A DNS Deep Dive into FUNULL's Triad Nexus

Table of Contents

Executive Report

Silent Push has been monitoring the FUNULL content delivery network (CDN) for two years now. They believe the network has played host to various cybercriminal campaigns, including investment scams, fake trading app distribution, suspect gambling networks, and the Polyfill supply chain attack.

The researchers discovered that FUNULL currently hosts a malicious domain cluster made up of more than 200,000 hostnames, 95% of which appear to have been created using a domain generation algorithm (DGA), that they have dubbed "Triad Nexus."

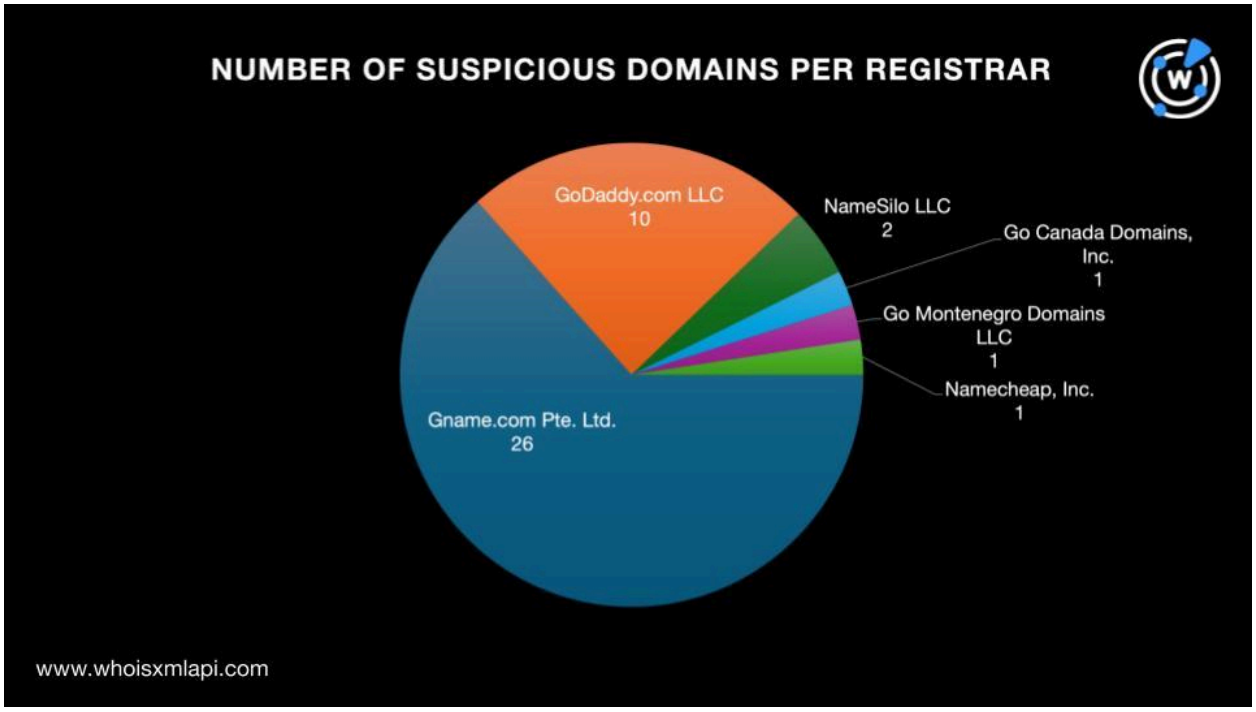
Their study identified 21 subdomains and 42 domains as suspicious indicators, which the WhoisXML API research team expanded. Our analysis led to the discovery of:

- 113 email-connected domains
- 33 IP addresses, four of which turned out to be malicious
- 274 IP-connected domains, one of which turned out to be associated with threats
- 144 string-connected domains
- 11,428 string-connected subdomains, 16 of which turned out to be malicious

