

.zipなどのドメインのリスクをDNSインテリジェンスで軽減

目次

1. [要旨](#)
2. [付録：アーティファクトとIoCの例](#)

要旨

Googleによる新gTLD「.zip」のドメイン名販売開始の発表は、物議を醸しました。[ファイル拡張子の.zipと混同されやすい](#)ことから、フィッシングなどの悪意あるキャンペーンに悪用されるかもしれない、と多くの方が考えたためです。そして、その[懸念は現実のものとなりました](#)。その発表からまもなく、フィッシング詐欺師が.zipドメインを使い始めたのです。

.zipを含む紛らわしい新gTLD (.app、.cab、.cam、.mobi、.mov、.pub、.rip、.win) がもたらすリスクを回避するため、WhoisXML APIでは、2023年1月1日から5月31日までの間に新規登録されたこれらのTLDのドメイン名についてDNS情報を分析し、不審なドメイン名を調べました。その結果、以下を発見しました。

- .app、.mov、.zip (Googleがレジストリとして管理しているTLD) のドメイン名が21,035個。そのうち33個はすでに悪意で使用された可能性あり
- .cab、.cam、.mobi、.pub、.rip、.win (Google以外のレジストリが管理しているTLD) のドメイン名が26,961個。そのうち130個はマルウェア攻撃に使用された可能性あり

紛らわしいドメインをDNSで深掘り

まず、現存する全ての新gTLDのリストを入手し、その中からファイル拡張子と混同される可能性のあるものを特定しました。その結果は以下の表の通りです。

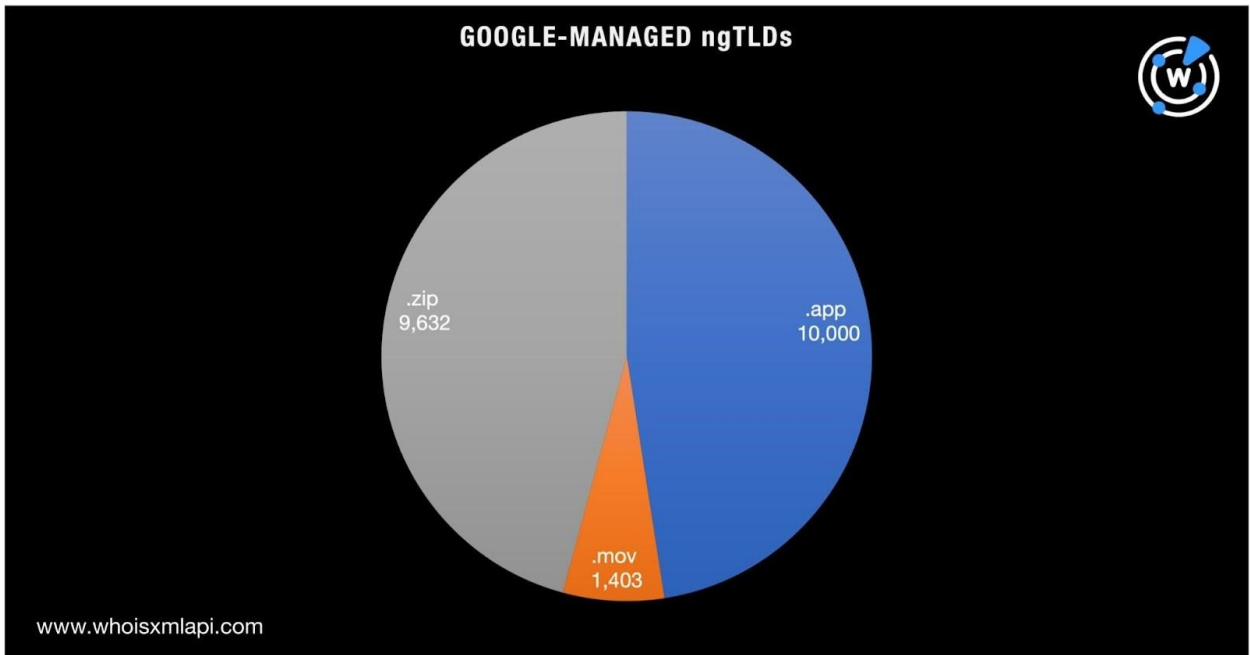
混同される可能性のある新gTLD	レジストリ/スポンサー	アプリケーションのファイル拡張子
.app	Google	macOSのアプリケーション・バンドル

.cab	Binky Moon, LLC	Microsoft Windowsのアーカイブファイル形式
.cam	CAM Connecting SarL	AutodeskのEagle Drawing Editorを使用して作成されたファイル
.mobi	dotMobi (Afiliasの傘下)	電子書籍用に設計されたファイル拡張子。主にAmazon Kindle用
.mov	Google	Appleが開発したビデオフォーマット。主にQuickTimeで使われるMPEG 4の動画コンテンツフォーマット
.pub	United TLD Holdco Ltd.が提案 (管理レジストリは未指定)	Microsoft Publisher文書のファイル形式
.rip	Rightside/Demand Media (United TLD Holdco Ltd.)	リッピングされたオーディオファイルの出力ファイル
.win	Global Registry Services Limited	Windowsシステムのバックアップファイルとして最も一般的な形式
.zip	Google	複数のファイルを1つのファイルに圧縮して収めることができるファイル形式

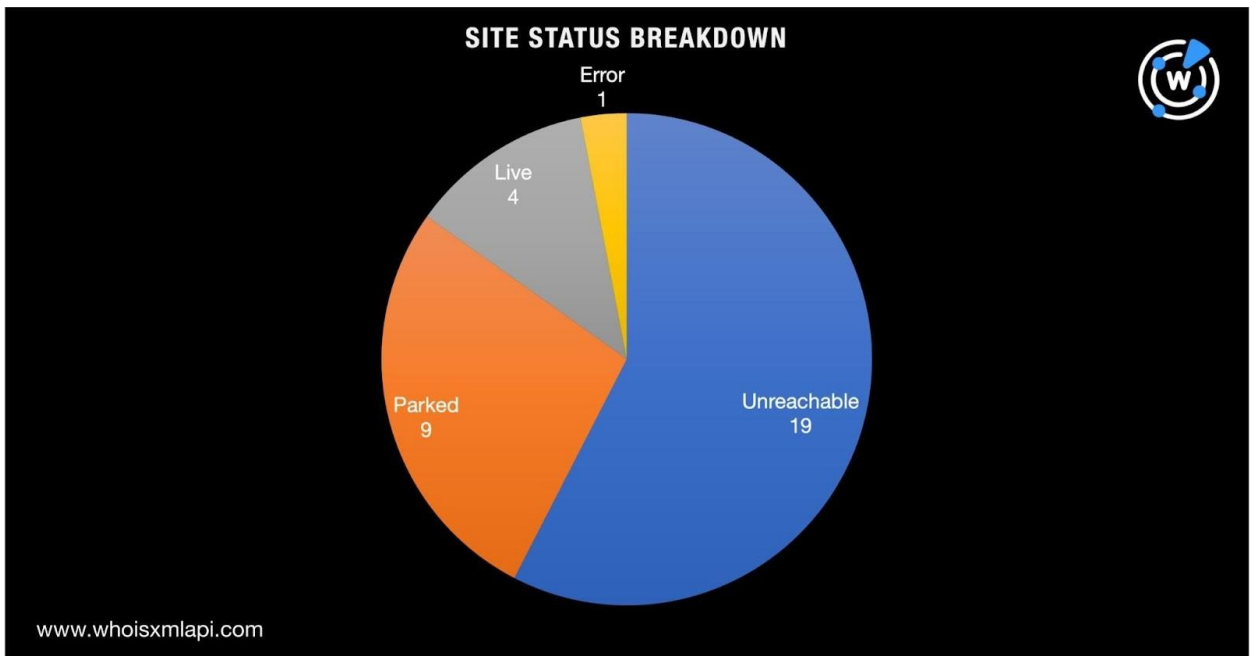
次に、[Domains & Subdomains Discovery](#)を使い、上の表にある新gTLDのドメイン名で、かつ2023年1月1日から5月31日までの間に登録されたものを洗い出しました。該当したドメイン名は、Googleが管理するものと他のレジストリが管理するものに区別しました。

