A DNS Deep Dive into BreachForums Domains

Table of Contents

Executive Report

The Federal Bureau of Investigation (FBI) shut down BreachForums, a forum for English-speaking black hat hackers, on 21 March 2023, following the arrest of its owner Conor Brian Fitzpatrick. More recent reports, however, stated it's back up under new management—that of hacking group ShinyHunters and original administrator Baphomet.

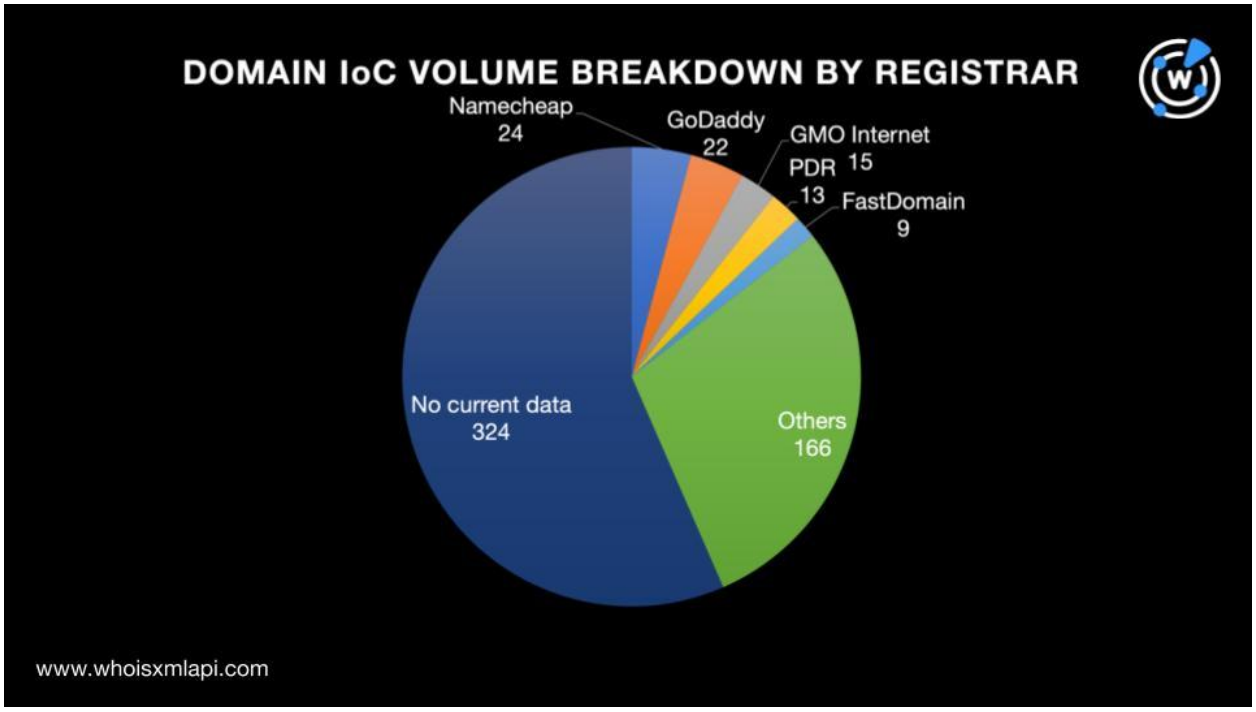
Threat researcher Dancho Danchev obtained 573 domains that belonged to several BreachForums members. The WhoisXML API research team expanded this list of indicators of compromise (IoCs) in an effort to obtain more information on their infrastructure. Our in-depth investigation led to the discovery of:

- 12 recently registered domains with the same registrant email addresses as some of the IoCs, one of which turned out to be malicious based on a bulk malware check
- 3,884 domains that shared the dedicated IP hosts of some of the domains identified as IoCs, 22 of which turned out to be malicious based on a bulk malware check
- 9,588 domains that contained strings akin to some of the IoCs, 30 of which turned out to be malicious based on a bulk malware check

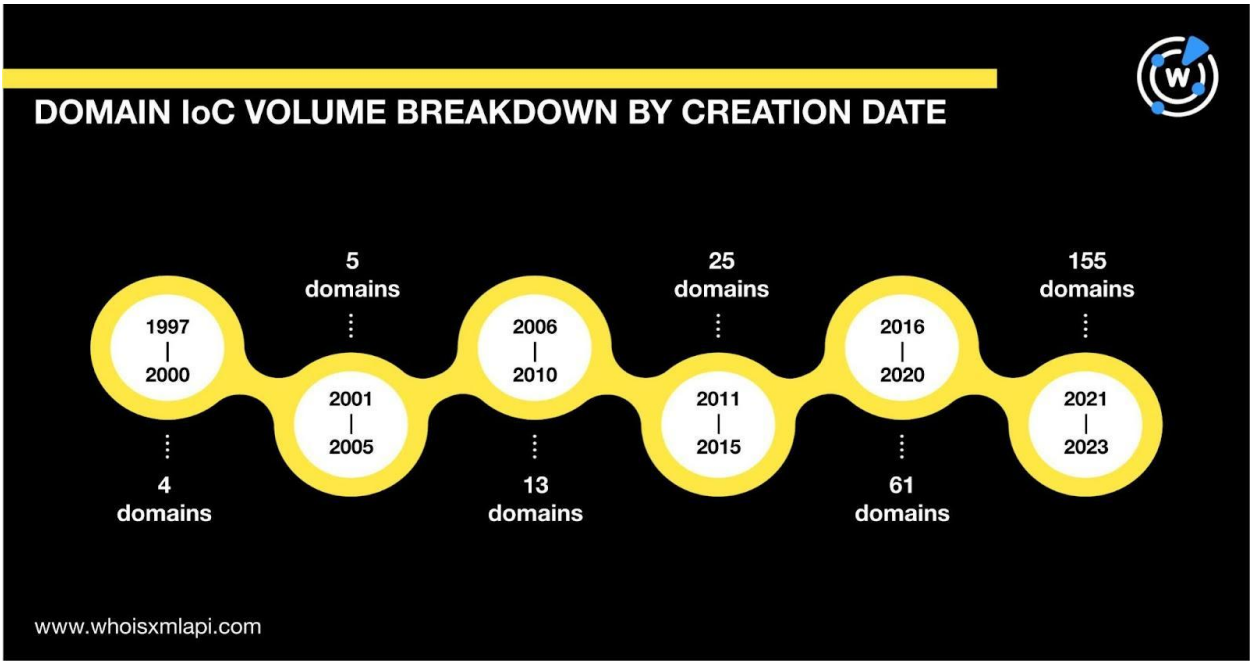
BreachForums Domains IoC Facts

The first step we took to investigate the BreachForums IoCs Danchev collated was perform a bulk WHOIS lookup that provided these results:

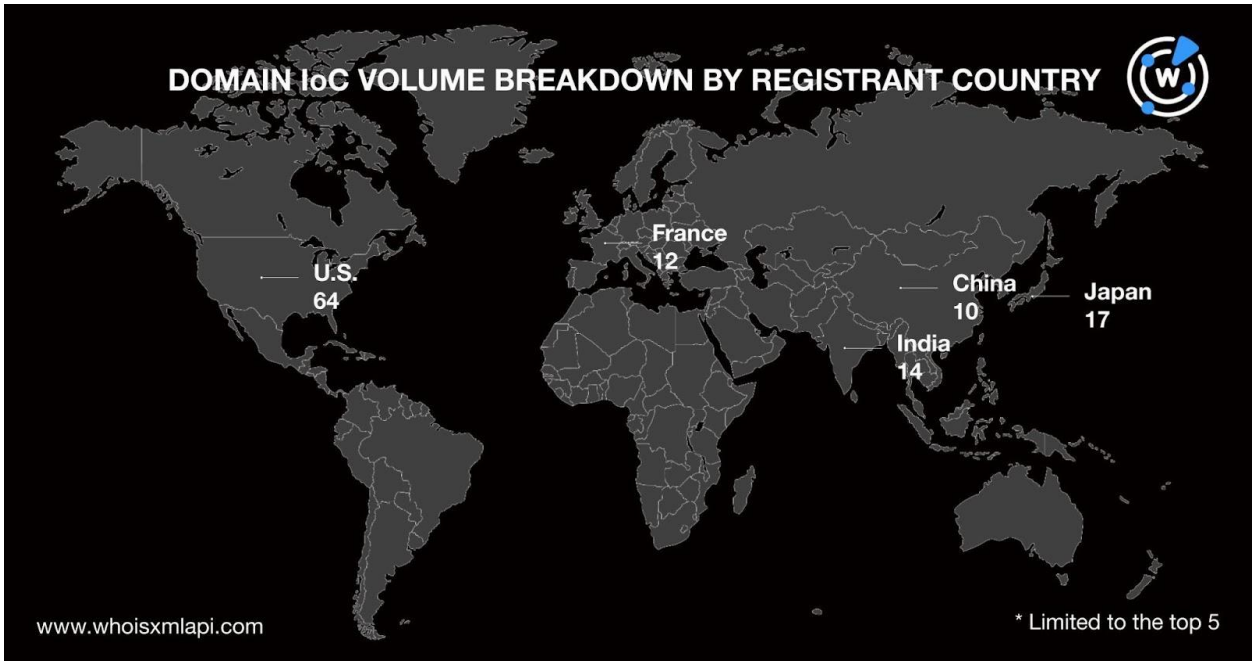
- While 324 of the domains identified as IoCs did not have retrievable public registrar data, the remaining 249 IoCs with current WHOIS records were distributed among 90 registrars led by Namecheap (24 domains), GoDaddy (22 domains), GMO Internet (15 domains), PDR (13 domains), and FastDomain (9 domains).



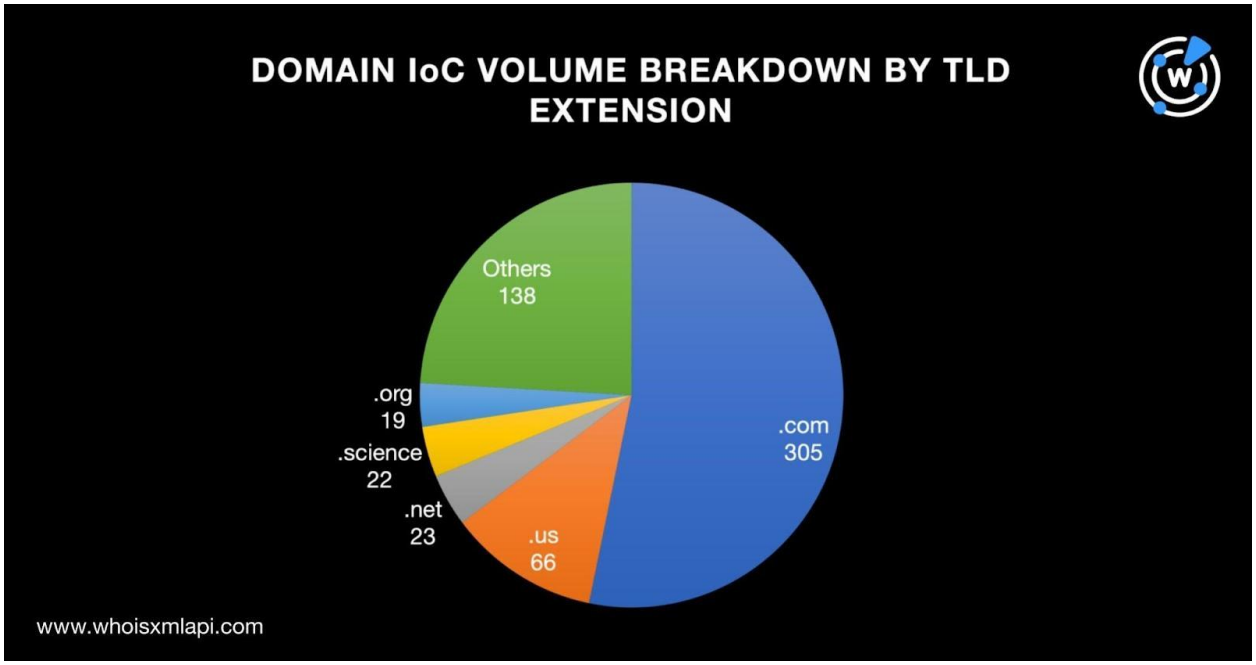
- While 310 of the domains did not have retrievable creation dates, the remaining 263 with current WHOIS records were created between 1997 and 2023, with most, 72 to be exact, created in 2022.



- While 358 IoCs did not have retrievable public registrant country data, the remaining 215 with current WHOIS records were spread across 32 countries led by the U.S. (64 domains), Japan (17 domains), India (14 domains), France (12 domains), and China (10 domains).



It is also interesting to note that the five most used top-level domain (TLD) extensions among the 573 domains identified as IoCs were .com (305 domains), .us (66 domains), .net (23 domains), .science (22 domains), and .org (19 domains). The remaining 138 domains sported 29 other TLD extensions.