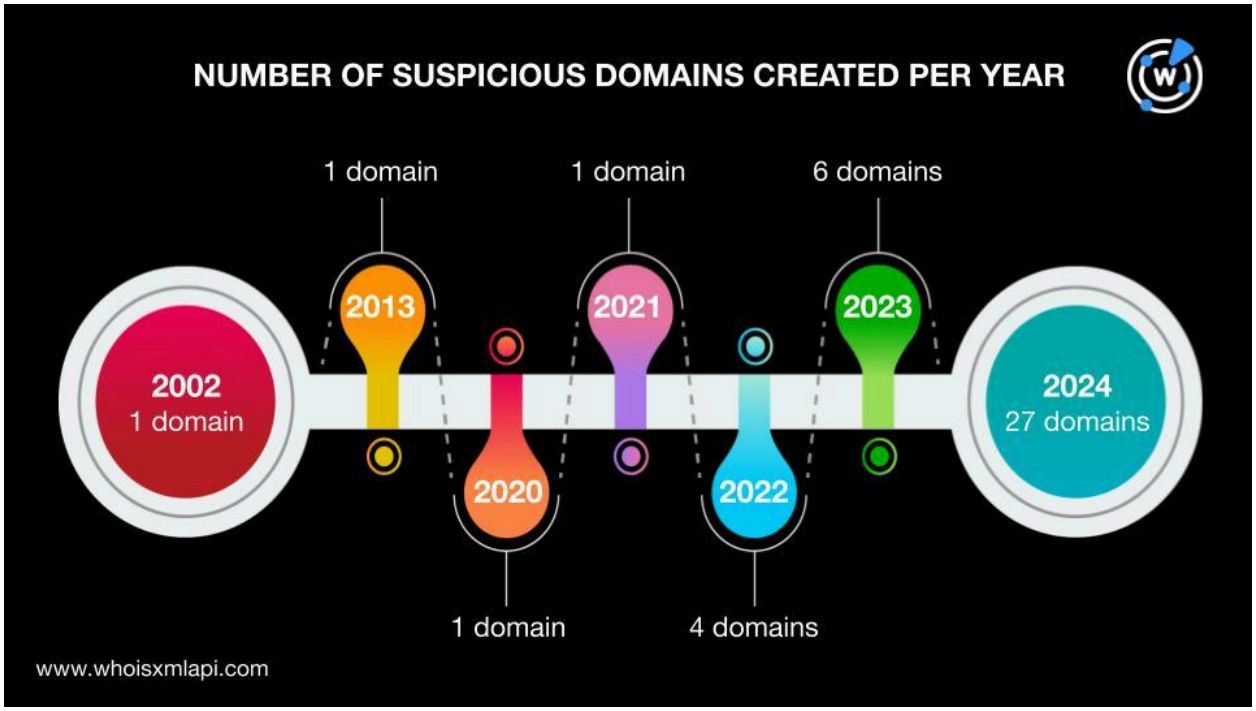
About the Triad Nexus Suspicious Indicators

We began our analysis of Triad Nexus with a bulk WHOIS lookup for the 42 domains identified as suspicious indicators. We found out that:

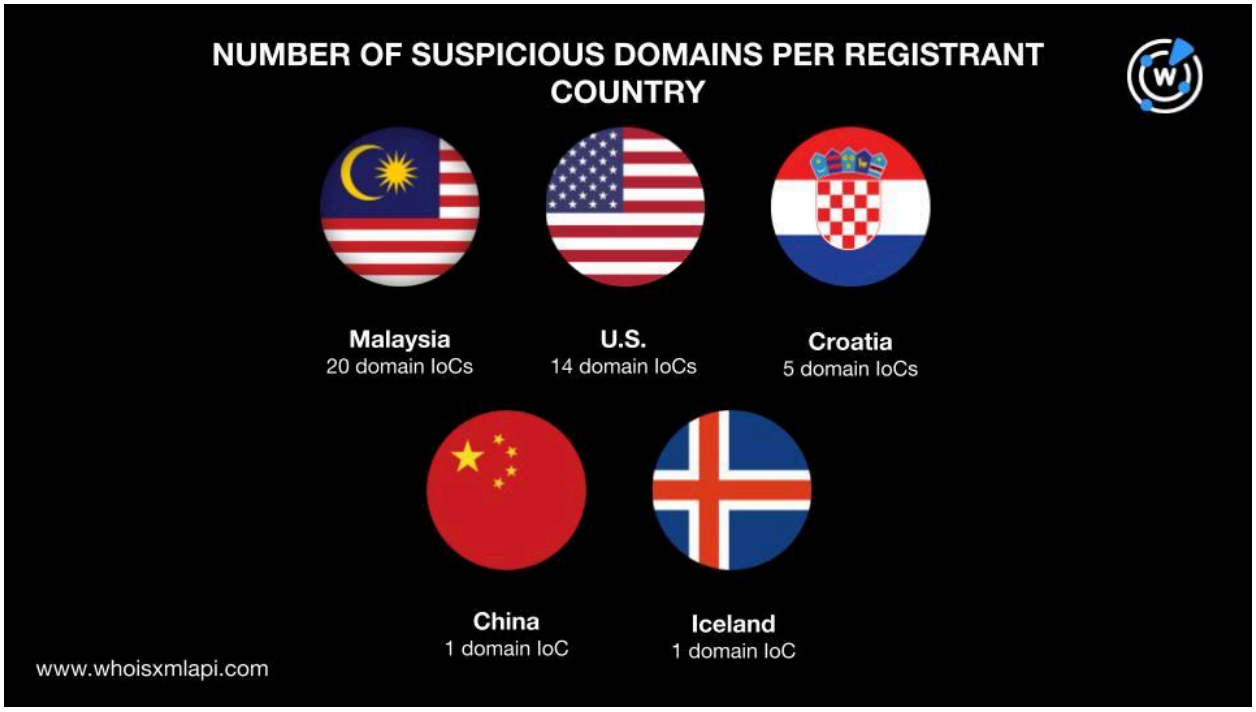
- Only 41 of the domains had current WHOIS records.
- They were distributed among six registrars topped by Gname.com Pte. Ltd. with 26 domains. GoDaddy.com LLC took the second spot with 10 domains. NameSilo LLC came in third place with two domains. Finally, Go Canada Domains, Inc.; Go Montenegro Domains LLC; and Namecheap, Inc. accounted for one domain each.



