpcai[.]com
- 785859[.]com
- 7curiousrituals[.]com
- 7xl-ggpoker[.]com
- adfoc[.]us
- adroll[.]us
- albunorm[.]com[.]sa
- alreadycontinue[.]net
- alreadyfound[.]net
- amazon-adsystem[.]com
- angelcrochet[.]com
- anipetkingdom[.]com
- appliedphotographics[.]com
- apps4fans[.]net
- aptracking1[.]com
- archden[.]link
- artboard[.]me
- arunisharma[.]com
- ashelby[.]realtor
- asiaism[.]com
- asianart[.]blog
- asicorporate[.]com
- askthehouse[.]com
- assurancesaxa[.]fr
- attesterecharge[.]fr
- auiviser[.]beauty
- aura[.]services
- aurelio[.]realtor
- aviewed[.]com
- azd3152[.]us
- azdcloud[.]com
- bamurindustries[.]com
- bankofamerica[.]org[.]gg
- bayislistings[.]com
- bayouselfmedia[.]com
- bb44zz[.]com
- bblmasoc[.]com
- bcae[.]us
- beginsuccess[.]net
- benjohnson[.]realtor
- betaalpas-onlinevervangen[.]info
- bettingpartners[.]com
- binaryaffiliates[.]com
- bitly[.]com
- blankind[.]com
- bluekai[.]com
- boisson-bolero[.]be
- bokeng[.]top
- boleromatti[.]be
- bomberzilla[.]com
- bransonconstructiontx[.]com
- brateneconst[.]com
- briative[.]com
- britishbusinessfunding[.]co
- brokenspring[.]net
- brooksbrowninsuranceagency[.]com
- buildingsuccess[.]net
- buildmydashboards[.]com
- buildonhope[.]org
- bukacinci[.]xyz
- business-acc[.]pro
- business-manage-support[.]info
- business-manage-support[.]online
- business-manage-support[.]pro
- business-policy-manage[.]pro
- business-portal[.]guru

- business-portal[.]site
- business-report-meta[.]pro
- business-report-security[.]info
- business-report-security[.]online
- business-report-security[.]pro
- business-report-service[.]online
- business-report-service[.]pro
- businessproductsincorporated[.]com
- buymacaron[.]com
- bytesblitz[.]com
- cagestoreshop[.]com
- call32logistics[.]com
- canonksa[.]com[.]sa
- canonksa[.]sa
- canonsaudiarabia[.]sa
- canonsolutions[.]sa
- cavmfg[.]com
- ccmetalfabricationsinc[.]com
- cdn-krxd[.]net
- cdn-unpkg[.]com
- ceoaccel[.]com
- certinia[.]us
- chamberofcommrcepierrearea[.]com
- chandanrai[.]com
- christanscorner[.]com
- chuckdenmark[.]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

- epostbnk-m[.]cloud
- go-bitly[.]com

IPアドレスへの名前解決の例

- 104[.]123[.]70[.]18
- 104[.]123[.]70[.]27
- 104[.]123[.]70[.]57
- 104[.]123[.]70[.]64
- 104[.]16[.]122[.]175
- 104[.]16[.]123[.]175
- 104[.]16[.]124[.]175
- 104[.]16[.]125[.]175
- 104[.]16[.]126[.]175
- 104[.]18[.]35[.]106
- 104[.]207[.]254[.]78
- 104[.]21[.]33[.]107
- 104[.]21[.]35[.]28
- 104[.]21[.]4[.]171
- 104[.]21[.]48[.]14
- 104[.]21[.]60[.]178
- 104[.]21[.]68[.]205
- 104[.]21[.]74[.]109
- 104[.]21[.]8[.]46
- 104[.]21[.]81[.]138
- 104[.]21[.]84[.]122
- 104[.]21[.]84[.]55
- 104[.]21[.]90[.]115
- 104[.]21[.]96[.]73
- 104[.]244[.]42[.]1
- 104[.]244[.]42[.]129
- 104[.]244[.]42[.]193
- 104[.]244[.]42[.]65
- 104[.]26[.]6[.]10
- 104[.]26[.]7[.]10
- 107[.]21[.]217[.]230
- 108[.]187[.]44[.]48
- 108[.]187[.]44[.]49
- 109[.]105[.]138[.]1
- 119[.]47[.]85[.]200
- 13[.]107[.]21[.]200
- 13[.]226[.]210[.]43
- 13[.]226[.]210[.]81
- 13[.]226[.]210[.]85
- 13[.]226[.]210[.]89

