# BreachForumsドメインのDNS徹底調査

## 目次



## 要旨

米連邦捜査局（FBI）が2023年3月21日、英語圏のブラックハットハッカーのためのフォーラム「BreachForums」を閉鎖しました。しかし最近になって、初代管理者のBaphometとShinyHuntersというハッキンググループによる新しい運営陣のもとでBreachForumsが再開された、との報道がありました。

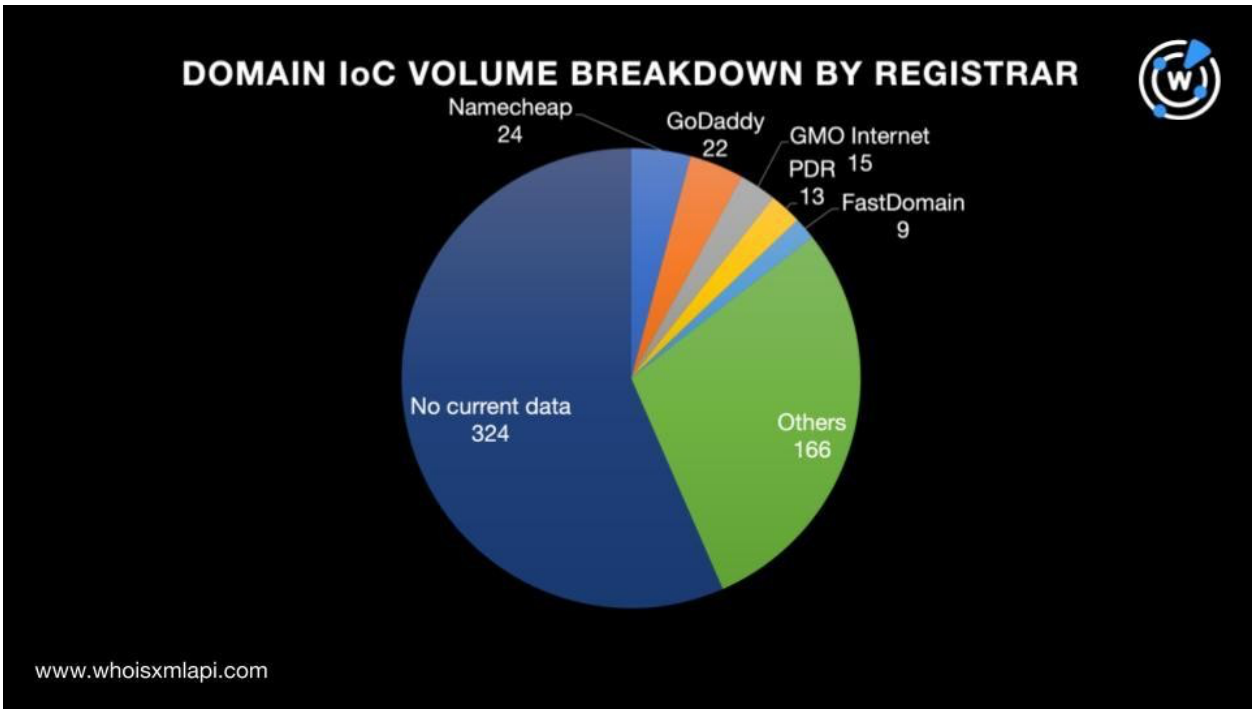
WhoisXML APIの脅威リサーチャーであるDancho Danchevはこのほど、複数のBreachForumsメンバーが所有する573個のドメイン名を見つけました。そこで、WhoisXML APIの研究チームがそのセキュリティ侵害インジケーター（IoC）リストを足がかりに、DNSインテリジェンスを駆使してBreachForumsに関するより多くの情報を探しました。この徹底的な調査により、以下が検出されました。