BreachForums IoC List Expansion Findings

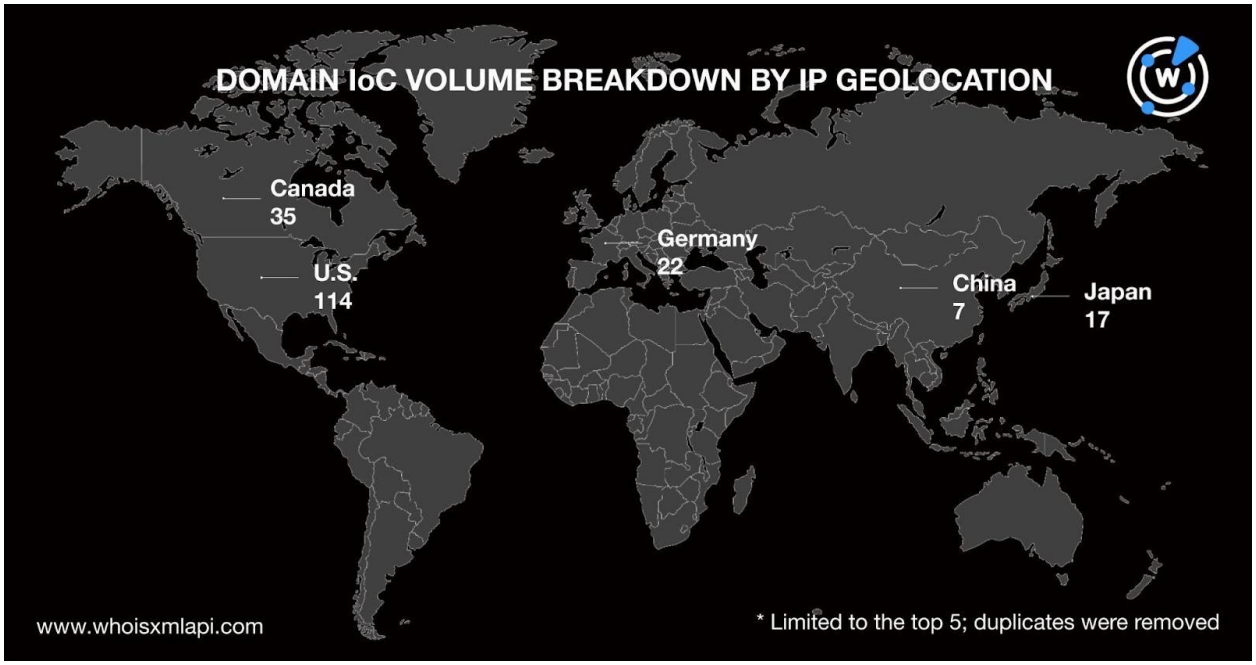
To know more about the BreachForums members' cybercriminal infrastructure, we subjected the 573 domains identified as IoCs to an expansion analysis.

A closer look at the IoCs with retrievable WHOIS records showed that several had public registrant email addresses (limited to those used to register 50 or fewer domains each), which were shared by 12 additional domains based on reverse WHOIS searches. One of the email-connected domains—carmainten[.]com—turned out to be malicious based on a bulk malware check.

Next, we conducted DNS lookups for the 573 domains identified as IoCs and found that they resolved to 253 IP addresses, one of which—137[.]184[.]161[.]21—turned out to be malicious based on malware checks.

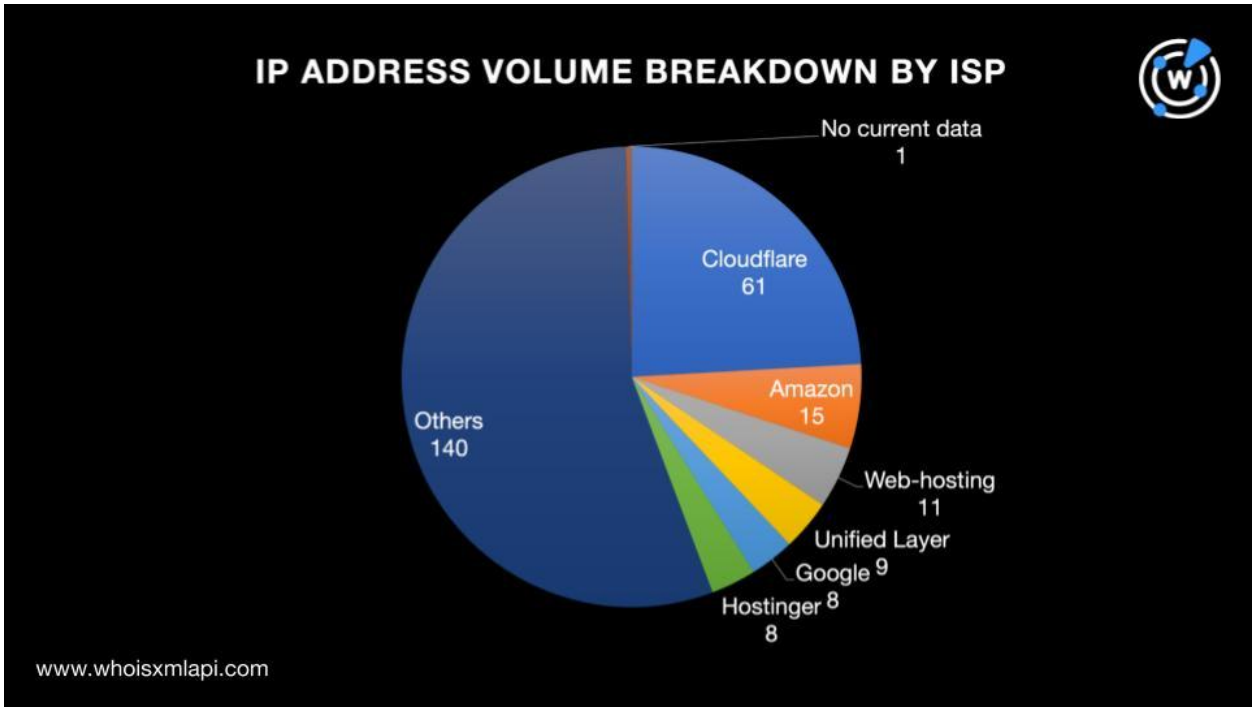
A bulk IP geolocation lookup for the 253 IP addresses showed that:

- While one did not have available geolocation country data, the remaining 252 were geolocated in 27 different countries led by the U.S. (114 IP addresses), Canada (35 IP addresses), Germany (22 IP addresses), Japan (17 IP addresses), and China (seven IP addresses).



Three of the top 5 IP geolocation and registrant countries—China, Japan, and the U.S.—coincided with one another.

- While one of the IP addresses did not have public Internet service provider (ISP) data, the remaining 252 were spread across 87 ISPs led by Cloudflare (61 IP addresses), Amazon (15 IP addresses), Web-hosting (11 IP addresses), Unified Layer (nine IP addresses), and Google and Hostinger (eight IP addresses each).



The lookups also allowed us to limit our study to the 60 dedicated IP addresses that played host to 3,884 domains based on reverse IP lookups. Twenty-two of the IP-connected domains turned out to be malicious based on a bulk malware check. All but two of the malicious domains remained accessible as of this writing.