- 13[.]248[.]169[.]48
- 140[.]82[.]114[.]4
- 141[.]98[.]6[.]168
- 142[.]250[.]188[.]228
- 142[.]250[.]189[.]8
- 142[.]250[.]68[.]4
- 142[.]250[.]72[.]164
- 142[.]250[.]72[.]174
- 142[.]251[.]40[.]46
- 144[.]76[.]29[.]42

悪意あるIPアドレスへの名前解決の例

- 104[.]207[.]254[.]78
- 104[.]244[.]42[.]129
- 104[.]244[.]42[.]193
- 104[.]244[.]42[.]65
- 104[.]26[.]6[.]10
- 104[.]26[.]7[.]10
- 108[.]187[.]44[.]49
- 13[.]107[.]21[.]200
- 13[.]248[.]169[.]48
- 141[.]98[.]6[.]168
- 15[.]197[.]142[.]173
- 15[.]197[.]148[.]33
- 172[.]234[.]26[.]236
- 173[.]233[.]137[.]36
- 173[.]233[.]137[.]44
- 173[.]233[.]137[.]52
- 173[.]233[.]137[.]60
- 173[.]233[.]139[.]164
- 182[.]22[.]25[.]252
- 183[.]66[.]100[.]53

共通のIPアドレスを使用していたドメイン名の例

- 01seifw7uv[.]com
- 05552677[.]com
- 08185211866[.]com
- 10292677[.]com
- 108slottica[.]com
- 10fourteenclassic[.]com
- 125slottica[.]com
- 126slottica[.]com
- 127slottica[.]com
- 128slottica[.]com
- 129slottica[.]com
- 12minutestrategy[.]com
- 12pinedale[.]com
- 130slottica[.]com
- 131slottica[.]com
- 132slottica[.]com
- 1334birchcliffdrive[.]ca
- 1337xxx[.]xyz
- 133slottica[.]com
- 134slottica[.]com
- 135slottica[.]com
- 136slottica[.]com
- 137slottica[.]com
- 139slottica[.]com
- 13ninjas[.]com
- 156enfield2611[.]com
- 157rivobahis[.]com
- 15carerecres[.]com
- 15windermere902[.]com
- 169rivobahis[.]com
- 16itech[.]com
- 174dunveganrd[.]ca
- 175tx[.]com
- 17ontario[.]com
- 17slottica[.]online
- 181davenport805[.]com
- 18732677[.]com
- 18holestillchristmas[.]com
- 18slottica[.]club
- 18slottica[.]online

- 19282677[.]com
- 19slottica[.]club
- 19slottica[.]online
- 1g53n3gtdo[.]com
- 1igame[.]com
- 1st[.]racing
- 1stcleaningservice[.]com[.]s3-website[.]us-east-2[.]amazonaws[.]com
- 200779[.]xyz
- 2023off[.]com
- 20slottica[.]club
- 2121[.]live
- 21alderbrook[.]com
- 21slottica[.]club
- 21slottica[.]online
- 22slottica[.]club
- 22slottica[.]online
- 23ig4j2yzb[.]com
- 23slottica[.]online
- 24hbg[.]nl
- 252woodley[.]com
- 25perf[.]net
- 2644minnesota[.]com
- 2655q8[.]com
- 28-ej-4-ik-6cs4i[.]com
- 28guestvilleave[.]com
- 2939t2939[.]com
- 2939v2939[.]com
- 2939vns1[.]com
- 2939vns2[.]com
- 2939vns3[.]com
- 2939vns4[.]com
- 2939vns5[.]com
- 2939w2939[.]com
- 2939x2939[.]com
- 2939z2939[.]com
- 2998[.]live
- 2dthaicuisine[.]com
- 2f-biapj-c2un[.]com
- 2upgw4db6[.]com
- 2y-t3j-4e[.]com
- 2ya6kuimdy[.]com
- 3-df-hfzjt[.]com
- 3-em-t2-5nh[.]com
- 3058[.]live
- 309jatc[.]org
- 30oldmillrdun603[.]ca
- 3133keokuk[.]com
- 317highpark[.]com
- 32juillet-pro[.]com
- 3526[.]live
- 3581[.]live
- 35claridge[.]com
- 360poolservices[.]com
- 360talos[.]co[.]uk
- 3856[.]live
- 3a7-c7-ic9[.]com
- 3ai[.]solutions
- 3b-3ih-c6k-z4[.]com
- 3d6y5bf67x[.]com
- 3dben[.]com
- 3ddynamicsolutions[.]com
- 3dprintviz[.]com
- 3drtst[.]ca
- 3jhuz7q5hb[.]com
- 3r6d-fcfpt6y[.]com
- 3rdwaveinnovation[.]com
- 3rdwaveinnovation[.]org
- 3rdwaveinnovations[.]com
- 3sg-g-eww68a[.]com
- 3tknt0awo0[.]com
- 3vboard[.]org
- 3w6e-db[.]com
- 3xtt813uc2[.]com
- 3z-cibuuz[.]com
- 3z[.]io
- 4-xw2degfj-sr3[.]com
- 4248juniata[.]com
- 4380tanglebrook[.]com
- 44-myx9p6[.]com