- IoCと同じ登録者のメールアドレスを持つ、最近登録された12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1個は悪意あるドメイン名と確認
- IoCと特定されたドメイン名の専用IPホストを共有していた3,884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22個は悪意あるドメイン名と確認
- IoCに類似した文字列を含む9,588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30個は悪意あるドメイン名と確認

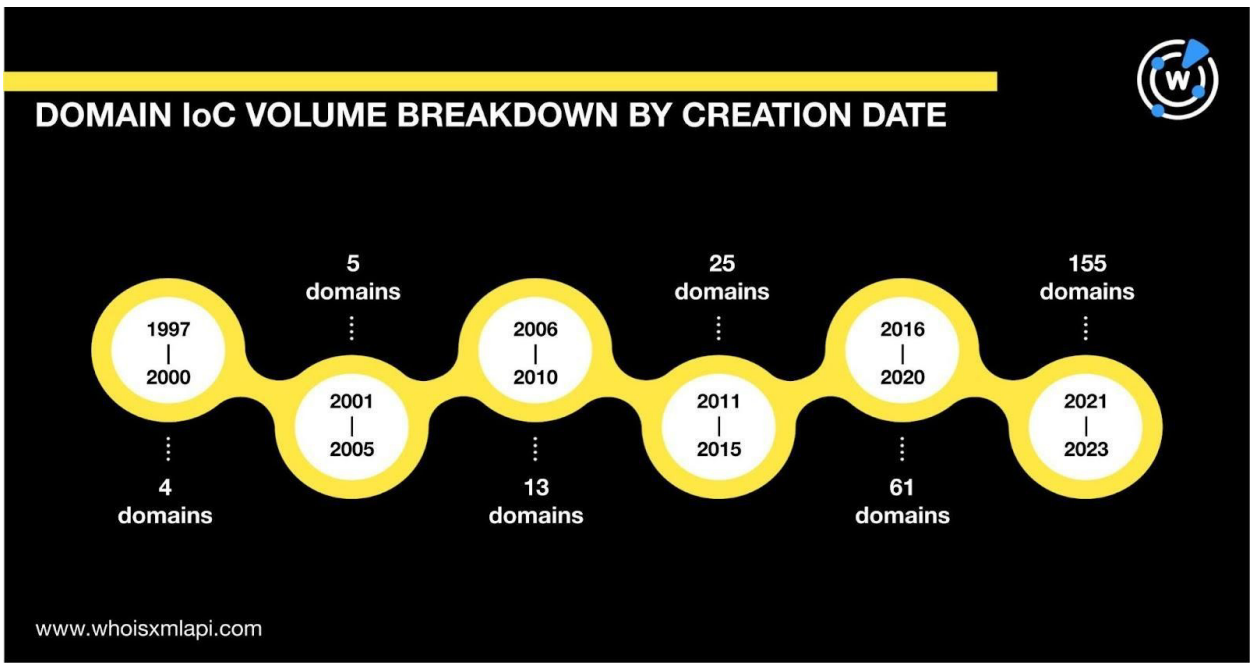
### BreachForumsのドメインIoCの実態

Danchevが収集したBreachForumsのIoCを精査するにあたり、研究チームが最初に行ったのはBulk WHOIS LookupによるIoCの検索でした。