- They were registered between 2002 and 2024, implying that the threat actors did not discriminate in terms of domain age. Note, though, that more than half of the suspicious domains, 27 to be exact, were newly registered.



- They were spread across five registrant countries led by Malaysia, which accounted for 20 domains. The U.S. came in second place with 14 domains. Croatia bagged third place with five domains. China and Iceland completed the list with one domain each.



From the Triad Nexus Suspicious Indicators to Artifacts

As the first step in our suspicious indicators expansion, we queried the 41 suspicious domains on WHOIS History API. They led to the discovery of seven email addresses, four of which were public.

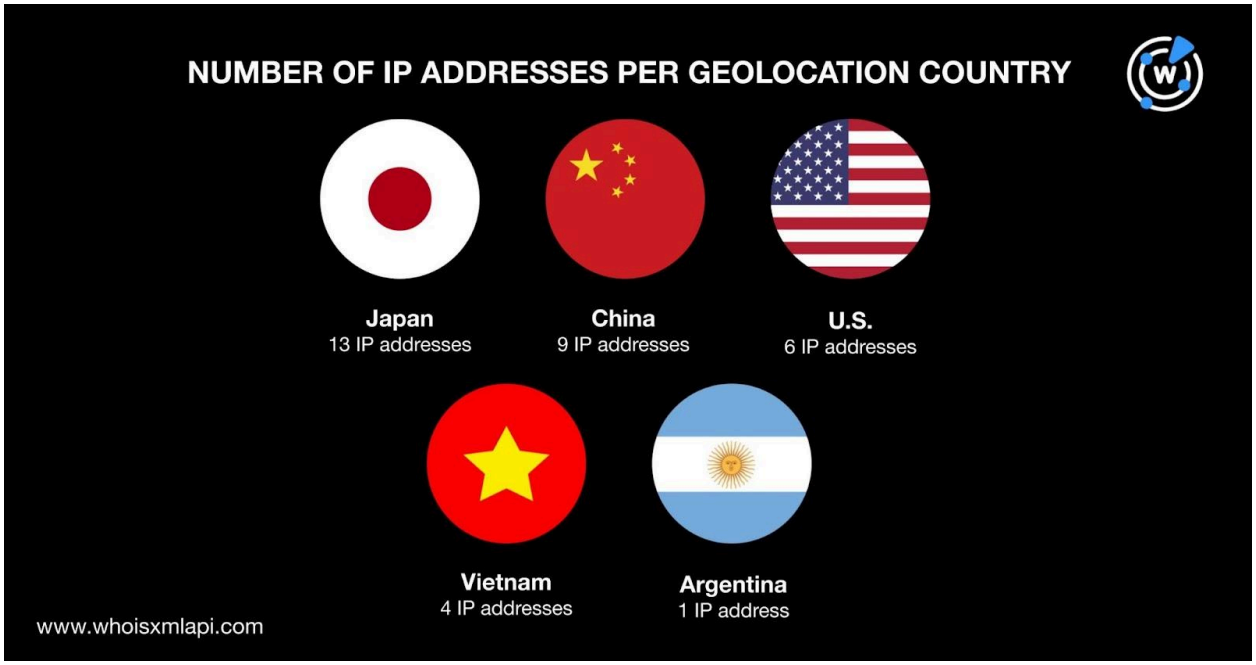
Using the four public email addresses as search strings for Reverse WHOIS API allowed us to obtain 113 email-connected domains after filtering out duplicates and the suspicious domains.