- 4423t9t0pb[.]com
- 44lesmount[.]com
- 466453[.]com
- 46wf-zjkgeu-kx[.]com
- 47northridgecres[.]com
- 48mt-segr[.]com
- 48surf[.]info
- 4948[.]live
- 4d-c7kimxga[.]com
- 4d722e526f626f74[.]com
- 4f[.]ua
- 4gameftp[.]ru
- 4gsam[.]com
- 4j9ksemv1q[.]com
- 4mv4y701kf[.]com
- 4my-em9-f7th[.]com
- 4nc5pc4-si[.]com
- 4nw-h99cjix[.]com
- 4ordr[.]com
- 4pnkt7-fda[.]com
- 4rn-z43yp[.]com
- 4rsgold[.]com
- 4s-dn-xe[.]com
- 4youargento[.]com[.]s3-website[.]us-east-2[.]amazonaws[.]com
- 5-2uy5x-3gznx-r[.]com
- 5-bjgedi[.]com
- 5035oscarpeterson[.]com
- 54silverview[.]com
- 5528waterman2s[.]com
- 56-y9mn[.]com
- 5ayrd-gix[.]com
- 5b72da-yh[.]com
- 5fivecanama[.]store
- 5glabdevsite[.]com[.]mx
- 5h-rw-68n75-8t[.]com
- 5ktees[.]com
- 5pz-b57tsj-8[.]com
- 5thelementordering[.]com
- 5tk-ezsfry[.]com
- 6-2jjuhkwkk[.]com
- 612888cashforhomes[.]com
- 6663z5w2js[.]com
- 6950montevideo[.]com
- 6aourt1qvb[.]com
- 6fhf-4ppi[.]com
- 6s-cujs3u-pna[.]com
- 705cumberland2[.]ca
- 724fairview[.]com
- 75slottica[.]com
- 78-h6hytd-6[.]com
- 7d-4m528-jbn[.]com
- 7jayonago[.]net
- 7kx-wgg-zx-up[.]com
- 7lakesbaseball-golf[.]com
- 7sevenmass[.]net
- 7tbzbv[.]live
- 7xp-uaabepa[.]com
- 8-byw96-zz[.]com
- 8-chbt-3k768pk[.]com
- 8-i27jb-y5[.]com
- 8031[.]live
- 816realty[.]com
- 818productions[.]com
- 81slottica[.]com
- 82realtygroup[.]com
- 82slottica[.]com
- 82w-2-pr5k[.]com
- 8308[.]live
- 8323[.]live
- 8351[.]live
- 8381[.]live
- 83slottica[.]com
- 8406[.]live
- 844-bcm78-8t8w[.]com
- 84slottica[.]com
- 85slottica[.]com
- 8600montgomery[.]com
- 86slottica[.]com
- 872mbmnt-u[.]com