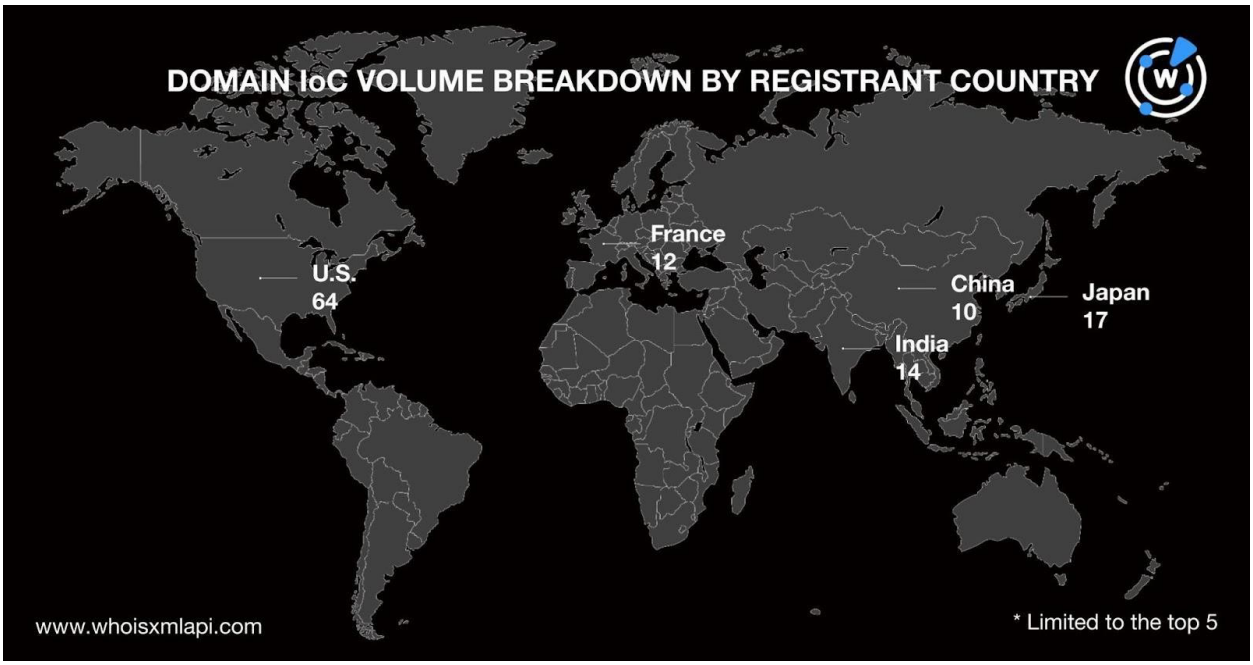
- DanchevがIoCと特定したドメイン名（以下「ドメインIoC」）のうち、324個についてはレジストラの情報がWHOISで公開されていませんでした。WHOISレコードが存在した残りの249個のIoCは、Namecheap（24個）、GoDaddy（22個）、GMOインターネット（15個）、PDR（13個）、FastDomain（9個）を筆頭に90のレジストラに分散して管理されていました。