Googleが管理する新gTLDのドメイン名

この作業により、.app、.movおよび.zipのドメイン名は21,035個特定されました。内訳は以下の通りです。



それらを一括マルウェアチェックにかけたところ、33個（26個の.appドメイン名と7個の.zipドメイン名）はすでに悪意あるキャンペーンで使用された可能性があるとわかりました。そうしたマルウェアホストまたはフィッシングドメインの大半は、アクセス不能でした。当社の [Screenshot Lookup](#) で判明したサイトのステータスは、以下の通りです。



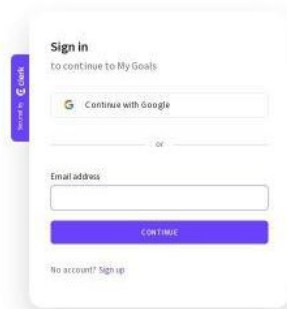
以下は、悪意あるドメイン名でホストされ、現在も稼働しているサイトのスクリーンショットです。



Screenshot of 358473[.japp



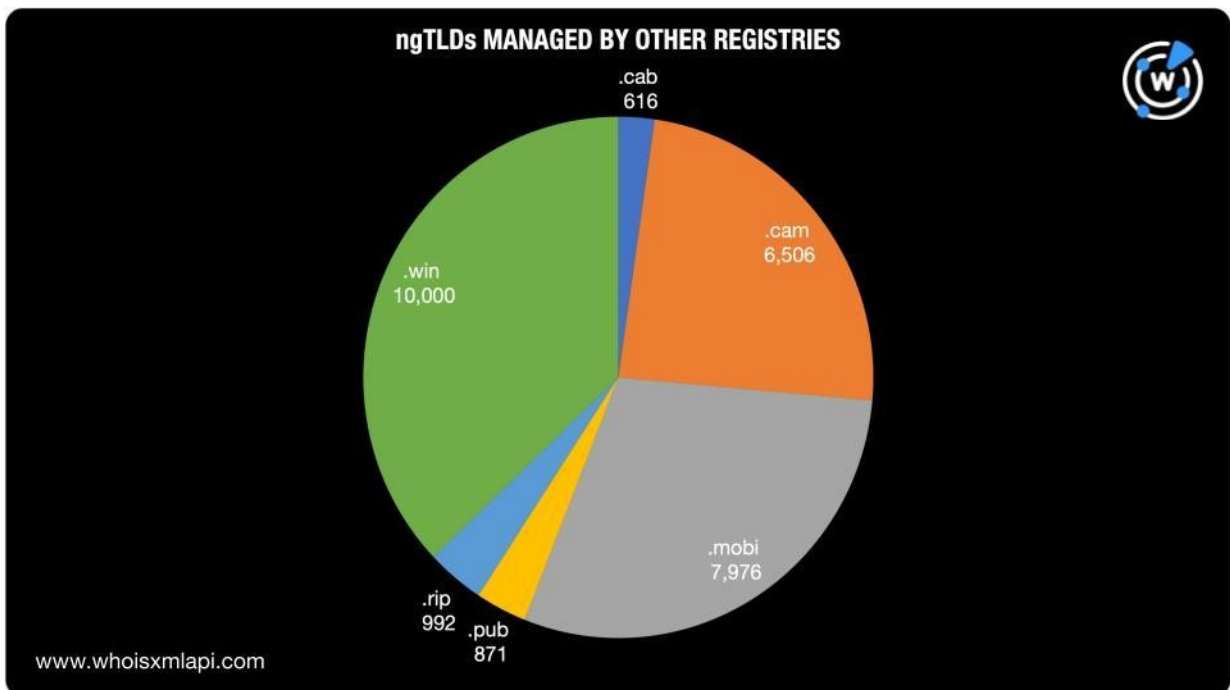
Screenshot of qt8[.japp



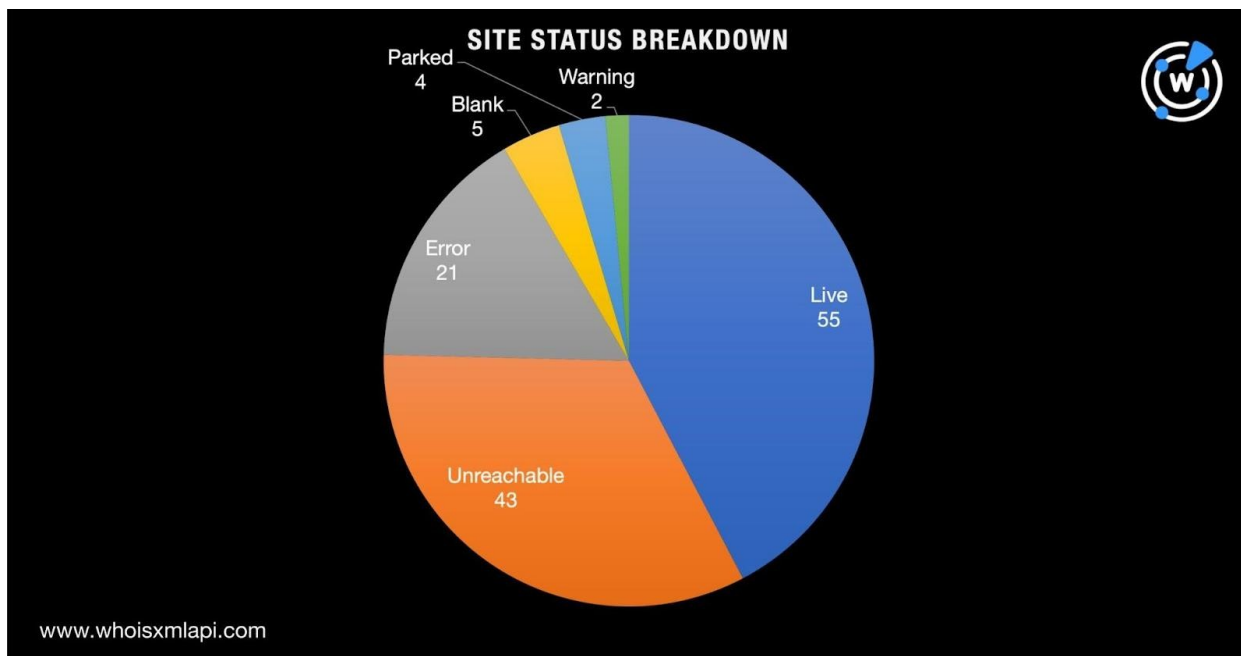
Screenshot of my-goals[.japp

Google以外のレジストリが管理する新gTLDのドメイン名

Google以外のレジストリが管理する.cab、.cam、.mobi、.pub、.ripおよび.winでは、合計26,961個のドメイン名が該当しました。その内訳は以下の通りです。