Next, we performed DNS lookups for the 41 suspicious domains and found that 34 of them actively resolved to 33 IP addresses to date after removing duplicates.

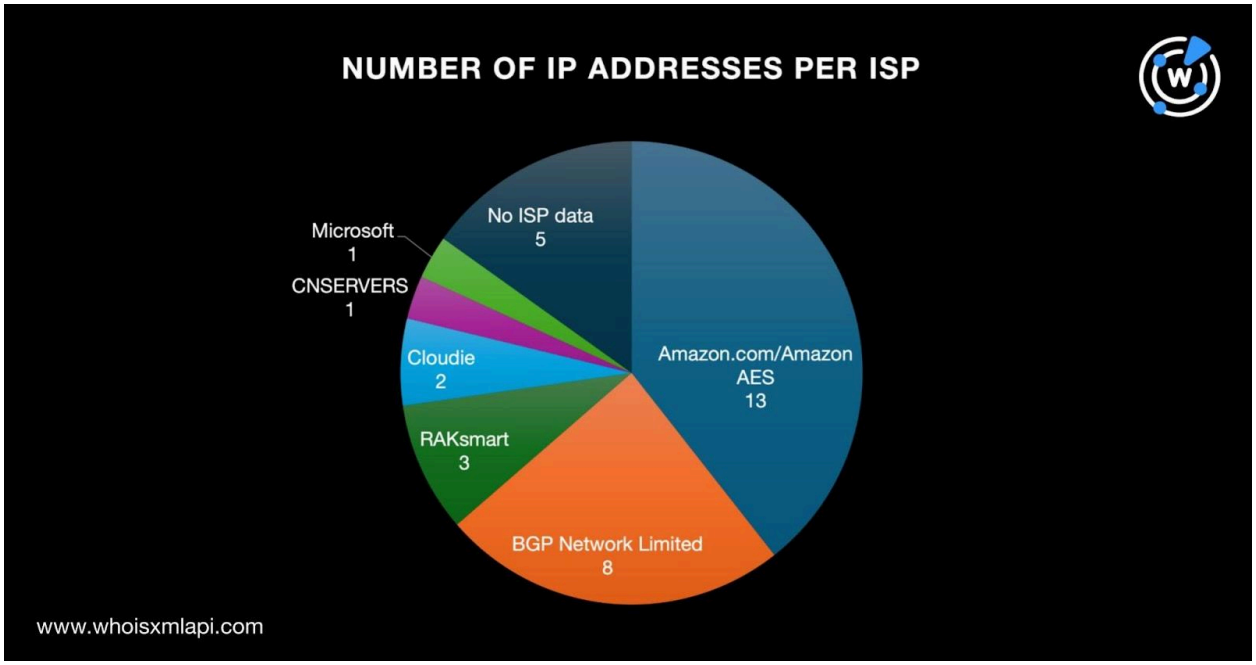
Threat Intelligence API queries for the 33 IP addresses showed that four were associated with various threats. The IP address 76[.]223[.]67[.]189, for instance, has been involved in command and control (C&C), generic threats, malware distribution, phishing, spam campaigns, and suspicious activities.

A bulk IP geolocation lookup for the 33 IP addresses revealed that:

- They were spread across five geolocation countries led by Japan, which accounted for 13 IP addresses. The remaining countries included China with nine IP addresses, the U.S. with six, Vietnam with four, and Argentina with one.



- They were distributed among six different ISPs topped by Amazon.com/Amazon AES, which accounted for 13 IP addresses. BGP Network Limited followed with eight IP addresses. RAKsmart accounted for three IP addresses while Cloudie accounted for two. CNSERVERS and Microsoft accounted for one IP address each. Finally, five IP addresses did not have ISP information.