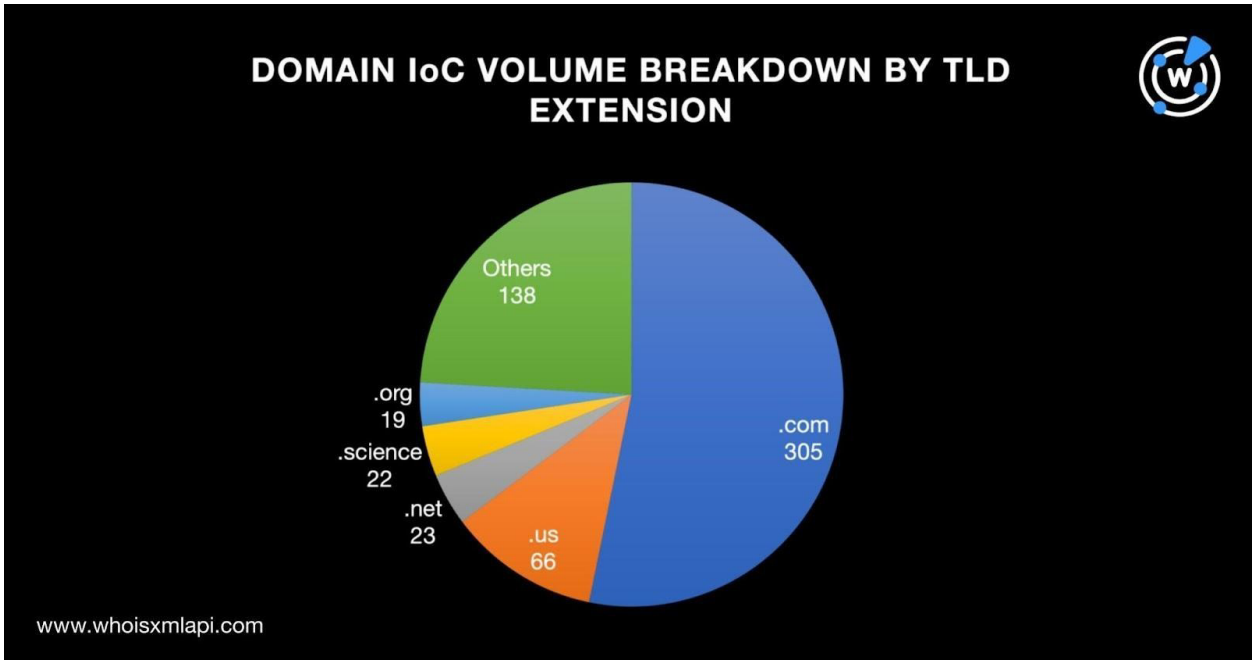

- 310個のドメインIoCは登録年月日が不明でしたが、残りの263個については、WHOISレコードから、1997年から2023年の間に新規登録されたものとわかりました。そして、そのうち最も多い72個は、2022年に登録されたドメイン名でした。



- 358個のドメインIoCは、公開のWHOISで登録者の国の情報を検索できませんでした。他方、WHOISレコードがある残りの215個は、米国（64個）、日本（17個）、インド（14個）、フランス（12個）、中国（10個）を筆頭に32カ国に広がっていました。




また、573個のドメインIoCの中で最も多く使われていた5つのTLDは、.com（305個）、.us（66個）、.net（23個）、.science（22個）、.org（19個）でした。残りの138個のドメインIoCは、他の29種類のTLDのドメイン名でした。




## BreachForumsのIoCリスト拡張

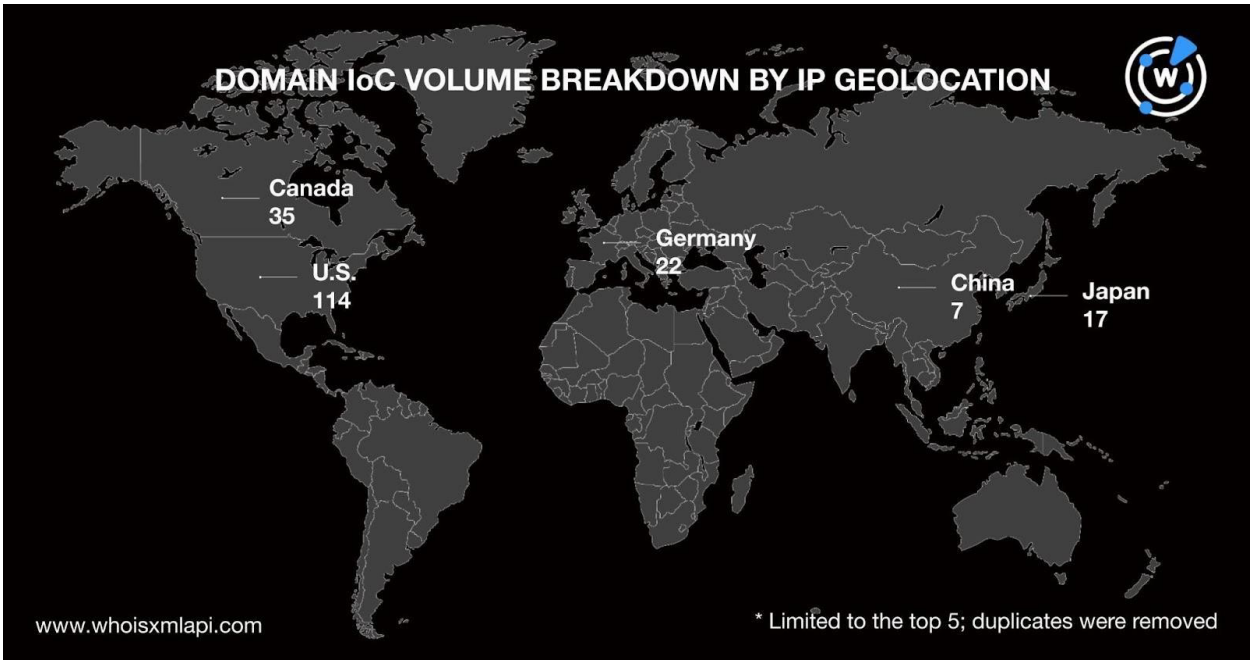
BreachForumsメンバーのサイバー犯罪インフラについて詳しく知るため、573個のドメインIoCの調査を横展開しました。

