WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Unlocking the DNS Strongbox of BADBOX 2.0

Table of Contents

Executive Report

HUMAN's Satori Threat Intelligence and Research Team recently uncovered and partially disrupted BADBOX 2.0 in collaboration with Google, Trend Micro, Shadowserver, and other partners. The threat has been dubbed "the largest botnet of infected connected TV (CTV) devices" uncovered to date.

BADBOX 2.0-infected devices become part of a huge botnet involved in programmatic ad and click fraud; residential proxy service, account takeover (ATO), and distributed denial-of-service (DDoS) attacks; fake account creation; malware distribution; and one-time password (OTP) theft. As of the report's publishing, the threat has affected more than 1 million consumer devices.

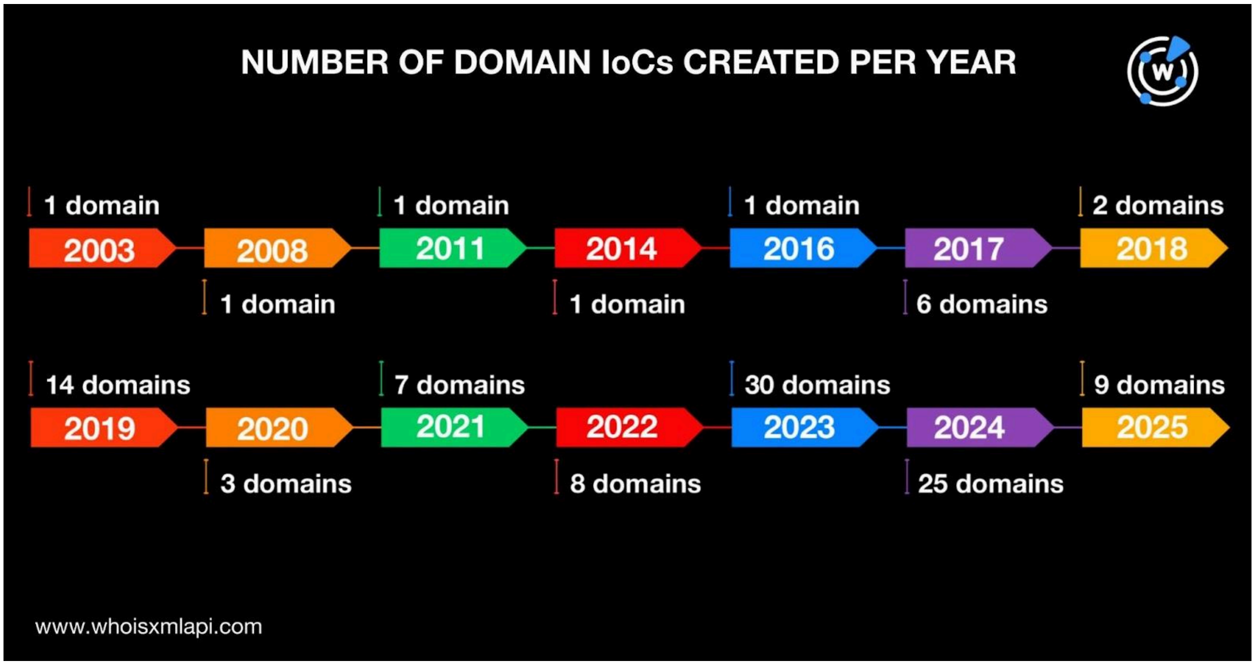
The researchers identified 109 command-and-control (C&C) domains as indicators of compromise (IoCs), which WhoisXML API analyzed and expanded. Our DNS investigation led to the discovery of:

- 915 email-connected domains, eight of which turned out to be malicious
- 50 IP addresses, 34 of which have already been weaponized for attacks
- 211 IP-connected domains
- 2,078 string-connected domains, two of which have already been associated with threats