Additionally, we determined the historical IP resolutions of the 41 suspicious domains using DNS Chronicle Lookup. Thirty-six had historical A record data. In particular:

- The domain polyfill[.]io resolved to more than 100 IP addresses since 4 October 2019.
- The 36 suspicious domains have had between one and 100+ active IP resolutions with the first seen dates ranging from 4 October 2019 to 12 October 2024.
- The suspicious domain valentinogtm[.]com has had the least number of IP resolutions—one—since 12 October 2024.

Take a look at the complete historical DNS A record findings for the suspicious domain 15991t[.]com below.

Reverse IP lookups for the 33 IP addresses showed that 16 of them could be dedicated hosts. The 16 possibly dedicated IP addresses hosted 274 domains after duplicates, the suspicious domains, and the email-connected domains were filtered out.

Based on our Threat Intelligence API queries for the 274 IP-connected domains, one—ebaymall168[.]shop—was associated with phishing.

We then performed Domains & Subdomains Discovery searches for 29 unique text strings found among the 41 suspicious domains. We found 114 domains that started with these 16 strings:

- fn03.
- funnull.
- giltbl.
- giltql.
- inditetx.
- jdfraa.
- jdfroa.
- polyfill.
- r4113.
- s3958.
- sakoffhue.
- sakoffirg.
- sakofforg.
- sonbuyre.
- sonbuyue.
- threevip.

Lastly, we scoured the DNS for 15 unique text strings found in the 21 suspicious subdomains. We uncovered 11,428 subdomains that started with these 12 strings:

- 12abb97f.
- aldo.
- asda.
- bonanza.
- cartier.
- casher.
- ebate.
- ebay.
- eby.
- etsy.
- marcus.
- tiffa.

Threat Intelligence API queries for the 11,428 string-connected subdomains showed that 16 were associated with various threats. Take a look at five examples below.

MALICIOUS STRING-CONNECTED SUBDOMAIN	ASSOCIATED THREAT TYPES
aldo[.]like2buy[.]curalate[.]com	Generic
cartier[.]like2buy[.]curalate[.]com	Generic
ebay[.]co[.]uk[.]26587424591[.]bid	Malware
etsy[.]trackinglibrary[.]prodperfect[.]com	Generic
marcus[.]com[.]ssl[.]sc[.]omtrdc[.]net	Generic

Triad Nexus: A Threat to Known Brands?

Several popular brands appeared in some of the suspicious subdomains and we specifically looked at three:

- Cartier
- eBay
- Etsy

The threat actors could have made it a point to spoof them as a social engineering tactic to gain more victims.

We uncovered 111, 4,314, and 1,378 subdomains that started with cartier., ebay., and etsy., respectively. Our WHOIS lookups for the spoofed companies' legitimate domains allowed us to obtain the following details for comparison with the possibly fake subdomains.

POPULAR BRAND'S LEGITIMATE DOMAIN NAME	PUBLIC REGISTRANT INFORMATION
cartier[.]com	**Organization:** Richemont DNS, Inc.
ebay[.]com	**Email address:** hostmaster@ebay[.]com **Organization:** eBay, Inc.
etsy[.]com	**Organization:** Etsy, Inc.

We found out that:

- None of the 111 cartier. subdomains were publicly attributable to Cartier.
- Only three of the 4,314 ebay. subdomains could be publicly attributed to eBay.
- Only three of the 1,378 etsy. subdomains were publicly attributable to Etsy.

—

Our Triad Nexus suspicious indicator expansion analysis led to the discovery of 11,992 potentially connected artifacts, 21 of which turned out to be malicious. It also revealed that the threat actors could be spoofing several world-known brands like Cartier, eBay, and Etsy to get more people to visit the pages they poisoned.

If you wish to 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

Sample Email-Connected Domains

- 001188[.]cn
- 001199[.]cn
- 004455[.]cn
- 005566[.]cn
- 028juzheng[.]cn
- 222111[.]cn
- 222888[.]cn
- 521sports[.]cn
- 52h2a8c10[.]cn
- 5352[.]cn