WHOIS レコードが取得できるドメインIoCを精査したところ、登録者のメールアドレスをWHOISで公開しているものがいくつかありました。そのうち50個以下のドメイン名の登録に使用されたメールアドレスに対象を絞り、Reverse WHOIS Searchで検索した結果、それらはさらに12個の別のドメイン名によって共有されていたことがわかりました。

次に、573個のドメインIoCに対してDNS Lookupを実行したところ、253個のIPアドレスに名前解決されました。そして、そのうちの1個（137[.]184[.]161[.]21）については、マルウェアチェックにより悪意があることが判明しました。

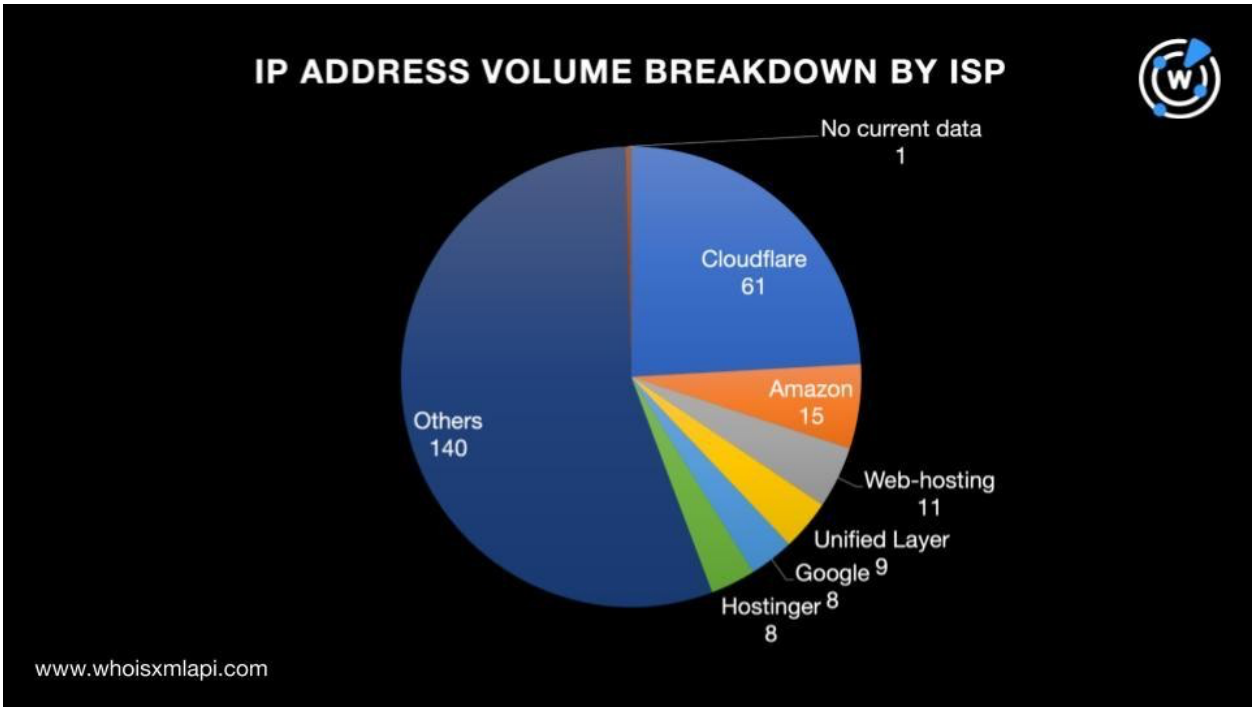
さらに、その253個のIPアドレスをBulk IP Geolocation Lookupにかけました。その結果、以下が明らかになりました。