Checks on Domains & Subdomains Discovery showed that 169 of the strings that appeared in the domains identified as IoCs were also present in 9,588 other domains. Thirty of them turned out to be malicious based on a bulk malware check.

Further scrutiny of the domains identified as IoCs allowed us to see that 23 of them contained six popular brand names—Amazon, Facebook, Gmail, iPhone, Tesla, and Yandex. It is interesting to note that these brand names also appeared in 127 IP- and string-connected domains. We identified some samples in the table below.

Famous Brand Name That Appeared a Text String	Domains Identified as IoCs	IP-Connected Domains	String-Connected Domains
Amazon	2 verification-amazon-fr[.]fr	2 amazonyrosa[.]in	5 amazon-firebiz[.]nom[.]za
Facebook	1		

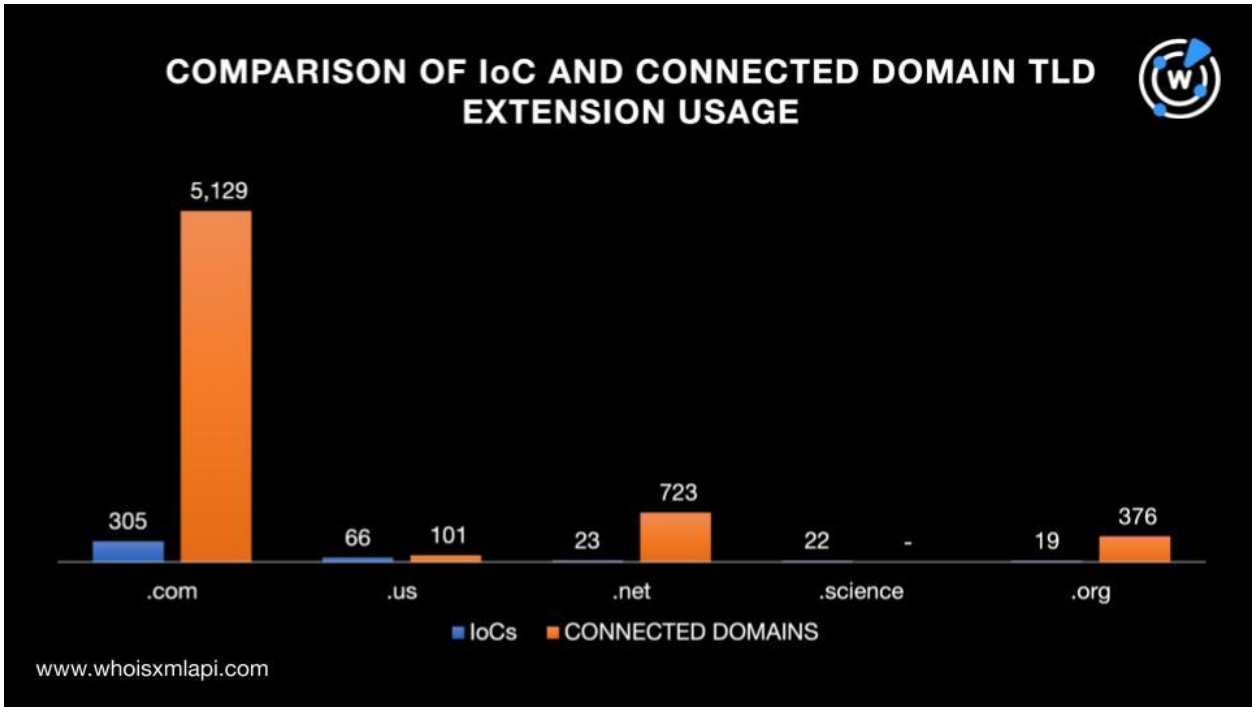
	facebooksexlist[.]com		
Gmail	17 f-gmail[.]com	4 account-my-mail-gmail[.]com	71 albagulizia-gmail[.]com
iPhone	1 findmyiphone-view[.]com	1 iphone-15.com[.]ua	1 iphonebiz[.]com[.]br
Tesla	1 teslamemorial[.]science		1 teslamemorial[.]biz[.]at
Yandex	1 yandex-toloka[.]ru[.]com		42 x0br[.]storage[.]yandexcloud[.]net

None of the 127 brand-containing domains we uncovered could be publicly attributed to any of the six companies cited above based on their WHOIS records. And based on screenshot lookups, 101 of them remained accessible as of this writing even though many led to error or index pages.

Finally, we sought to find out how many of the 13,484 domains potentially connected to the threat by email address, IP address, or string usage shared the five TLD extensions the threat actors most abused based on our further scrutiny of the IoCs earlier. We found that:

- A total of 6,329 connected domains shared four of the top 5 TLD extensions used by the domains identified as IoCs.
- A huge majority of the connected domains, 5,129 to be exact, sported the .com TLD extension.
- Only 101 of the connected domains used the .us TLD extension.
- A total of 723 connected domains utilized the .net TLD extension.
- None of the connected domains sported the .science TLD extension.
- Only 376 of the connected domains used the .org TLD extension.

Take a look at the comparison between the TLD extension usage among the domains identified as IoCs and connected domains below.



—

Our analysis and expansion of the list of BreachForums domains allowed us to uncover 13,484 potentially connected web properties, 53 of which turned out to be malicious based on malware checks. We also identified commonalities between the domains identified as IoCs and the connected domains, such as that .com seemed to be the most abused TLD extension.

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

BreachForums IoCs

- secured-logins[.]online
- microsoftupdale[.]com
- amzn-offer[.]com[.]ng
- paypalcustomerservices[.]com