- 555666[.]cn
- 63[.]cn
- 73z[.]cn
- 771155[.]com[.]cn
- 888333[.]cn
- 888qc[.]com[.]cn
- 888xianhua[.]cn
- 8aqu[.]cn
- 997700[.]cn
- 999222[.]cn
- 999yule[.]cn
- aiyingwang[.]cn
- babybu[.]cn
- by099[.]cn
- cfsvc[.]cn
- changzang[.]cn
- chenhong0214[.]cn
- csthc[.]cn
- cycnu[.]cn
- d8197[.]cn
- dgzy17[.]cn
- e12501[.]cn
- fc3d868[.]cn
- feiniao01[.]cn
- gfdefd[.]cn
- ggsjvip[.]cn
- gmpqgdc[.]com[.]cn
- guanai8[.]cn
- gz060[.]cn
- gz173[.]cn
- hbecs[.]cn
- hbpd168[.]cn
- hbzsrj[.]cn
- hhswxt[.]cn
- hnrc[.]com[.]cn
- huiwind[.]cn
- huntsou[.]cn
- huohulii[.]cn
- huzhouoa[.]cn
- l1316[.]cn

Sample IP Addresses

- 103[.]231[.]15[.]133
- 107[.]148[.]152[.]147
- 107[.]148[.]152[.]149
- 107[.]148[.]152[.]154
- 122[.]10[.]113[.]114
- 13[.]231[.]147[.]70
- 13[.]231[.]94[.]131
- 13[.]248[.]213[.]45
- 134[.]122[.]184[.]106
- 137[.]220[.]146[.]140
- 137[.]220[.]202[.]170
- 137[.]220[.]225[.]126
- 137[.]220[.]225[.]155
- 137[.]220[.]225[.]81
- 15[.]220[.]121[.]180

Sample IP-Connected Domains

- 12abb97f[.]u[.]fn01[.]vip
- 12abb97f[.]u[.]fn03[.]vip
- 13-231-147-70[.]peatix[.]dev
- 145[.]cc
- 145[.]cc[.]redirection7[.]com
- 187[.]com
- 187[.]com[.]redirection7[.]com
- 2207[.]com
- 2207[.]com[.]redirection7[.]com
- 2aa08077[.]u[.]fn03[.]vip
- 3337430f[.]n[.]fnvip100[.]com
- 3833[.]site
- 46d5530dc[.]n[.]fnvip100[.]com
- 48087[.]vip

- 66v[.]app
- 66v[.]app[.]redirection7[.]com
- 6828[.]com[.]redirection7[.]com
- 688[.]ceo
- 689364[.]com
- 735[.]cc
- 735[.]cc[.]redirection7[.]com
- 766abf91[.]u[.]fn03[.]vip
- 78087[.]vip
- 7811[.]ltd
- 7811[.]ski
- 7811i[.]com
- 7811o[.]com
- 7811xxppjj[.]com
- 8866199[.]com
- 8a87ff2e[.]n[.]fnvip100[.]com
- 8ffe0976[.]u[.]fn02[.]vip
- 8ffe0976[.]u[.]fn03[.]vip
- aa123[.]com
- asedda[.]com
- aseddabh[.]com
- aseddach[.]com
- aseddack[.]com
- aseddadk[.]com
- assaeda[.]com
- asseeda[.]com
- bcbgsoead[.]com
- bcbkead[.]com
- bf595[.]com
- bf595[.]com[.]redirection7[.]com
- bf6602[.]com[.]redirection7[.]com
- blackboit[.]com
- bo365[.]com
- bo365[.]com[.]redirection7[.]com
- bonanza[.]jiadeo[.]cc
- bonanza[.]keerc[.]cc
- bvavos[.]com
- bvvee[.]com
- bvveee[.]com
- cjmaelall[.]com
- cjmall02[.]com
- cjmall03[.]com
- cjmalls001[.]top
- cjmallsa[.]com
- cjmallso[.]com
- cjmollaw[.]com
- com[.]redirection7[.]com
- coslwao[.]top
- cy888[.]com
- cy888[.]com[.]redirection7[.]com
- cy898[.]com
- cy898[.]com[.]redirection7[.]com
- d3e899b9[.]u[.]fn03[.]vip
- d4ca4cce[.]u[.]fn01[.]vip
- d4ca4cce[.]u[.]fn03[.]vip
- dgbets[.]net
- e5b8bab6[.]n[.]fnvip100[.]com
- ebansd[.]com
- ebasdec[.]com
- ebayma66[.]com
- ebaymall168[.]shop
- ec2-18-167-121-68[.]ap-east-1[.]compute[.]amazonaws[.]com
- ec2-18-183-220-150[.]ap-northeast-1[.]compute[.]amazonaws[.]com
- ec2-3-92-165-57[.]compute-1[.]amazonaws[.]com
- ec2-35-78-206-18[.]ap-northeast-1[.]compute[.]amazonaws[.]com
- emandtt[.]com
- f4901539[.]n[.]fnvip100[.]com
- f6a3980c[.]n[.]fnvip100[.]com
- f8887[.]com
- f8887[.]com[.]redirection7[.]com
- fd13[.]vip
- fd13[.]vip[.]redirection7[.]com
- fd17[.]vip
- fd17[.]vip[.]redirection7[.]com
- fidebit[.]com
- fortuneparadise[.]net