- 1個のアドレスには国のジオロケーションデータなし。残りの252個は、米国（114個）、カナダ（35個）、ドイツ（22個）、日本（17個）、中国（7個）を筆頭に、27の異なる国に位置




IPジオロケーションとドメイン名登録者所在地の上位5カ国を見比べたところ、中国、日本、米国の3カ国が一致

- 1個のIPアドレスについては、管理するインターネットサービスプロバイダー（ISP）のデータが公開されておらず。残りの252個は87のISPに分散。代表的なISPは、Cloudflare（61個）、Amazon（15個）、Web-hosting（11個）、Unified Layer（9個）、Google（8個）およびHostinger（8個）




また、上述の名前解決の検索結果をさらにReverse IP Lookupにかけることで、3,884個のドメイン名をホストしている60個の専用IPアドレスに調査対象を絞り込むことができました。

Domains & Subdomains Discoveryを使ったチェックにより、ドメインIoCに見られた文字列のうち169個が、他の9,588個のドメイン名にも含まれていることがわかりました。マルウェアの一括チェックにより、そのうち30個のドメイン名には悪意があることが判明しました。

ドメインIoCをさらに精査したところ、23個のドメイン名に6個の人気ブランド名（Amazon、Facebook、Gmail、iPhone、Tesla、Yandex）が含まれていることがわかりました。興味深いことに、これらのブランド名は、共通のIPアドレスを使っている、または共通の文字列を含んでいる127個のドメイン名にも見られました。幾つかの例を下表に示します。

| ドメイン名の文字列に含まれていた人気ブランド名 | ドメインIoC | 共通のIPアドレスを使っていたドメイン名 | 共通の文字列を含むドメイン名 |
|---|---|---|---|
| Amazon | 2<br>verification-amazon-fr[.]fr | 2<br>amazonyrosa[.]in | 5<br>amazon-firebiz[.]nom[.]za |
| Facebook | 1 | | |