それらのうち130個（.cab 1個、.cam 49個、.mobi 13個、.pub 3個、.rip 1個、.win 63個）は、すでにマルウェアの配布やフィッシング攻撃に使用された可能性があります。当社のScreenshot Lookupによると、大半のドメイン名は現在も有効です。ドメイン名の状態の内訳は以下の通りです。

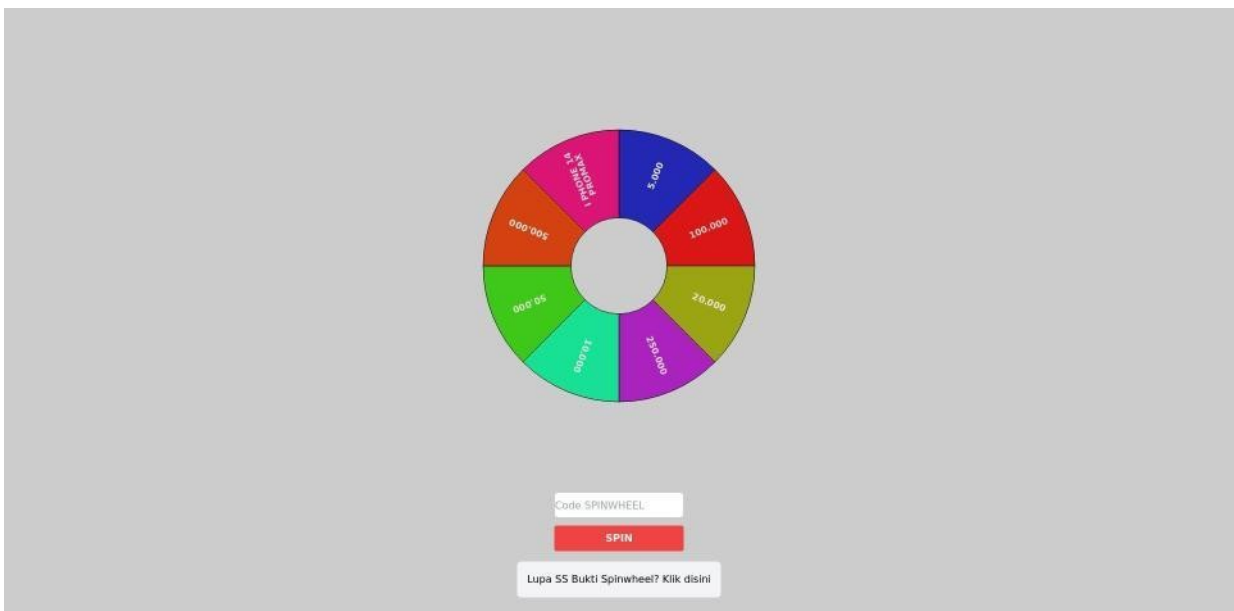


例として、悪意ある43個のドメイン名でホストされており、現在もアクセス可能なサイトのスクリーンショットを以下に示します。



Screenshot of rap78[.]win and 39 other .win domains

40個の悪意あるドメイン名は同じコンテンツを使用していました。また、ランダムな数字と文字の組み合わせで構成されているという共通点がありました。このことは、それらのドメイン名が同じマルウェア攻撃で使用された可能性を示唆しています。



Screenshot of spnwheelido88[.]win and spnwheelnewply88[.]win

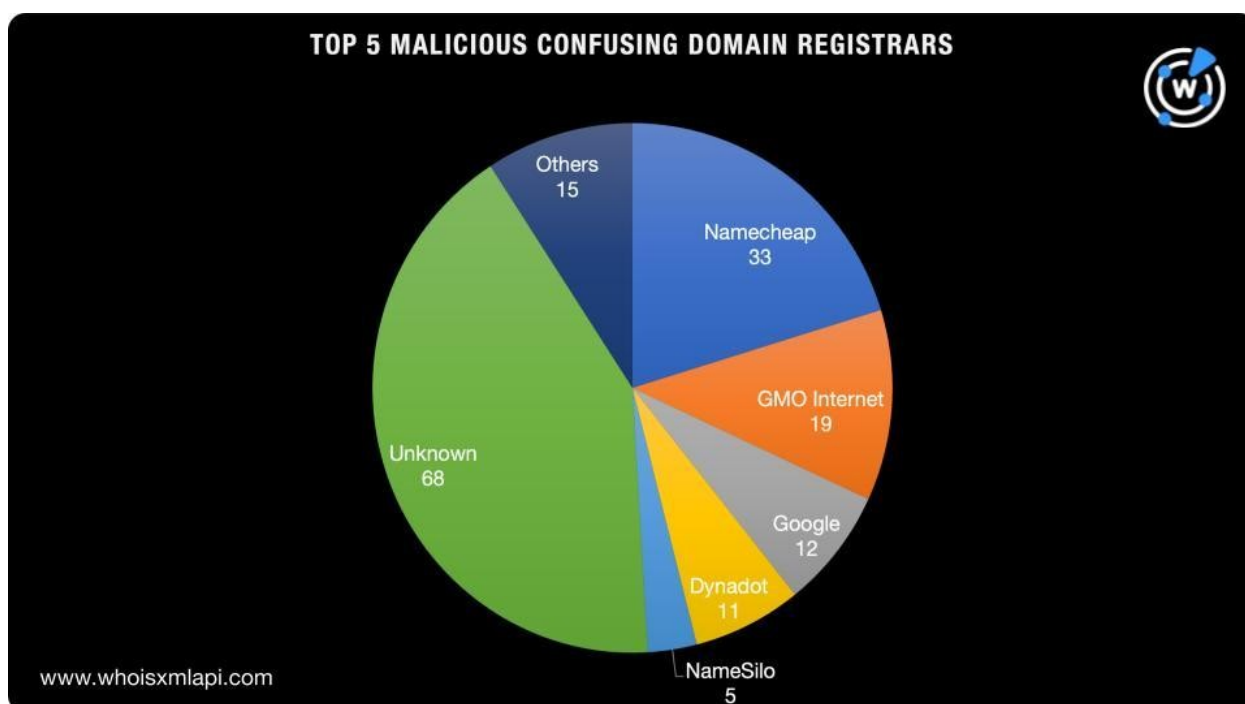
同様に、2つのドメイン名が同じコンテンツとTLDを使用していることから、同じ悪意あるキャンペーンに参与した可能性があります。その2つは全く同じ **spnwheel** という文字列を含んでいます。