- gd55[.]com[.]redirection7[.]com
- gd66[.]com[.]redirection7[.]com
- girlttl01[.]com
- girlttl02[.]com
- girlttl03[.]com
- gqx4ejsk-u[.]funnull01[.]vip
- gxhxdh[.]cn
- h5050[.]com
- haixingtiyu[.]live
- haixingtiyu[.]tv

Sample String-Connected Domains

- fn03[.]arab
- fn03[.]ca
- fn03[.]cn
- fn03[.]com
- fn03[.]com[.]ph
- fn03[.]com[.]ws
- fn03[.]fr
- fn03[.]icu
- fn03[.]info
- fn03[.]lat
- fn03[.]net
- fn03[.]nl
- fn03[.]nom[.]za
- fn03[.]org[.]ph
- fn03[.]org[.]ws
- fn03[.]top
- fn03[.]vg
- fn03[.]ws
- fn03[.]xyz
- funnull[.]ai
- funnull[.]app
- funnull[.]asia
- funnull[.]biz
- funnull[.]blog
- funnull[.]buzz
- funnull[.]camp
- funnull[.]cc
- funnull[.]center
- funnull[.]cloud
- funnull[.]club
- funnull[.]co
- funnull[.]com
- funnull[.]company
- funnull[.]cool
- funnull[.]email
- funnull[.]expert
- funnull[.]fun
- funnull[.]games
- funnull[.]guru
- funnull[.]host
- funnull[.]info
- funnull[.]io
- funnull[.]live
- funnull[.]me
- funnull[.]mobi
- funnull[.]net
- funnull[.]online
- funnull[.]org
- funnull[.]ph
- funnull[.]pro

Sample String-Connected Subdomains

- 12abb97f[.]u[.]fn01[.]vip
- 12abb97f[.]u[.]fn02[.]vip
- aldo[.]00[.]int[.]ad[.]smartnews[.]net
- aldo[.]10yuankaihutiyanjin-okta-network-metrics-s3p-net[.]hiltonbusinessonline[.]com
- aldo[.]addev[.]git[.]keturah[.]org
- aldo[.]admin[.]accs[.]farm