- 87slottica[.]com
- 88parksidedr[.]com
- 88slottica[.]com
- 8928[.]live
- 89slottica[.]com
- 8e3-kizg2-3i[.]com
- 8f9c1f15-23b1-489c-a47d-a23ed09a3cab[.]com
- 8ke2-i-wdekg7[.]com
- 8marigoldave[.]ca
- 8t34n-npe3-i5c[.]com
- 8xedkhlty1[.]com
- 8z-ycs-cna[.]com
- 8z7r-97h4c-8ym[.]com
- 9005[.]live
- 9094podcast[.]com
- 90slottica[.]com
- 91nude[.]com
- 9233[.]live
- 9285[.]live
- 92slottica[.]com
- 936d-iyn55-s[.]com
- 9391[.]live
- 94eh-k-9yk-ap4e[.]com
- 94slottica[.]com
- 95slottica[.]com
- 9631[.]live
- 9681[.]live
- 9698[.]live
- 9865[.]live
- 98slottica[.]com
- 9985[.]live
- 99dolarmusicvideos[.]com
- 9aw-j-pr-4w[.]com
- 9b-azcr-egmemza[.]com
- 9bus8e-4ejx[.]com
- 9c3-s45k5-947[.]com
- 9fynjg-78[.]com
- 9ipcnvyuqq[.]com
- 9j-tbbxa-6kjh[.]com
- 9k-pjdeida6g8[.]com
- 9k3-pinnwn-pt[.]com
- 9l0glo0yo6[.]com
- 9m-zrip4u[.]com
- 9pk-kww657a-z[.]com
- 9q1ve9fmwn[.]com
- 9r3-3-3r8w9h[.]com
- 9tffzy55-sais[.]com
- 9u-hb4-gsd-on[.]com
- a-7rgupy-7dbxd[.]com
- a-84-8w-s-mz8h[.]com
- a-fw7cy7i[.]com
- a-way-aisf[.]com
- a1kebabsgirvan[.]co[.]uk
- a3pmfatima[.]xyz[.]s3-website[.]us-east-2[.]amazonaws[.]com
- a3tw-h766ce4i[.]com
- a59-fjhnj4-whs[.]com
- a8-yk-rr-rf[.]com
- aargroup[.]co[.]uk
- ababobschool[.]com
- abapna[.]com
- abbacare[.]org
- abc[.]wtf
- abc[.]xyz
- abiral[.]us
- abnamrob-nl[.]com
- abnamrocomfin[.]fr
- abusaki[.]com[.]s3-website[.]us-east-2[.]amazonaws[.]com
- academiadoimportador[.]com[.]br
- academiatechnos[.]com[.]br
- acadianpsych[.]com
- acceleratewithgoogle[.]com
- accountantcareerquerypros[.]co
- accp2[.]openbusiness[.]ing[.]de
- accsolutions[.]com[.]br
- accucleanfresh[.]com
- aceeliteservices[.]com
- acertagroup[.]com

- acqua[.]nl
- acquasoftwaresolutions[.]eu
- acquasoftwaresolutions[.]nl
- acramatic-control-retrofit[.]com
- acrewoodholdings[.]com
- active-ergonomics[.]co[.]uk
- activewills[.]com
- actuallybadsecurity[.]com
- adamdear[.]me
- adamsmock[.]net
- adamspanswick[.]com
- adcache[.]bargaintraderonline[.]com
- addictioncarenavigator[.]com
- adec[.]co
- adenaflorida[.]com
- adenasprings[.]org
- adencontracting[.]co[.]uk
- adfoc[.]us
- adgoogle[.]net
- adhdtreatments[.]xyz
- adlingo[.]com
- adllab[.]co
- admeld[.]com
- admtech[.]click
- adoptionri-freecollege[.]org
- adsense[.]com[.]hk
- adsense[.]com[.]ru
- adsense[.]cv
- adsense[.]re
- adslogix[.]com
- advancecycle[.]com
- advancedemtchallenge[.]com
- adventureengine[.]goog
- adventurelog[.]co[.]uk
- advertiseondish[.]com
- advertisercommunity[.]com
- advertiserscommunity[.]com
- adviceowl[.]google
- advocatecapital[.]com
- advokat-olsen[.]no
- adwords-community[.]com
- aeproduction[.]com
- afdevb[.]com
- afilmblog[.]com
- ag-plumbingheating[.]com
- ag-specstore[.]com
- aga2-zx-ag[.]com
- agathe-battestini[.]com
- agathebattestini[.]com
- age-za-5i[.]com
- agentfee[.]com[.]au
- agiletea[.]com
- agmensadvance[.]com
- agnewinsurance[.]co[.]uk
- agrhighdrivetourney[.]com
- agrium[.]bg
- agrium[.]ro
- agrowt[.]com
- agsys[.]net
- aid[.]monmouthcollege[.]edu
- aig-xu-w3-7s-h[.]com
- aigua[.]io
- aircelli[.]com
- airfundraiser[.]com
- airpizzahouse[.]co[.]uk
- airsense[.]us
- aishakespeare[.]io
- ajronline[.]org
- akalab[.]tech
- akathisia[.]org
- akshun[.]io
- akshvac[.]com
- aktivballangen[.]no
- al-campeggio[.]com
- al-campeggio[.]it
- alabamabasementfinishing[.]com
- alanacoworker[.]com
- alanapowersports[.]com
- alantree[.]net
- albertinasacaca1[.]com