- biunj[.]top
- wzmxec[.]cn
- semainedelapopphilosophie[.]fr
- haileybeauty[.]fr
- kellyblake[.]us
- securitylab[.]hk
- texasaction[.]us
- kazuko[.]us
- purgestresser[.]xyz
- bagipokemon[.]com
- moneymatterswitheric[.]com
- idriss[.]fr
- bluesteelcraft[.]net
- phohangcu[.]com
- kookwinkels[.]net
- mediumsonja[.]net
- ukmshops[.]com
- makebelief[.]science
- depressioncure[.]science
- aisukoneko[.]net
- 82flex[.]club
- ssri[.]science
- snri[.]science
- gadjahmada[.]org
- keralacultural[.]science
- internetmarketergroup[.]com
- sampitroda[.]science
- apjabdulkalam[.]science
- floatingmind[.]science
- neurotransmission[.]science
- sunitawilliams[.]science
- teslamemorial[.]science
- moodregulation[.]science
- antipsychotic[.]science
- originofearth[.]science
- wardenclyffetower[.]science
- antidepressant[.]science
- chuvabravasolfeliz[.]com
- vasthu[.]science
- resumosparaprovas[.]com[.]br
- ultra1337s[.]pro
- indiancultural[.]science
- resuminhosparaprovas[.]com
- benchfee[.]net
- homijbhabha[.]science
- blunder[.]science
- paradisusloscabos[.]com
- meums[.]edu[.]ly
- serinformatico[.]com
- gs-france[.]fr
- modaparatodo[.]com[.]br
- proshoponline[.]com[.]br
- sr-ken1[.]com
- iltdamktdigital[.]com[.]br
- meums[.]ly
- sportday[.]com[.]br
- chauffeur24[.]ma
- shoukai-system[.]net
- fuertedestination[.]com
- bykvu[.]com
- f-gmail[.]com
- marsoul-tech[.]ly
- alanosempre[.]com
- esercizi-e-rimedi[.]com
- whdhwfawla[.]com
- vectorofdream[.]club
- p-at-g[.]info
- recruitmentsourcing[.]us
- koisit[.]com
- your-candle[.]com
- woshilaosijikuaishangche[.]xyz
- casadipasta[.]fr
- connectionloop[.]jp
- osamathabet[.]com
- capl[.]com[.]sg
- puccinis[.]us
- allinfotoday[.]us
- btler[.]kz
- aventerpriseindia[.]com
- smart99sendai[.]com

- mgo777[.]us
- ced-guitare34[.]fr
- suntech[.]com[.]pa
- merhawitravels[.]com
- weknownothingpodcast[.]com
- purehempsoap[.]ca
- organia[.]com[.]ua
- lnwgame[.]com
- vikingventures[.]us
- vygoranie[.]su
- my-mail-gmail[.]com
- login-mail-gmail[.]com
- fundaciondeespecialistas[.]com
- market365[.]com[.]ua
- lindsayfashions[.]com
- jornaldosbairrosonline[.]com[.]br
- petirketarketir[.]vip
- siam1[.]net
- hi9765[.]com
- fathersclub[.]us
- account-my-mail-gmail[.]com
- myaccount-my-mail-gmail[.]com
- goodgirls101[.]com
- freender[.]us
- myaccounts-mail-gmail[.]com
- hot-auto[.]com[.]ua
- ygu-1[.]net
- xn--jn2a86s[.]tw
- kvadrat-m[.]com
- curriculo2022[.]com
- vishakafoundation[.]com
- app12123[.]com
- donnaree[.]net
- e-standart[.]com
- neposidko[.]com
- mgo55[.]us
- bidiknews24[.]com
- mosclub[.]su
- iniq[.]us
- mfenno[.]com
- 2t[.]gs
- deesign[.]co[.]kr
- mail-gmail[.]com
- iorganicpetshop[.]com
- iorganichouse[.]com
- humresource[.]com
- ko-bo-440[.]com
- hayao0819[.]com
- hog-lab[.]com
- hi12123[.]com
- hshealt[.]com
- myaccounts-my-mail-gmail[.]com
- findabitch[.]info
- my-account-mail-gmail[.]com
- gosspcrepair[.]com
- my-accounts-mail-gmail[.]com
- lizihost[.]com
- copticsite[.]com
- petenjess[.]com
- shinobu[.]kr
- shinbou[.]co[.]kr
- hamptoonu[.]com
- cryptbits[.]us
- cryptoskope[.]us
- blockhodl[.]us
- cryptomonist[.]us
- cityofcrypto[.]us
- chainofthings[.]us
- hesapcibaba[.]com
- emeraldenzosculptures[.]com
- gh-herbals[.]us
- hallareview[.]com
- solnyshko-2022[.]kz
- rce[.]net[.]cn
- arol[.]us
- consejoscomunalesparaladefensaintegral[.]xyz
- noticiasnaweb[.]net
- quick2pey[.]us
- sribiosys[.]com

- proxmoxve[.]cn
- whmcsservices[.]cn
- virtualizor[.]cn
- goodealhosting[.]cn
- fetomagduruaileler[.]net
- 28subatvefetomagduruaileler[.]net
- zjmftheme[.]cn
- shieyingxiong[.]cn
- whmcshelp[.]com
- habersilvangazetesi[.]com
- dusunce360[.]com
- hurtakipci[.]com
- urfahurhaber[.]com
- dieq41[.]com
- arminarekaperdanahalim[.]com
- cains[.]party
- topsalestoday[.]us
- stuartpowell[.]us
- animu[.]su
- cleanconnect[.]us
- truthtrend[.]us
- milina[.]jp
- pchd[.]one
- ricambiauto[.]us
- rachelmorton[.]us
- shopauro[.]us
- sppt[.]us
- effectivtech[.]us
- careerchanger[.]us
- jleon-automation[.]us
- johnlwaite[.]com
- lakeshore[.]tw
- no-no-no-no[.]com
- alisonjones[.]us
- segner[.]us
- charliem[.]us
- valuation[.]co[.]il
- no-no[.]com
- trumpersonly[.]us
- posten-no-no[.]com
- totallyavir[.]us
- kathypizzino[.]us
- wildburger[.]us
- cfodesk[.]co[.]il
- whisky-a-no-no[.]com
- trevorhill[.]us
- charliemoore[.]us
- no-no-no[.]com
- michaelstamerfarms[.]com
- voidedparadox[.]com
- my-no-no[.]com
- zeromatter[.]us
- cuntmode[.]com
- figyak[.]com
- oht[.]com[.]tw
- herbalhongkong[.]com
- mo-no-no[.]com
- jumphost[.]kz
- nana-no-no[.]com
- liveearth-no-no[.]com
- candronepilotcoop[.]com
- celebrity-no-no[.]com
- escobarproductions[.]us
- yasu-no-no[.]com
- vjdiamonds[.]co[.]il
- burkardt[.]us
- buy-no-no[.]com
- makabaka[.]us
- me-no-no[.]com
- pnrsyntax[.]us
- big-no-no[.]com
- visentagroup[.]com
- aki-no-no[.]com
- carte-vital-notification[.]fr
- epichi[.]us
- vpnsvr[.]top
- verification-amazon-fr[.]fr
- laurencecouture[.]fr
- it-serve[.]pro
- thefeelgoodhood[.]com