悪意ある紛らわしいドメイン名を観察

さらに調査を深めるため、悪意の可能性のある紛らわしい新gTLDドメイン名を全て洗い出しました。この作業の結果、.app、.cab、.cam、.mobi、.pub、.rip、.winおよび.zipのドメイン名163個をリストアップできました。

それらを [Bulk WHOIS Lookup](#) で一括検索した結果、以下がわかりました。

- それらのうち最も多くのドメイン名を管理していたレジストラはNamecheapで、33個。次いで、多い順にGMOインターネット、Google、Dynadot、NameSilo。



- 95個は新規に登録されたドメイン名で、残りの68個はWHOISの新規登録日の欄が空白。
- 全てのドメイン名の登録者メールアドレスは編集されており、特定できず。

さらに [Bulk IP Geolocation Lookup](#) で検索したところ、以下のことも判明しました。

- 悪意ある紛らわしいドメイン名163個のうち、IPアドレスに名前解決したのは67個のみ。
- 67個のドメイン名は82個のユニークなIPアドレスに解決。そのうち91%はIPv4アドレス。
- マルウェアチェックの結果、15個のIPアドレスには悪意があることが判明。そのうち4個は専用ホスト。

可能な限り多くの潜在的アーティファクトを特定するための最終ステップとして、その4個の悪意あるIPアドレスを[Reverse IP Lookup](#)にかけました。その結果、さらに137個のドメイン名が見つかり、そのうち32個がマルウェアホストに分類されました。

まとめ

広く使用されているファイル名の拡張子「.zip」などと混同されやすい新gTLDのドメイン名をDNSで詳しく調査したところ、その多くが既に脅威アクターによって悪用されている可能性があることがわかりました。

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。

付録：アーティファクトとIoCの例

Googleが管理する紛らわしい新gTLDのドメイン名の例

- wendys[.]zip
- wandero[.]app
- smartaichat[.]app
- monitee[.]app
- techtronics[.]app
- 1xapk[.]app
- validusportal[.]app
- 7bp[.]app
- playgame[.]zip
- edgetracker[.]app
- sentinel[.]zip
- bootleg[.]zip
- cubehq[.]app
- fileextractor[.]zip
- powerpoints[.]zip
- ingest[.]zip
- beatsxyz[.]app
- dreambox[.]zip
- studiokarma[.]app
- dickpics[.]zip
- insurance[.]zip
- dbdump[.]zip
- chromebook[.]mov
- 3039n[.]app
- backup2[.]zip
- smartfrog[.]app
- apoel[.]zip
- minesweeper[.]zip
- kniffel-block[.]app
- healthtechconnect[.]app
- spothunt[.]app
- locuspace[.]app
- pjwhjtos[.]app
- jnty111[.]app
- myhomesphere[.]app
- 4919e[.]app
- feedbackflow[.]app
- backrs[.]app
- saleorx[.]app
- 678178[.]app
- 123456[.]zip
- tryimpulse[.]app
- recappedai[.]app
- heisi[.]zip

- sumitup[.]app
- slay[.]zip
- nowcher[.]app
- cowandrooster[.]zip
- Onlyfans[.]zip
- ihateit[.]zip
- signature-required[.]zip
- zipzap[.]zip
- placestorent[.]app
- locator[.]zip
- airshield[.]app
- qwerty[.]zip
- paylocity[.]zip
- jointbudget[.]app
- blacktrust[.]app
- kompresja[.]zip
- reuron[.]app
- bbc[.]zip
- bdtmsdcapital[.]zip
- yourpassword[.]zip
- yello[.]zip
- bdtcompanyinternational[.]mov
- secure-share[.]zip
- updatedfirmware[.]zip
- qantasloyalty[.]mov
- astroservices[.]app
- defender-update-kit-x64[.]zip
- rootedopportunity[.]zip
- cbfin[.]app
- trottdellco[.]zip
- accesslog[.]zip
- 6686442[.]app
- jiangnan399[.]app
- jieya[.]zip
- warriorbox[.]app
- venmosafe[.]app
- contract-draft[.]app
- 303vip[.]app
- scriptease[.]app
- trottdell[.]zip
- explosion[.]zip
- mt31[.]app
- gpt-ai[.]app
- www3039ah[.]app
- porsche[.]zip
- dentsu[.]zip
- kodrs[.]app
- casestudy[.]zip
- vulonkaaz[.]zip
- trottfamilyfoundations[.]mov
- cloud-domains-cep-serverless-cancellation-fee-1392119256[.]app
- appdetectivepro[.]zip
- drisky[.]app
- locasun[.]mov
- personalize[.]app
- jnyl858[.]app
- obamawhitehousearchive[.]zip
- gioc[.]app
- bliz[.]zip
- archive2023[.]zip
- logitechdriverupdate[.]zip
- safe[.]zip
- keithstore[.]app
- contentai[.]app
- geab[.]app
- ox6[.]zip
- 0click[.]zip
- c0w[.]zip
- padelhub[.]app
- wildfire[.]zip
- forwardsms[.]app
- manifesto[.]zip
- bootypics[.]zip
- 6686289[.]app
- bet-mgm[.]app
- ma03[.]app
- presentatie[.]zip
- pegasusghost[.]zip
- filehub[.]zip

- kannanation[.]app
- managekit[.]app
- xj6666[.]app
- echohammond[.]zip
- esgindex[.]app
- h2-agency[.]app
- prorate[.]app
- jnyule399[.]app
- purehub[.]app
- mulesoft[.]zip
- kiteup[.]app
- inferi[.]zip
- money911[.]app
- 6686571[.]app
- sportshero[.]app
- scanboy[.]app
- breachdata[.]zip
- sensilla[.]zip
- captions[.]zip
- datafuze[.]zip
- 409group[.]app
- valleystar[.]zip
- thedongheang[.]app
- quizomatic[.]app
- mamie[.]zip
- lookerstudio[.]mov
- blaster[.]zip
- msazure[.]zip
- productions[.]mov
- jordanjeffries[.]zip
- macquariebank[.]zip
- cartorionat[.]app
- casasdesconto[.]app
- final-1[.]zip
- rstars[.]zip
- jnty138[.]app
- archive1[.]zip
- 6686421[.]app
- restoreai[.]app
- tfe-install[.]zip
- khalifa[.]zip
- meeting-notes[.]zip
- unhide[.]app
- egress[.]zip
- betalingen[.]zip
- sonsofprophets[.]app
- esm[.]zip
- xspeed[.]app
- packshot[.]mov
- album2023[.]zip
- sebastian[.]zip
- kabelkom[.]zip
- discordbot[.]zip
- convotis[.]zip
- resume[.]zip
- echoohio[.]zip
- p2pview[.]app
- faraz[.]zip
- marvel[.]mov
- ghumantu[.]app
- lookla[.]app
- onememo[.]app
- archlinux[.]zip
- amy[.]mov
- bandao11[.]app
- 94027[.]zip
- odisi[.]app
- microsoftupdate[.]zip
- innovest[.]app
- gtfs[.]zip
- emsy[.]mov
- oceanfirst[.]mov
- assetlab[.]app
- bdbet5[.]app
- galgame[.]zip
- lenny[.]zip
- glyatirim[.]app
- download-form[.]zip
- download-a-car[.]zip
- hgtvsweepstakescentral[.]app