- albertosmxfood-riverside-olomenu[.]com
- alborzfeizi[.]com
- alcampeggio[.]com
- alcampeggio[.]it
- alchemytechnologyresource[.]io
- aldumas[.]com
- alekseykovalchuk[.]com
- alexander-stark[.]com
- alexapowered[.]com
- alexborthwick[.]com
- alexfilm[.]cam
- alexhernandezlawyer[.]com
- alexsmolen[.]com
- alfanar-atc[.]com
- alfanar-calibration[.]com
- alfanar-es[.]com
- alfanaraluminium[.]com
- alfanarbena[.]com
- alfanarbuildingsystems[.]com
- alfanarconstruction[.]com
- alfanarenergy[.]com
- alfanarjobs[.]com
- alfanarmep[.]com
- alfanarprecast[.]com
- alfanarsmartsolutions[.]com
- alfanarsteel[.]com
- alfanartechnicalservices[.]com
- alfaromeoofscottsdale[.]com
- alfaromeousaofmelbourne[.]com
- alfaromeousaofnorthhouston[.]com
- alianzasalud[.]org[.]mx
- allareamovingcompany[.]com
- allbooked[.]co
- allcraigslistsearch[.]com
- allenandassociates[.]agency
- allgoodenergies[.]com
- allgoodenergy[.]net
- allpay[.]net
- allterrainsoup[.]com
- alm[.]hk
- almgolfouting[.]com
- alpaclass-hom[.]com
- alphatheranews[.]com
- alsteincloud[.]com
- alternativeairlines[.]com
- altosales[.]com
- am-hbjh2-6[.]com
- amawsau[.]com
- ambacosec[.]com
- amconline[.]co[.]uk
- amd-pctr[.]c[.]yimg[.]jp
- ameenster[.]com
- amegybk[.]com
- amegybtx[.]com
- americanarmorial[.]com
- americanbankersassociation[.]net
- americanhomeshield[.]com
- americanloans[.]com
- amicus9[.]com
- amo[.]site
- ampproject[.]com
- amslezak[.]com
- amsoftwaredesign[.]co[.]uk
- amtap[.]com
- amtauto[.]co[.]uk
- amtleasing[.]co[.]uk
- amtote[.]com[.]au
- amtspecialistcars[.]co[.]uk
- amydmorris[.]com
- analogmiko[.]com
- anarchius[.]org
- anavimarket[.]com
- ancientdoors[.]us
- andrejglavic[.]com
- andresmorelos[.]me
- andrewandmidori[.]com
- andrewcutler[.]info
- andrewpmiles[.]com
- androidtv[.]com

- anduokang[.]com[.]s3-website[.]us-east-2[.]amazonaws[.]com
- andyainsworth[.]tech
- andykautza[.]com
- angel2ladies[.]com
- angelcrochet[.]com
- angelguard[.]net
- angelospizzawausau[.]com
- animalcaregroup[.]com
- animlist[.]com
- anislerouge[.]com
- anmsolutions[.]com
- annmezzo[.]com
- annumapp[.]com
- anoiarock[.]com[.]s3-website[.]us-east-2[.]amazonaws[.]com
- anonymind[.]co[.]uk
- anonymind[.]com
- answear[.]hr
- anthonylmilholen[.]com
- anthonynguyen[.]lol
- antonywarring[.]com
- any[.]edge[.]bing[.]com
- anystaff[.]com
- anytimeccu[.]com
- anytimefitnesslanokaharbor[.]com
- anzelcwelding[.]com
- apagolf[.]com
- apata[.]coffee
- apexpertwitness[.]com
- apexplumbingky[.]com
- api[.]scrolller[.]com
- apicirclepay[.]com
- apictureofa[.]kiwi
- apieceofmyheartgolf[.]com
- apolishedfinish[.]com
- app-even[.]com
- app-tideway[.]london
- app[.]clickselly[.]s3-website[.]us-east-2[.]amazonaws[.]com
- app[.]postprod[.]honeycode[.]aws
- app[.]postprod[.]lowcodeapp[.]dev
- appdefensealliance[.]dev
- appitbyte[.]com[.]au
- appointmentking[.]com
- appritus[.]com
- apps4fans[.]net
- appsenterprisecustomers[.]com
- appspot[.]com
- aprathim[.]com
- aptracking1[.]com
- aqaorg[.]uk
- aquidneckcleaning[.]com
- aquilamg[.]com
- aquiobottles[.]com
- aralb[.]com
- aramcoworld[.]com
- arbol217[.]com[.]s3-website[.]us-east-2[.]amazonaws[.]com
- architectsvsengineersgolf[.]com
- archives[.]ge
- arcidc[.]com
- arcticpasts[.]org
- ardentgolf[.]com
- arielarmor[.]com
- arket[.]ly
- armonddaltoncloud[.]com
- armorpestcontrolmd[.]com
- aroundconnections[.]nl
- artemis-international[.]ch

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

- capitalbkusa[.]com
- emiratestaxfree[.]cloud
- epostbnk-bg[.]cloud
- epostbnk-m[.]cloud

- evinrude[.]com[.]au