- bookrichandsassy[.]com
- pio-no-no[.]com
- apt4[.]kr
- minjs[.]us
- demandredesign[.]org
- riches-elenas[.]kz
- test-ryhall-dns-is-us-test-gmail[.]com
- try-no-no[.]com
- eliteautoloans[.]ca
- akixi-test-gmail[.]com
- get-no-no[.]com
- fatemzassl[.]com[.]ng
- aryamatbaa[.]com
- official-no-no[.]com
- thizastore[.]com[.]br
- everydayweplay365new[.]com
- curiousq[.]info
- hgarbaglobalventures[.]com[.]ng
- dafdfeafeae[.]com
- facebooksexlist[.]com
- attavitacons[.]com
- test-bh-staging-domain28082021025944[.]com
- politics-is-a[.]science
- alexcohen[.]us
- esv[.]jp
- wagnitzsoftware[.]com
- cdcysj[.]cn
- demonslayerswords[.]net
- wolftecno[.]com
- epic-hi[.]us
- outletku[.]com
- serialmail[.]net
- oh-no-no[.]com
- cysj1[.]cn
- skjdnsn[.]com
- sallybestor[.]com
- hotelfortkolesnik[.]com
- birdy[.]com[.]tw
- ebiz[.]co[.]il
- youngfaith[.]us
- vitejambe[.]com
- kittybox[.]us
- artech-a[.]fr
- jrspipesandtubes[.]com
- herbsandnature[.]us
- tlftest[.]us
- laboratorioedn[.]com
- subprimary[.]com
- cyrusmedia[.]ca
- trogdor-test-teststs-devee[.]com
- leenuts[.]com
- gmo-test-2022-05-05-ishitoya01[.]com
- dd9[.]co[.]kr
- smsvg[.]com
- s-proj[.]co[.]il
- spartanguild[.]com
- becysj[.]cn
- test-bh-staging-domain06092021131217[.]com
- tjcysj[.]cn
- thanushcreations[.]com
- cartevitale-am[.]fr
- piephomedia[.]com
- theinquiryhub[.]com
- smsnh[.]com
- yuanayu[.]com
- plusswagath[.]com
- asukaindonesia[.]com
- smsrb[.]com
- maacademia[.]com
- topfactsglobal[.]com
- prakrie[.]com
- i-socialapp[.]com
- luzxd[.]us
- findmyiphone-view[.]com
- ipklll[.]us
- ip-pbx[.]su

- terminodador[.]com
- test1122[.]net
- manurnu[.]com
- testingdomainwsuite12345[.]net
- jorcustoms[.]com
- testingdomainwsuite123456[.]net
- 0br[.]us
- yandex-toloka[.]ru[.]com
- dollpls[.]com
- weeblycombo2[.]com
- whcysj[.]cn
- weeblycombotesting1[.]com
- programadorweb[.]net
- aaravidevelopers[.]com
- 44518[.]cn
- inviz[.]host
- kz123[.]cn
- collectifpolar[.]fr
- naromedia[.]space
- secandosemparar[.]com
- steemdice[.]online
- uvlfastmarket[.]com
- trackblogexperthealth[.]space
- changyouworld[.]cn
- weeblycombo[.]com
- lovepets[.]fr
- gombong[.]asia
- lei-nuo[.]com[.]cn
- runhr[.]us
- kaya-bunga[.]com
- dimensionengiservices[.]com
- thomashcliu[.]com
- ttglobaladvisory[.]net
- 0xe[.]us
- underarmourstore[.]us
- friendsland[.]pp[.]ua
- eoczy[.]host
- qualiteletrica[.]com[.]br
- heskes[.]info
- quemseduzconquista[.]com
- nitix[.]biz
- starhelectricalservicesllc[.]com
- 2xlipat[.]com
- mugyuphotoworks[.]com
- exroot[.]us
- promicom[.]ma
- ibracket[.]net
- compteabonnement[.]fr
- gotowka-doreki[.]info
- pamyu-pamyu[.]com
- ismarcoscastro[.]com
- a-gmail[.]com
- doremi-hochouki[.]com
- hahapetshop[.]com
- joshuahatten[.]com
- reza-najafi[.]com
- lloyds-area[.]com
- fibvo[.]com
- codenific[.]com
- linhtinhcenter[.]com
- zo1984[.]com
- lifevantagethai-nrf2[.]com
- greenenershop[.]com
- gaytravelcrowd[.]com
- aythotellock[.]com
- doooectb[.]com
- gratiasmarthome[.]com
- myrenttoownhomes[.]us
- voxchronicle[.]com
- cloudtest[.]asia
- teedin789[.]org
- car789[.]org
- alarmmoney[.]info
- cctvnon[.]com
- ouvoleravecmondrone[.]com
- vtechwriter[.]com
- greenmage321[.]com
- avtoremont36[.]xyz
- carav[.]us
- flowerwseb[.]info

- cjford[.]org
- ouvoleravecmondrone[.]net
- suns-vip[.]com
- mindyshousecleaners[.]com
- gaytravelcrowd[.]biz
- healthlantern[.]us
- greens333[.]com
- vacation-crowd[.]com
- blockpays[.]info
- rem971verslesucces[.]com
- nsr-sys[.]com
- aminpour[.]info
- ba2b[.]xyz
- nwtgck[.]xyz
- classhelper[.]us
- dustbinservices[.]com
- checkiclouds[.]info
- lclsecuret[.]com
- toretto[.]host
- antoinetbt[.]host
- ecomyparty[.]com
- vil-diesel[.]host
- ontime-a[.]com
- canlammotteam[.]host
- dominic-toretto[.]host
- semailaanhem[.]host
- badromance[.]host
- cd-storage-reviews[.]com
- antoinegriezmann[.]host
- seeyouagain[.]host
- mrtbt[.]host
- line-dn[.]com
- eklink[.]org
- emlakhaberleri[.]org
- eklink[.]info
- legendturk[.]biz
- 64bitcongnghe[.]com
- pocket0077[.]com
- dallaporte[.]com
- etchmall[.]com
- accounts-my-mail-gmail[.]com
- account-mail-gmail[.]com
- accounts-mail-gmail[.]com
- art-photo-story[.]com
- azarter[.]com
- youractiontoys[.]com
- sil21[.]com
- indicatorchoice[.]com
- myaccount-mail-gmail[.]com
- teamkill[.]pro
- mdhanastha[.]com
- smpplugin[.]com
- smp-plugin[.]com
- todaymagazine[.]xyz
- thecouponparty[.]com
- todayradio[.]xyz
- serva4ok[.]pro
- forteam[.]pro
- facebuilder[.]xyz
- irandirectory[.]xyz
- mixandmastering[.]xyz
- nameforbaby[.]xyz
- justpayforshipping[.]biz
- justpayforshipping[.]org
- justpayforshipping[.]info
- lambdaf[.]info
- herdiesel-santoso[.]com
- keywordriches[.]org
- energybodyart[.]com
- floresemangola[.]com
- sonyatour[.]com
- doktorhatasi[.]biz
- probono123[.]org
- personalitynetwork[.]org
- gold4money[.]us
- odt[.]moscow
- okget[.]xyz
- mixedfire[.]com
- batikidalestari[.]com
- frugalandresponsibleliving[.]com