- cfre[.]app
- 6686vn89[.]app
- trottdellcap[.]mov
- gold724[.]app
- surprise[.]zip
- meituan[.]zip
- 35ty8[.]app
- 8868099[.]app
- accuda[.]app
- skillai[.]app
- desisocial[.]app
- tequilasuite[.]app
- loyalty[.]zip
- nr0[.]app
- nudity[.]mov
- brightchat[.]app
- macos-update[.]zip
- security-patch-update[.]zip
- uhaul[.]zip
- e-ticket[.]zip
- xn--passwrt-47a[.]zip
- edgeupdate[.]zip
- deployments[.]zip
- access-logs[.]zip
- cursed[.]zip
- fiel[.]zip
- cocacola[.]zip
- 8bit[.]zip
- audiolive[.]app
- melvin[.]zip
- defcon32[.]zip
- untitled-project[.]app
- jnyl123[.]app
- saaswiz[.]app
- summercircle[.]app
- burnsandwilcox[.]mov
- tarrrescue[.]app
- kitchencompanion[.]app
- dubaicustoms[.]app
- q2131205wh2k[.]app
- 69dsp[.]app
- notoist[.]app
- family[.]zip
- 3885hhh[.]app
- purchasing-invoice[.]zip
- allmasters[.]app
- n2e[.]app
- haussmann-recouvrement[.]zip
- chunithm[.]zip
- peepssoftware[.]zip
- sighun[.]zip
- unencrypted[.]zip
- mm888[.]app
- paloaltonetworks[.]zip
- connected[.]mov
- elsalvadorbtc[.]app
- fredbsc[.]app
- polyhomory[.]app
- mcksalaries[.]zip
- shiproutepro[.]app
- zip[.]zip
- bubblesupsoapery[.]app
- alomoves[.]mov
- aathmi[.]app
- kleinanzeigen[.]mov
- barkparkbistro[.]app
- zbsm[.]zip
- 8868m2[.]app
- swyrl[.]app
- aa88686[.]app
- avinoc[.]app
- keyhole[.]zip
- smartmatrix[.]app
- jnyl555[.]app
- keyminer[.]app
- activist[.]app
- transcend[.]mov
- zrbet30[.]app
- foto[.]zip
- tohru[.]zip

- shopnest[.]app
- bdtcp[.]mov
- fortytwo[.]zip
- esims[.]zip
- qr[.]zip
- mineralprices[.]app
- snfsolutions[.]zip
- lumina-ai[.]app
- tinzien[.]zip
- firmware-files[.]zip
- sentfiles[.]zip
- nbcnews[.]zip
- solily[.]app
- ddh10[.]app
- theme-export[.]zip
- reee[.]zip
- gesheft[.]app
- collegeessay[.]app
- asdasxa0676[.]app
- offer[.]zip
- modernsafetysolutions[.]app
- 1tamilmv[.]zip
- albert[.]zip
- secwatch[.]zip
- googleonandroid[.]mov
- cbmtechnology[.]zip
- pulsefi[.]app
- jiangnan123[.]app
- whaz[.]zip
- 678292[.]app
- account-info[.]zip
- anrok[.]app
- irris[.]app
- petsolv[.]app
- wowzers[.]app
- wohlfahrts[.]app
- exportfile[.]zip
- kiri[.]zip
- ricin[.]zip
- ware[.]zip
- roamin[.]app
- binspace[.]app
- stockdads[.]app
- tata1[.]app
- weventure[.]app
- utilitease[.]app
- fahr-teacher[.]app
- toteslegitnotmalware[.]zip
- electrictry[.]zip
- socialwell[.]app
- jnyule224[.]app
- mdr[.]zip
- chokidaar[.]app
- 88681082[.]app
- huntonak[.]mov
- defenderupdates[.]zip
- sitefly[.]app
- testyourfirewall[.]zip
- plotplot[.]app
- order-cancel[.]zip
- umbrellagroup[.]app
- sushi-land[.]app
- kisah[.]app
- approvals[.]zip
- tltfamilyoffice[.]zip
- coxenterprises[.]zip
- xkeyscore[.]zip
- bdy168[.]app
- jnyule80[.]app
- 6686828[.]app
- ptpshipping[.]app
- peachbar[.]app
- firo[.]zip
- jiangnan243[.]app
- cellar8[.]app
- repository[.]zip
- hashjack[.]app
- shabinx[.]zip
- hgajshdsadh[.]app
- attachments[.]zip

- obamawhitehousearchive[.]mov
- t-store[.]app
- jntiyu157[.]app
- pokupki[.]app
- dreambeaver[.]app
- 678144[.]app
- apache[.]zip
- jiliko747[.]app
- handwerksportal[.]app
- elektrikka[.]app
- kittyx[.]app
- lickity[.]zip
- movies123[.]zip
- googledrivesetup[.]zip
- v69[.]zip
- idonation[.]app
- dataliberty[.]app
- bankofnewzealand[.]zip
- proportio[.]app
- webseeds[.]app
- companysalaries[.]zip
- troyano[.]zip
- setecastronomy[.]zip
- jnty387[.]app
- gelishmorgantaylor[.]zip
- 6686264[.]app
- plt[.]mov
- thisisnotmalware[.]zip
- matt[.]mov
- opie[.]zip
- equinor[.]zip
- alltournatives[.]app
- infosys[.]zip
- 88681163[.]app
- verflugungen[.]app
- offseclab[.]zip
- unpaidinvoices[.]zip
- 2023judi89[.]app
- googlechrome[.]zip
- wordpress[.]zip
- ubuntu22-04[.]zip
- codepoetry[.]app
- backupconfig[.]zip
- digital-rebels[.]app
- yourmum[.]zip
- coxenterprise[.]zip
- whip[.]zip
- buyersight[.]app
- pigeondocuments[.]app
- dyqp8[.]app
- ford[.]zip
- my02[.]app
- wristcaddy[.]app
- sysadmin[.]zip
- upspore[.]app
- readpanda[.]app
- macmind[.]zip
- assumedbreach[.]zip
- asm[.]zip
- pew[.]zip
- e2e-test-v1-everything-1679412348[.]app
- cjw000[.]app
- qianxin[.]zip
- shopee[.]zip
- paymentorder[.]zip
- program-installer[.]zip
- uniquefoods[.]app
- aiconsulting[.]app
- client-download[.]zip
- gurezy[.]app
- converse[.]zip
- luminous[.]mov
- beestock[.]app
- legalize[.]zip
- usgov[.]zip
- gltf[.]zip
- bd222[.]app
- aliveness[.]app
- betterus[.]app