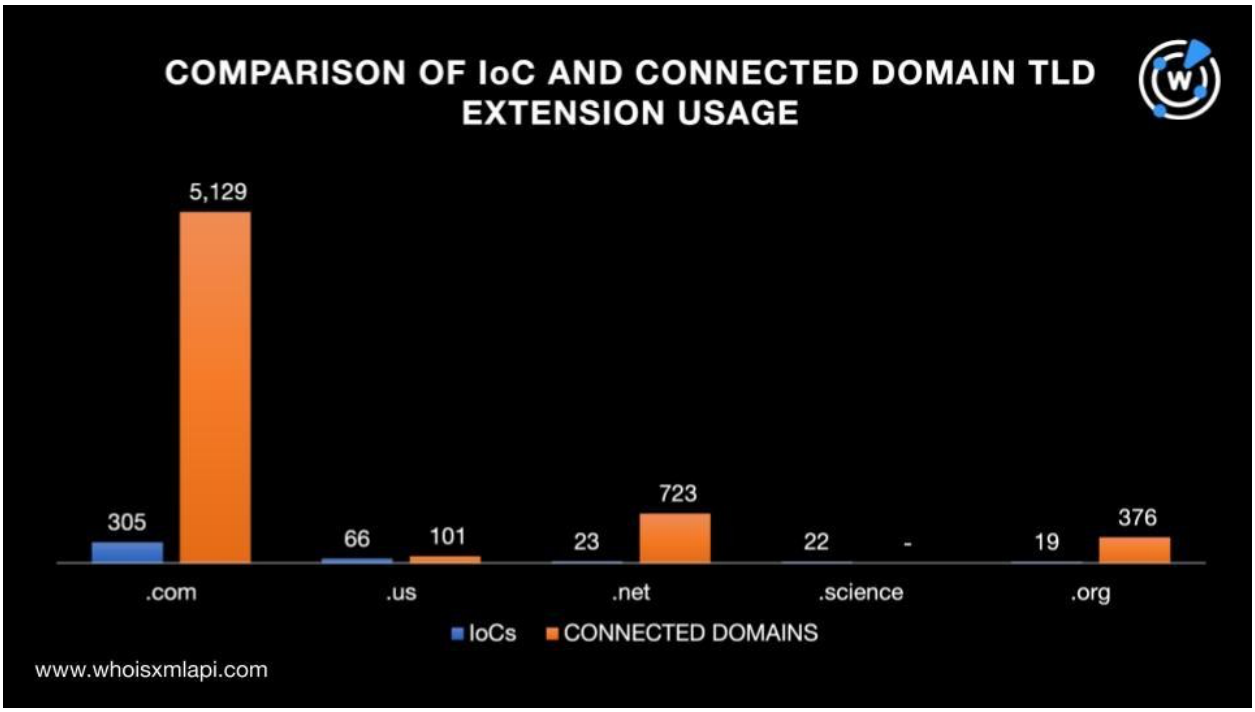
| | | | |
|---|---|---|---|
| | facebooksexlist[.]com | | |
| Gmail | 17<br>f-gmail[.]com | 4<br>account-my-mail-gmail[.]com | 71<br>albagulizia-gmail[.]com |
| iPhone | 1<br>findmyiphone-view[.]com | 1<br>iphone-15.com[.]ua | 1<br>iphonebiz[.]com[.]br |
| Tesla | 1<br>teslamemorial[.]science | | 1<br>teslamemorial[.]biz[.]at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

その127個のドメイン名のうち、公開のWHOISレコードから上記6社のドメイン名であることを確認できたものはありませんでした。これらについてScreenshot Lookupを実行したところ、本稿執筆時点では、101個のドメイン名がアクセス可能なまま維持されています。ただし、その多くはエラーページやインデックスページに誘導されます。

最後に、メールアドレス、IPアドレスまたは文字列の使用状況から脅威への繋がりが疑われる13,484個のドメイン名に着目し、先のIoC精査でわかった5つのTLDを使ったものか幾つあるかを調べました。その結果、以下が判明しました。

- 合計6,329のドメイン名が、ドメインIoCの使用する上位5 TLDのうち4 TLDを使用
- 大部分である5,129個は.comドメイン名
- .usドメイン名はわずか101個
- .netドメイン名は723個
- .scienceドメイン名は0個
- .orgドメイン名はわずか376個

以下のグラフは、ドメインIoCと今回特定された関連ドメイン名のTLD利用状況を比較したものです。




—

このたび行ったBreachForumsのIoCリストの分析から、潜在的な関連ウェブプロパティを新たに13,484個発見することができました。そして、マルウェアチェックにより、そのうち53個には悪意があることも判明しました。また、ドメインIoCと関連ドメイン名の間には、.com TLDの多用などの共通点があることも確認しました。

***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

### BreachForumsのIoC

- 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

## 共通のメールアドレスを使用していたドメイン名の例

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

## 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

- carmainten[.]com

## 名前解決したIPアドレスの例

- 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

### 悪意あるIPアドレスの例

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

### 共通のIPアドレスを使用していたドメイン名の例

- 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

## 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

- 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

## 共通の文字列を使用していたドメイン名の例

- 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

### 共通の文字列を使用していた悪意あるドメイン名の例

- 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