- makrandownload[.]com
- yfilatov[.]xyz
- artbodyart[.]com
- meme-generator[.]info
- delhitransport[.]info
- trisnoidamanbatik[.]com
- modadhanasta[.]com
- okemoviezone[.]com
- gowanusindustrial[.]org
- ydafmc[.]com
- books-mania[.]com
- buettner[.]science
- vdeserve[.]com
- k-u-n-s-t-s-t-o-f-f[.]com
- f-f[.]com
- f-l-u-f-f[.]com
- a-f-f[.]com
- t-a-f-f[.]com
- b-f-f[.]com
- k-f-f[.]com
- f-f-f[.]com
- m-f-f[.]com
- g-f-f[.]com
- p-u-f-f[.]com
- s-t-a-f-f[.]com
- okrok[.]info
- d-i-f-f[.]com
- roukio[.]info
- t-f-f[.]com
- teotio[.]info
- s-u-n-o-f-f[.]com
- s-t-i-f-f[.]com
- okrok[.]org
- w-f-f[.]com
- teotio[.]org
- h-f-f[.]com
- pokere[.]org
- v-f-f[.]com
- roukio[.]org
- f-a-c-e-o-f-f[.]com
- s-u-f-f[.]com
- take-o-f-f[.]com
- u-s-f-f[.]com
- qeou[.]online
- u-f-f[.]com
- karatsu-f-f[.]com
- j-f-f[.]com
- l-f-f[.]com
- o-f-f[.]com
- f--f[.]com
- e-f-f[.]com
- gardener-f-f[.]com
- i-f-f[.]com
- p-j-f-f[.]com
- y-f-f[.]com
- s-f-f[.]com
- c-f-f[.]com
- boulangerie-dupont-f-f[.]com
- s-t-f-f[.]com
- n-u-f-f[.]com
- ca-f-f[.]com
- sts-rci-rogers[.]ca
- p-f-f[.]com
- scholarlysources[.]com
- f-f-f-f[.]com
- globalrealez[.]com
- df-we-4234-f-we-fw-4234-f-we-f-f[.]com
- iconarise[.]com
- hamad-f-f[.]com
- toplifedailylive[.]com
- n-f-f[.]com
- s-o-f-f[.]com
- p-i-s-s-o-f-f[.]com
- c-u-f-f[.]com
- d-f-f[.]com
- z-f-f[.]com
- r-i-f-f[.]com
- r-f-f[.]com
- innovationoffice[.]org

- mindsxchange[.]com
- marketresearchcolloquium[.]com
- danielles-f-f-f[.]com
- x-f-f[.]com
- q-f-f[.]com
- platformxchange[.]com
- d-i-l-l-i-g-a-f-f[.]com
- c-i-f-f[.]com
- k-y-f-f[.]com
- kairosteknoloji[.]download
- enesaldemir[.]net
- tenadesign[.]net
- shyfzorg[.]com
- disdikbud-papua[.]org
- al-azharaslichmughny[.]org

Sample Email-Connected Domains

- altamahasboykinspaniels[.]com
- azarter[.]com
- carmainten[.]com
- curatareauto[.]com
- dellaporte[.]com
- evergreencommunties[.]com
- mezha[.]net

Malicious Email-Connected Domain

- carmainten[.]com

Sample IP Resolutions

- 185[.]230[.]63[.]171
- 185[.]230[.]63[.]186
- 185[.]230[.]63[.]107
- 15[.]197[.]148[.]33
- 3[.]33[.]130[.]190
- 2001:19f0:5:13e0:5400:4ff:fe12:890e
- 144[.]202[.]4[.]58
- 75[.]2[.]37[.]224
- 162[.]241[.]2[.]55
- 2001:12ff:0:2::95
- 200[.]160[.]2[.]95
- 35[.]186[.]223[.]180
- 168[.]119[.]8[.]237
- 66[.]228[.]61[.]234
- 2001:8d8:100f:f000::2ff
- 217[.]160[.]0[.]30
- 23[.]227[.]38[.]65
- 135[.]181[.]142[.]43
- 2a02:4780:13:1012:0:996:2a53:10
- 45[.]14[.]89[.]164
- 174[.]142[.]95[.]84
- 133[.]242[.]13[.]180
- 2606:4700:20::ac43:4a03
- 2606:4700:20::681a:9e8
- 2606:4700:20::681a:8e8
- 104[.]26[.]9[.]232
- 104[.]26[.]8[.]232
- 172[.]67[.]74[.]3
- 116[.]202[.]80[.]213
- 192[.]64[.]119[.]202
- 75[.]2[.]85[.]42
- 99[.]83[.]196[.]71
- 109[.]234[.]164[.]153
- 118[.]27[.]125[.]218
- 2a02:4780:8:1224:0:302f:dd28:3
- 185[.]224[.]137[.]105
- 162[.]241[.]216[.]110

- 2606:4700:3035::6815:3729
- 2606:4700:3035::ac43:9082
- 104[.]21[.]55[.]41
- 172[.]67[.]144[.]130
- 195[.]210[.]46[.]36
- 34[.]66[.]135[.]39
- 157[.]7[.]107[.]85
- 2a01:238:20a:202:1148::
- 81[.]169[.]145[.]148
- 66[.]235[.]200[.]119
- 185[.]209[.]230[.]214
- 75[.]126[.]104[.]249
- 62[.]173[.]149[.]122

Malicious IP Resolution

- 137[.]184[.]161[.]21

Sample IP-Connected Domains

- 01daigorou[.]com
- 01kotarou[.]com
- 024hy[.]com
- 02kojirou[.]com
- 03kosaburou[.]com
- 04koshirou[.]com
- 05kogorou[.]com
- 06korokurou[.]com
- 07koshichirou[.]com
- 08kohachirou[.]com
- 09kokurou[.]com
- 100yearssong[.]com
- 1020riku[.]com
- 10bestseo[.]com
- 10kojyuurou[.]com
- 123clearmyticket[.]com
- 18-sumy[.]com[.]ua
- 18coupons[.]com
- 1kissasian[.]co
- 1minworkouts[.]com
- 1stplaceautorepair[.]com
- 2022web3[.]net
- 24pt[.]jp
- 28wai[.]com
- 2t[.]gs
- 31design[.]com[.]hk
- 34riki[.]blog
- 35261646[.]com
- 359travel[.]com
- 365travel[.]news
- 3m-tech[.]co[.]jp
- 40man0718[.]com
- 432printing[.]com
- 4livingc[.]com
- 5-si[.]co[.]jp
- 512byte[.]ua
- 51885188[.]com
- 52221368[.]com
- 57promenade[.]id
- 5jigen[.]jp
- 5toolgym-lp[.]com
- 63862211[.]com
- 78shopping[.]com
- 88-888[.]com
- 884mado[.]com
- 8friends[.]org
- 91311548[.]com
- 933[.]co[.]kr
- 9kft[.]com
- a-i-solution[.]com
- a-room[.]work
- a1astrology[.]com
- aaa-web[.]design
- aabbaab[.]cram-shop[.]com