- 88681157[.]app
- hg129vip[.]app
- ravestag[.]app
- telatris[.]app
- salaire[.]zip
- e-core[.]app
- sdr[.]zip
- macpomo[.]app
- dotnetinstaller[.]zip
- redbull[.]mov
- windows-updates[.]zip
- airconditioning[.]zip
- resultid[.]app
- dg-patientenhilfe[.]zip
- spam-mail[.]app
- tavnermartin[.]zip
- justificante[.]zip
- magnetmaker[.]app
- mygovau[.]app
- streamlinesolutions[.]app
- basic-setup[.]zip
- titanic[.]mov
- encrypted-file[.]zip
- multimedia[.]zip
- mobileuniononline[.]app
- anglais[.]zip
- catalyticit[.]zip
- wethefriends[.]app
- download01[.]zip
- jkinfotech[.]app
- jiangnan895[.]app
- dord[.]app
- yusri[.]app
- openthis[.]zip
- sysInternals[.]zip
- arepero[.]app
- bluewaters[.]zip
- returnsuite[.]app
- pizzazz[.]zip
- doodlegpt[.]app
- noforn[.]zip
- evrim[.]app
- layn[.]mov
- m3u[.]zip
- mrsafe[.]app
- pricelist[.]zip
- jacobd[.]zip
- ak7020[.]app
- holo[.]zip
- chromeupdates[.]zip
- successsubliminals[.]app
- policyupdate[.]zip
- definitely-not-a-virus[.]zip
- nurupi[.]app
- 0496686[.]app
- ural[.]zip
- dontopenme[.]zip
- andy[.]zip

Googleが管理する紛らわしい新gTLDの悪意あるドメイン名の例

- hist[.]zip
- 358473[.]app
- michi[.]zip
- shatter[.]zip
- poc[.]zip
- starfive[.]app
- marketer[.]zip
- unitedbirth[.]app
- featureinstaller[.]app
- qt8[.]app
- my-goals[.]app
- goblinhideout[.]mov
- screenshot[.]mov
- hcg[.]zip
- alerts-commbank[.]app
- silkayetler[.]app
- mycommbank-secured[.]app

Google以外のレジストリが管理する紛らわしい新gTLDのドメイン名の例

- 001top[.]win
- 007k[.]win
- 00853lhc[.]mobi
- 009285[.]win
- 01586988g98[.]win
- 016876[.]win
- 016877[.]win
- 016880[.]win
- 019451[.]win
- 01afacan[.]win
- 01x[.]mobi
- 029293[.]win
- 02940[.]win
- 02yue[.]win
- 0310[.]cab
- 03120[.]win
- 035003[.]win
- 03hh[.]cab
- 0447880798908[.]mobi
- 04hh[.]cab
- 0549983717[.]win
- 056432[.]win
- 057210[.]win
- 057211[.]win
- 059hg[.]mobi
- 06030[.]mobi
- 068-fk[.]win
- 075842[.]win
- 0800[.]rip
- 088663[.]win
- 09060[.]win
- 093522[.]win
- 09vip[.]win
- 0ara[.]cam
- 0c8s6[.]win
- 0chan[.]rip
- 0cikg[.]win
- 0dte[.]win
- 0h[.]rip
- 0icloud[.]cam
- 0l3xg[.]win
- 0onlyfans[.]cam
- 0s[.]rip
- 0us9g[.]win
- 0vwn8[.]win
- 0x4141414141[.]rip
- 0x420[.]pub
- 0x62[.]rip
- 0x8kt[.]win
- 0xx0[.]win
- 1-cima4u[.]cam
- 1-k6[.]rip
- 1-kb4474419-v3-x64[.]cab
- 1-m5[.]rip
- 1000x[.]win
- 10010[.]cab
- 1001lessons[.]pub
- 100861[.]cam
- 100btc[.]cam
- 100k[.]rip
- 1028[.]cab
- 106501[.]win
- 10amkarachitimein[.]win
- 10bucks[.]cab
- 10cric[.]mobi
- 10dlcvetting[.]mobi
- 10investing[.]cam
- 10s[.]cam
- 110-at[.]win
- 111-at[.]win
- 111-ky[.]win
- 111111[.]rip

- 1111m[.]win
- 112-at[.]win
- 1120036[.]win
- 11235678uw2[.]win
- 114-at[.]win
- 114514[.]cab
- 115-at[.]win
- 117-at[.]win
- 118-at[.]win
- 119-at[.]win
- 11bet[.]cab
- 11bet1[.]mobi
- 11bet1[.]win
- 11bet11[.]mobi
- 11bet11[.]win
- 11bet12[.]mobi
- 11bet12[.]win
- 11bet13[.]mobi
- 11bet14[.]mobi
- 11bet15[.]mobi
- 11bet16[.]mobi
- 11bet16[.]win
- 11bet17[.]mobi
- 11bet17[.]win
- 11bet18[.]mobi
- 11bet18[.]win
- 11bet19[.]mobi
- 11bet19[.]win
- 11bet2[.]mobi
- 11bet20[.]mobi
- 11bet20[.]win
- 11bet21[.]mobi
- 11bet22[.]mobi
- 11bet23[.]mobi
- 11bet24[.]mobi
- 11bet25[.]mobi
- 11bet25[.]win
- 11bet26[.]mobi
- 11bet27[.]mobi
- 11bet27[.]win
- 11bet28[.]mobi
- 11bet28[.]win
- 11bet29[.]mobi
- 11bet29[.]win
- 11bet3[.]mobi
- 11bet3[.]win
- 11bet30[.]mobi
- 11bet30[.]win
- 11bet31[.]mobi
- 11bet31[.]win
- 11bet32[.]mobi
- 11bet32[.]win
- 11bet33[.]mobi
- 11bet34[.]mobi
- 11bet35[.]mobi
- 11bet35[.]win
- 11bet36[.]mobi
- 11bet36[.]win
- 11bet37[.]mobi
- 11bet37[.]win
- 11bet38[.]mobi
- 11bet38[.]win
- 11bet39[.]mobi
- 11bet39[.]win
- 11bet4[.]mobi
- 11bet4[.]win
- 11bet40[.]mobi
- 11bet40[.]win
- 11bet41[.]mobi
- 11bet41[.]win
- 11bet42[.]mobi
- 11bet42[.]win
- 11bet43[.]mobi
- 11bet43[.]win
- 11bet44[.]mobi
- 11bet45[.]mobi
- 11bet45[.]win
- 11bet46[.]mobi
- 11bet46[.]win
- 11bet47[.]mobi