- aldo[.]admin[.]cloud[.]openloyalty[.]io
- aldo[.]admin[.]csagdev[.]cz
- aldo[.]ai[.]trouble-free[.]net
- aldo[.]and[.]co[.]free[.]fr
- aldo[.]api-feature[.]rev[.]com
- aldo[.]api[.]sociaplus[.]com
- aldo[.]api[.]useinsider[.]com
- aldo[.]apollo[.]sirclo[.]net
- aldo[.]apps[.]lair[.]io
- aldo[.]area[.]pi[.]cnr[.]it
- aldo[.]atl[.]jelastic[.]vps-host[.]net
- aldo[.]axtest[.]zumper[.]org
- aldo[.]bank[.]apitree[.]cz
- aldo[.]barsyonline[.]co[.]com[.]au
- aldo[.]barsyonline[.]co[.]de
- aldo[.]barsyonline[.]co[.]xyz
- aldo[.]bayarea[.]purpleoakrealty[.]com
- aldo[.]bg[.]aldo[.]pro
- aldo[.]bignals[.]pagesperso-orange[.]fr
- aldo[.]biomec[.]ior[.]it
- aldo[.]bnhm[.]berkeley[.]edu
- aldo[.]bomentio[.]ru[.]com
- aldo[.]buyer[.]zackyyofficial[.]my[.]id
- aldo[.]cc[.]71501[.]425762[.]byxmqjjf[.]com
- aldo[.]cialdem2[.]dev2[.]magenio[.]com
- aldo[.]client[.]cloud[.]openloyalty[.]io
- aldo[.]cloud[.]interhostsolutions[.]be
- aldo[.]cloud[.]mattermost[.]com
- aldo[.]co[.]th[.]integration-5ojmyuq-lal7qr7da772o[.]ap-3[.]magentosite[.]cloud
- aldo[.]co[.]th[.]integration3-b5sbmty-lal7qr7da772o[.]ap-3[.]magentosite[.]cloud
- aldo[.]co[.]th[.]master-7rqtwti-lal7qr7da772o[.]ap-3[.]magentosite[.]cloud
- aldo[.]co[.]th[.]production-vohbr3y-lal7qr7da772o[.]ap-3[.]magentosite[.]cloud
- aldo[.]cognome[.]rivcash[.]com
- aldo[.]com[.]br[.]admin-eu[.]cas[.]ms
- aldo[.]com[.]br[.]admin-eu2[.]cas[.]ms
- aldo[.]com[.]br[.]admin-mcas[.]ms
- aldo[.]com[.]br[.]admin-us[.]cas[.]ms
- aldo[.]com[.]br[.]admin-us2[.]cas[.]ms
- aldo[.]com[.]br[.]admin-us3[.]cas[.]ms
- aldo[.]com[.]br[.]eu[.]cas[.]ms
- aldo[.]com[.]br[.]eu2[.]cas[.]ms
- aldo[.]com[.]br[.]hotsited[.]com
- aldo[.]com[.]br[.]mcas[.]ms
- aldo[.]com[.]br[.]multi[.]uribl[.]com
- aldo[.]com[.]br[.]us[.]cas[.]ms
- aldo[.]com[.]br[.]us2[.]cas[.]ms
- aldo[.]com[.]br[.]us3[.]cas[.]ms
- aldo[.]com[.]br[.]websiteoutlook[.]com
- aldo[.]configuration[.]azure-api[.]net
- aldo[.]corgiat[.]cerdinamo[.]it
- aldo[.]corgiat[.]somset[.]it
- aldo[.]crescini[.]free[.]fr
- aldo[.]cust[.]dev[.]thingdust[.]io
- aldo[.]cust[.]disrec[.]thingdust[.]io
- aldo[.]daineyet[.]ru[.]com
- aldo[.]data[.]azure-api[.]net
- aldo[.]dccreative[.]a2hosted[.]com
- aldo[.]dde[.]ufv[.]br
- aldo[.]demo[.]taction[.]in
- aldo[.]dev[.]agti[.]eng[.]br
- aldo[.]dev[.]livebay[.]it
- aldo[.]dev[.]summasolutions[.]net
- aldo[.]dev[.]warnerbros[.]com
- aldo[.]dev2[.]magenio[.]com
- aldo[.]developer[.]azure-api[.]net

- aldo[.]direct[.]quickconnect[.]to
- aldo[.]dombosco[.]eadrj[.]com
- aldo[.]dryrun[.]kineo[.]com
- aldo[.]dssp[.]unisa[.]it
- aldo[.]dyn[.]ddnss[.]de
- aldo[.]else[.]admin[.]web-8[.]hiltonbusinessonline[.]com
- aldo[.]else[.]buenomini[.]org[.]pl
- aldo[.]else[.]daura[.]ch
- aldo[.]else[.]echosign[.]com
- aldo[.]else[.]eu[.]org
- aldo[.]else[.]fallguys-mobile[.]com
- aldo[.]else[.]fallguys[.]global
- aldo[.]else[.]fallguys2[.]com
- aldo[.]else[.]fallguys3d[.]com
- aldo[.]else[.]fallguysmobile[.]com
- aldo[.]else[.]fallguysmusic[.]net
- aldo[.]else[.]fallguystwo[.]com
- aldo[.]else[.]fallguysultimateknockout[.]com
- aldo[.]else[.]fortnite[.]com
- aldo[.]else[.]foulplaygame[.]com
- aldo[.]else[.]freshnow[.]biz
- aldo[.]else[.]giro[.]priv[.]at
- aldo[.]else[.]joghurtschnitte[.]pl
- aldo[.]else[.]jogurt-slice[.]com
- aldo[.]else[.]kinderbuenowhite[.]pl
- aldo[.]else[.]kinderjoyroadshowzabawanacalego[.]eu
- aldo[.]else[.]kinderpanchlodek[.]com[.]pl
- aldo[.]else[.]maxichillout[.]com[.]pl
- aldo[.]else[.]natflix[.]ca