- aaitravel[.]com
- aamazingshopp[.]com
- abattisconsulting[.]com
- abcdwelfarefoundation[.]org
- abcsoft[.]dev
- abfingredients[.]com
- abminfocity[.]in
- abs-manaus[.]com[.]br
- absolutair[.]in
- abuanas[.]om
- aburgslife[.]com
- ac16outlook[.]com
- accinternational[.]net
- account-my-mail-gmail[.]com
- acecareonsite[.]com
- acerecordsng[.]com
- acervocuracaense[.]com[.]br
- actyveotc[.]com
- acuteproductions[.]com
- ad-max[.]jp
- adidevproperties[.]com
- adinata[.]com
- adiyamananadolu[.]com
- adl[.]sn
- admsystemsllc[.]com
- adrenalin[.]dance
- advancedmarketinginnovations[.]com
- advancemarketinginnovations[.]com
- advmarques[.]com
- advocaciasantos[.]net[.]br
- advocateshanthala[.]com
- advogadoscordeiro[.]com
- aeccsl[.]com
- aeedea[.]com
- aees-gym[.]com
- aegblog[.]com
- aexongraphics[.]com
- afikim-38[.]com
- afklsalestlv[.]co[.]il
- afrikanmum[.]com
- afromaker[.]com
- afxanimation[.]in
- agenciadstecnologia[.]com[.]br
- agenciastart[.]com[.]br
- agentecredenciadotim[.]com[.]br
- agigear[.]com

Sample Malicious IP-Connected Domains

- 78shopping[.]com
- 88-888[.]com
- a1astrology[.]com
- bagelsa[.]com
- bitstechno[.]com
- bomacargo[.]id
- buildwisecontractor[.]com
- chanchal[.]co
- christechsupport[.]net
- cialisfw[.]com
- lileweb[.]cram-shop[.]com
- login-mail-gmail[.]com

Sample String-Connected Domains

- 000br[.]vip
- 00br[.]bashkiria[.]su
- 00br[.]c[.]la
- 00br[.]cleverapps[.]io
- 00br[.]co
- 00br[.]co[.]com
- 00br[.]daplie[.]me
- 00br[.]filegear-de[.]me
- 00br[.]gotpantheon[.]com
- 00br[.]gr[.]com

- 00br[.]hepforge[.]org
- 00br[.]jp[.]net
- 00br[.]ocelot[.]mythic-beasts[.]com
- 00br[.]operaunite[.]com
- 00br[.]paas[.]massivegrid[.]com
- 00br[.]sphinx[.]mythic-beasts[.]com
- 00br[.]storage[.]yandexcloud[.]net
- 00br[.]thingdustdata[.]com
- 00br[.]vip
- 00br[.]website[.]yandexcloud[.]net
- 00br[.]webspace[.]rocks
- 00xe[.]bplaced[.]de
- 00xe[.]caa[.]li
- 00xe[.]codespot[.]com
- 00xe[.]df[.]gov[.]br
- 00xe[.]edu[.]ws
- 00xe[.]gb[.]net
- 00xe[.]hepforge[.]org
- 00xe[.]nid[.]io
- 00xe[.]nl
- 00xe[.]platter-app[.]com
- 00xe[.]soc[.]srcf[.]net
- 00xe[.]static[.]observableusercontent[.]com
- 00xe[.]us[.]org
- 012oht[.]cyou
- 0167ck2ozfzoht[.]com
- 035oht[.]cyou
- 07shinobu[.]wixsite[.]com
- 0800br[.]tk
- 0br[.]12hp[.]ch
- 0br[.]1kapp[.]com
- 0br[.]2ix[.]de
- 0br[.]adobeaemcloud[.]com
- 0br[.]appengine[.]flow[.]ch
- 0br[.]barsy[.]net
- 0br[.]barsyonline[.]com
- 0br[.]blogspot[.]com[.]ng
- 0br[.]browsersafetymark[.]io
- 0br[.]cloudns[.]us
- 0br[.]lat
- 0br[.]mil[.]ph
- 0br[.]n4t[.]co
- 0br[.]nid[.]io
- 0br[.]us-3[.]evennode[.]com
- 0cjh0br[.]cn
- 0d0br[.]xn--fiqz9s
- 0e5at0br[.]shop
- 0oht[.]adobeaemcloud[.]net
- 0oht[.]blogspot[.]ro
- 0oht[.]de[.]cool
- 0oht[.]definima[.]net
- 0oht[.]fastly-terrarium[.]com
- 0oht[.]filegear-de[.]me
- 0oht[.]hb[.]cldmail[.]ru
- 0oht[.]loginline[.]dev
- 0oht[.]myforum[.]community
- 0oht[.]nid[.]io
- 0oht[.]readthedocs[.]io
- 0oht[.]sochi[.]su
- 0oht[.]us-1[.]evennode[.]com
- 0oht[.]us[.]platform[.]sh
- 0oht[.]zapto[.]xyz
- 0q3n0xe[.]cn
- 0tnv0br[.]com
- 0xe[.]adobeaemcloud[.]net
- 0xe[.]appengine[.]flow[.]ch
- 0xe[.]arab
- 0xe[.]blogspot[.]co[.]id
- 0xe[.]blogspot[.]rs
- 0xe[.]cust[.]dev[.]thingdust[.]io
- 0xe[.]cust[.]prod[.]thingdust[.]io
- 0xe[.]daplie[.]me
- 0xe[.]edu[.]ws
- 0xe[.]grozny[.]ru
- 0xe[.]hepforge[.]org
- 0xe[.]lat
- 0xe[.]loginline[.]dev
- 0xe[.]lol
- 0xe[.]london[.]cloudapps[.]digital

- 0xe[.]myhome-server[.]de
- 0xe[.]ocelot[.]mythic-beasts[.]com
- 0xe[.]shop
- 0xe[.]space
- 0xe[.]telebit[.]app
- 0xe[.]user[.]srcf[.]net
- 100br[.]blogspot[.]sn
- 100br[.]bloxcms[.]com
- 100br[.]br[.]com
- 100br[.]caa[.]li
- 100br[.]codespot[.]com

Sample Malicious String-Connected Domains

- 00br[.]co
- 700br[.]com
- 1020br[.]com
- yri0br[.]cfd
- www00br[.]com
- f0xe[.]armenia[.]su
- liamsonvaluation[.]autos
- fboht[.]top
- aucoht[.]buzz
- cashtaskoht[.]buzz
- basesuntech[.]ru
- nudebiz[.]xyz
- aguebiz[.]site
- renamebiz[.]com
- provebiz[.]online
- youprivilegebiz[.]life