- 11bet47[.]win
- 11bet48[.]mobi
- 11bet49[.]mobi
- 11bet49[.]win
- 11bet5[.]mobi
- 11bet5[.]win
- 11bet50[.]mobi
- 11bet50[.]win
- 11bet51[.]mobi
- 11bet52[.]mobi
- 11bet52[.]win
- 11bet53[.]mobi
- 11bet53[.]win
- 11bet54[.]mobi
- 11bet54[.]win
- 11bet55[.]mobi
- 11bet55[.]win
- 11bet56[.]mobi
- 11bet57[.]mobi
- 11bet57[.]win
- 11bet58[.]mobi
- 11bet58[.]win
- 11bet59[.]mobi
- 11bet59[.]win
- 11bet6[.]mobi
- 11bet6[.]win
- 11bet60[.]mobi
- 11bet60[.]win
- 11bet61[.]mobi
- 11bet61[.]win
- 11bet62[.]mobi
- 11bet63[.]mobi
- 11bet64[.]mobi
- 11bet65[.]mobi
- 11bet66[.]mobi
- 11bet66[.]win
- 11bet67[.]mobi
- 11bet68[.]mobi
- 11bet68[.]win
- 11bet69[.]mobi
- 11bet69[.]win
- 11bet7[.]mobi
- 11bet7[.]win
- 11bet70[.]mobi
- 11bet71[.]mobi
- 11bet71[.]win
- 11bet72[.]mobi
- 11bet72[.]win
- 11bet73[.]mobi
- 11bet74[.]mobi
- 11bet74[.]win
- 11bet75[.]mobi
- 11bet76[.]mobi
- 11bet76[.]win
- 11bet77[.]mobi
- 11bet77[.]win
- 11bet78[.]mobi
- 11bet78[.]win
- 11bet79[.]mobi
- 11bet8[.]mobi
- 11bet8[.]win
- 11bet80[.]mobi
- 11bet80[.]win
- 11bet81[.]mobi
- 11bet82[.]mobi
- 11bet82[.]win
- 11bet83[.]mobi
- 11bet83[.]win
- 11bet84[.]mobi
- 11bet85[.]mobi
- 11bet86[.]mobi
- 11bet86[.]win
- 11bet87[.]mobi
- 11bet87[.]win
- 11bet88[.]mobi
- 11bet89[.]mobi
- 11bet89[.]win
- 11bet9[.]mobi
- 11bet9[.]win
- 11bet90[.]mobi

- 11bet90[.]win
- 11bet91[.]mobi
- 11bet91[.]win
- 11bet92[.]mobi
- 11bet92[.]win
- 11bet93[.]mobi
- 11bet93[.]win
- 11bet94[.]mobi
- 11bet94[.]win
- 11bet95[.]mobi
- 11bet95[.]win
- 11bet96[.]mobi
- 11bet96[.]win
- 11bet97[.]mobi
- 11bet98[.]mobi
- 11bet98[.]win
- 11bet99[.]mobi
- 11bet99[.]win
- 11exch[.]mobi
- 11exchange[.]mobi
- 11xplay[.]win
- 12-cd[.]win
- 120-at[.]win
- 121-at[.]win
- 123-ab[.]win
- 123-by[.]win
- 123-fr[.]win
- 123-jd[.]win
- 123-lm[.]win
- 1234567[.]cab
- 123b01[.]cam
- 123boss[.]win
- 123bronze[.]win
- 123bvn[.]cam
- 123game[.]win
- 123milhas[.]win
- 123movies-online[.]cam
- 123pan[.]cam
- 123python[.]cam
- 123telugu[.]cam
- 123whdb[.]cam
- 123win[.]mobi
- 123win01[.]cam
- 124-at[.]win
- 125-lm[.]win
- 125ecdc[.]win
- 126-at[.]win
- 126-lm[.]win
- 1266[.]cab
- 126uu[.]win
- 127-lm[.]win
- 127j3[.]win
- 128-at[.]win
- 128-ky[.]win
- 128-lm[.]win
- 129-at[.]win
- 129fh[.]win
- 12bet[.]cam
- 130casino[.]mobi
- 130casino[.]win
- 130com[.]win
- 131-at[.]win
- 131-lm[.]win
- 132-ac[.]win
- 132-at[.]win
- 132-lm[.]win
- 1326991[.]win
- 133-at[.]win
- 133-lm[.]win
- 134-at[.]win
- 135-lm[.]win
- 136-at[.]win
- 138-at[.]win
- 139-at[.]win
- 1400fs[.]win
- 149902[.]win
- 14bet[.]win
- 150-lm[.]rip
- 151-lm[.]rip
- 152-lm[.]rip

- 15355-ty[.]win
- 153coin[.]mobi
- 156ea[.]win
- 159ig[.]win
- 162un[.]win
- 163-cn[.]cam
- 163c[.]cam
- 163dns[.]pub
- 164279[.]win
- 16501[.]win
- 1674985421379185[.]mobi
- 16k[.]cam
- 16pu[.]win
- 171-lm[.]rip
- 171884[.]win
- 172-lm[.]rip
- 173-lm[.]rip
- 1759-pt[.]win
- 17shopn[.]cam
- 17vip[.]win
- 18-fh[.]win
- 18002thelaw[.]mobi
- 1842818[.]win
- 1888263[.]win
- 18bet[.]mobi
- 18wheels[.]mobi
- 1929-deik[.]win
- 1946325[.]win
- 1ace[.]win
- 1acr[.]mobi
- 1b1[.]mobi
- 1bet1[.]mobi
- 1betx[.]win
- 1byte8bit[.]mobi
- 1creator[.]win
- 1cw xv[.]win
- 1czz5hs[.]win
- 1daikin[.]mobi
- 1fgb[.]cam
- 1fnbtnf1cb[.]mobi
- 1g[.]rip
- 1g7ypb8[.]cam
- 1i2mo[.]win
- 1jz2aoh[.]win
- 1nvuti[.]cab
- 1play-demo[.]mobi
- 1post[.]mobi
- 1starbartender[.]mobi
- 1stdegree[.]mobi
- 1tamilv[.]mobi
- 1familyogi[.]cam
- 1u[.]rip
- 1up[.]win
- 1usdt[.]win
- 1wi[.]rip
- 1win[.]pub
- 1wingiris[.]win
- 1wiz[.]mobi
- 1wr[.]mobi
- 1xbet-bk1211[.]win
- 1xbet-bk232[.]win
- 1xbet-stavka-official72[.]win
- 1xbet-stavka-official78[.]win
- 1xbet-tar43[.]win
- 1xbet-tar56[.]win
- 1xbet-xbet90[.]win
- 1xbet-xbet91[.]win
- 1xbet-zerkalo51[.]win
- 1xbet74bet[.]win
- 1xbetclub[.]cam
- 1xbetfr[.]mobi
- 1xbetindia[.]mobi
- 1xbetph[.]mobi
- 1xbetvn[.]mobi
- 1xboro[.]cam
- 1xduj1a[.]win
- 1xplay[.]mobi
- 1z40ys[.]win
- 2-cima4u[.]cam
- 20-four-hour-sud[.]mobi

- 20-four-hour-suds[.]mobi
- 2021qile[.]win
- 202303cyj[.]win
- 2024eclipse[.]cam
- 2024the[.]win
- 203-lm[.]rip
- 205-lm[.]rip
- 206-lm[.]rip
- 206937[.]win
- 207-lm[.]rip
- 20bombermenslug--hitvk[.]mobi
- 20citygame[.]mobi
- 20fourhoursud[.]mobi
- 20fourhoursuds[.]mobi
- 20hdjan24[.]cam
- 20pearlspartydecor[.]mobi
- 20xg4[.]win
- 210-lm[.]win
- 213-lm[.]win
- 21supplyf[.]cam
- 21win[.]win
- 21zascq0eqc[.]win
- 220vk[.]win
- 222ds[.]win
- 22630hmgj[.]win
- 22betgiris[.]mobi
- 231hb[.]win
- 23456889ru1[.]win
- 234b[.]win
- 23519hmgj[.]win
- 2359-up[.]win
- 24-hour-sud[.]mobi
- 24-hour-suds[.]mobi
- 24-vulkan[.]cam
- 245155[.]win
- 247pestcontrol[.]cam
- 249-lm[.]rip
- 24hoursud[.]mobi
- 24hoursuds[.]mobi
- 24nl9av[.]win
- 24up[.]cam
- 24video[.]cam
- 24x7games[.]mobi
- 25-76[.]win
- 251jn[.]win
- 2523-pt[.]win
- 255621[.]win
- 256no[.]mobi
- 257177[.]win
- 25skwum[.]win
- 261ja[.]win
- 263839[.]win
- 2641997[.]win
- 26bet[.]win
- 275tf[.]win
- 2789[.]cab
- 279194[.]win
- 29-53[.]win
- 2952-ng[.]win
- 2956-yu[.]win
- 2967-qh[.]win
- 29bet[.]win
- 2a5e8[.]win
- 2alogistics[.]cam
- 2anadolucasinogiris[.]win
- 2beeb[.]mobi
- 2bong[.]cam
- 2c[.]rip
- 2c5401[.]win
- 2chaturbate[.]cam
- 2cy[.]mobi
- 2ds[.]mobi
- 2ezas[.]mobi
- 2fa[.]rip
- 2goplay[.]win
- 2hlmh[.]win
- 2io30[.]rip
- 2k[.]rip
- 2krn[.]cam
- 2krn[.]mobi

- 2krm[.]win
- 2l-i3[.]mobi
- 2ln[.]mobi
- 2lnzc[.]mobi
- 2lreb[.]win
- 2ndchance4rescue[.]mobi
- 2rbina[.]cam
- 2shb[.]win
- 2sms[.]win
- 2thebit[.]win
- 2ww-coi-nex-login[.]cam
- 2yueu[.]win
- 3-ssiptv[.]win
- 30335hmgj[.]win
- 304622[.]win
- 308088[.]win
- 30diasgratis[.]win
- 30wattee[.]cam
- 312-lm[.]win
- 313-lm[.]win
- 3142641[.]win
- 321goshop[.]mobi
- 321goshopping[.]mobi
- 322672[.]win
- 323726[.]win
- 323782[.]win
- 3265-tg[.]win
- 32damst[.]win

Google以外のレジストリが管理する紛らわしい新gTLDの悪意あるドメイン名の例

- rap78[.]win
- tmr6n[.]win
- mufg-aq[.]cam
- jrjjo[.]win
- etc-seieai[.]cam
- o68h5[.]win
- spnwheellido88[.]win
- overseasbulker[.]cam
- order912837[.]win
- npgco[.]cam
- 20xg4[.]win
- instgo[.]win
- fhb1[.]cam
- jpau[.]cam
- cv3g7[.]win
- down-imtoken[.]pub
- missionbell[.]cam
- robiiiox[.]cam
- simpleclickcounter[.]mobi
- dmee8[.]win
- order92183791234[.]win
- 81jnr[.]win
- 9n4ug[.]win
- qfsp2[.]win
- oyonn[.]win
- a-g0av[.]cam
- order9182739182378122[.]win
- ekienetceija[.]cam
- emiratepost[.]mobi
- order19818191929[.]win
- etc-ssimci[.]cam
- eeqw2[.]win
- prlvat24[.]win
- addressdawn[.]win
- qerpt[.]win
- g2yev[.]win
- e9mji[.]win
- lookserare[.]cam
- lsupport[.]mobi
- order912837179283[.]win
- gooc1[.]win
- qwww-robiox[.]cam
- re9yw[.]win
- okgvm[.]win

- post-nord[.]mobi
- l2l6o[.]win
- mullaa3len[.]cam
- urlsoft[.]win
- area4[.]mobi
- a5nnm[.]win

悪意ある紛らわしいドメイン名の専用IPホストの例

- 185[.]177[.]93[.]164
- 45[.]147[.]229[.]166

共通の悪意ある専用IPホストを使用していたドメイン名の例

- 0[.]riavideo[.]cam
- 0[.]tinyvideo[.]cam
- 0[.]vegavideo[.]cam
- 1[.]riavideo[.]cam
- 1[.]tinyvideo[.]cam
- 1[.]vegavideo[.]cam
- 2[.]riavideo[.]cam
- 2[.]tinyvideo[.]cam
- 2[.]vegavideo[.]cam
- 3[.]riavideo[.]cam
- 3[.]tinyvideo[.]cam
- 3[.]vegavideo[.]cam
- 4[.]riavideo[.]cam
- 4[.]tinyvideo[.]cam
- 4[.]vegavideo[.]cam
- addsleeper[.]com
- aicontenta[.]me
- allovideo[.]biz
- answerswords[.]xyz
- azclip[.]co[.]ua
- badrobotz[.]biz
- beksvideo[.]lol
- belavideo[.]biz
- bexivideo[.]live
- bexivideo[.]cam
- bexivideo[.]com
- bimvideo[.]cam
- booongo-uz[.]com
- bosicvideo[.]biz
- boxervideo[.]biz
- buenovideo[.]lat
- cashisnotrash[.]com
- chekmylinks[.]biz
- chilloutforus[.]com
- conusvideo[.]cam
- coralvideo[.]biz
- dennyvideo[.]biz
- detailvideo[.]biz
- dixivideo[.]biz
- duvideo[.]cam
- elpushnot[.]ru
- evavideo[.]biz
- fisivideo[.]cam
- fistikvideo[.]biz
- fixikvideo[.]biz
- galavideo[.]biz
- galavideo[.]lat
- git-store[.]online
- gitvideo[.]cam
- goodvibesforus[.]com

悪意ある紛らわしいドメイン名のIPホストを共用していた悪意あるドメイン名の例

- 0[.]tinyvideo[.]cam
- 1[.]tinyvideo[.]cam

- 2[.]tinyvideo[.]cam
- 3[.]tinyvideo[.]cam
- 4[.]tinyvideo[.]cam
- bexvideo[.]cam
- bexvideo[.]com
- bosicvideo[.]biz
- chekmylinks[.]biz

- conusvideo[.]cam
- dennyvideo[.]biz
- goodvibesmatterforus[.]com
- holavideo[.]cam
- hopivideo[.]live
- ixovideo[.]biz
- jeocontent[.]live
- kellyvideo[.]cam