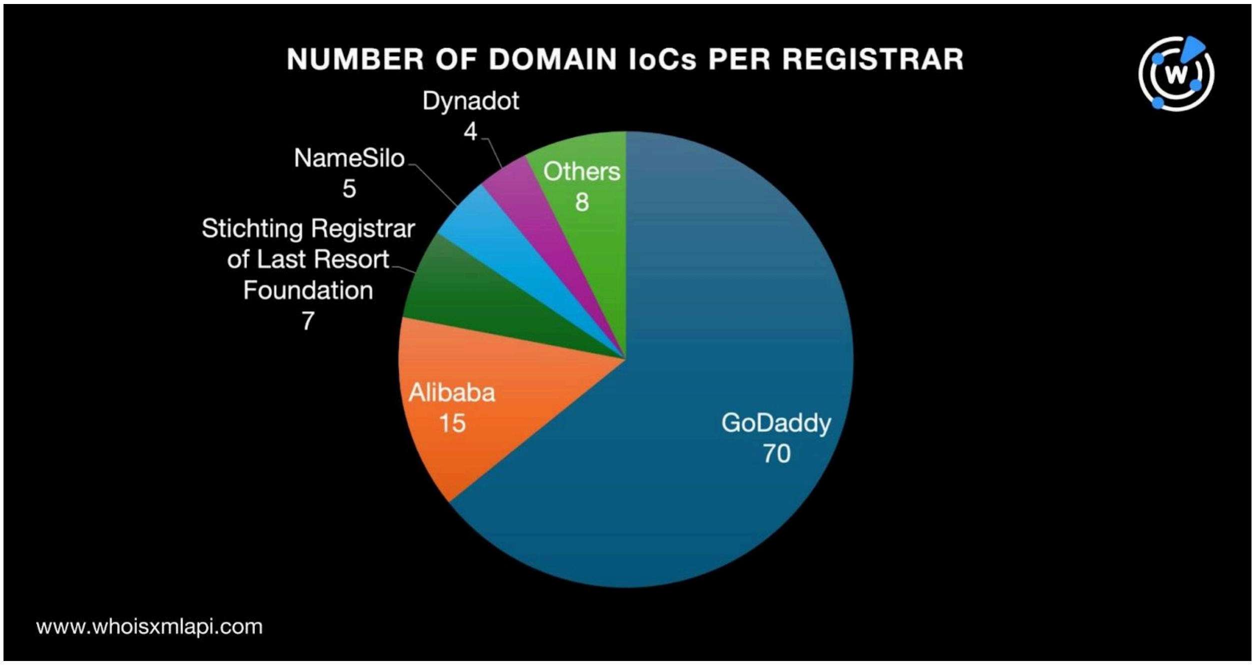
A Closer Look at the BADBOX 2.0 IoCs

We kicked off our DNS deep dive by looking into the WHOIS records of the 109 domains tagged as IoCs and found that they all had current WHOIS information based on the results of our Bulk WHOIS API query. We also discovered that:

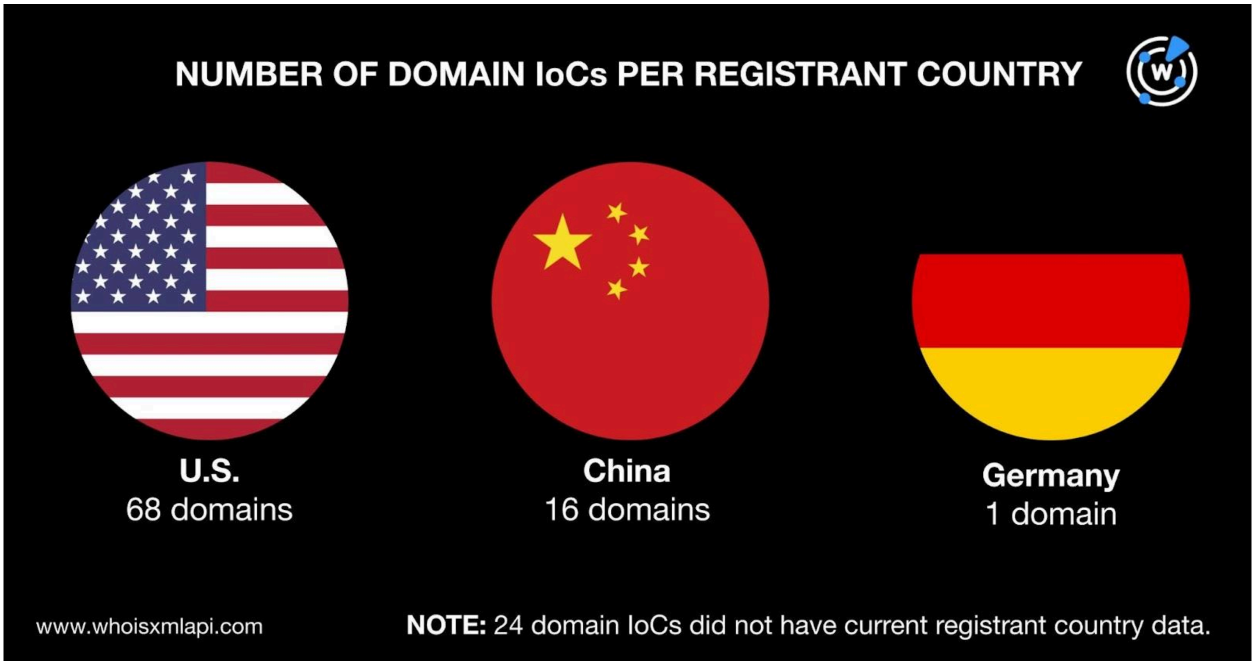
- The 109 domains were created between 2003 and 2025. Specifically, 30 were created in 2023; 25 in 2024; 14 in 2019; nine in 2025; eight in 2022; seven in 2021; six in 2017; three in 2020; two in 2018; and one each in 2003, 2008, 2011, 2014, and 2016.



- The 109 domains were administered by 11 registrars led by GoDaddy, which accounted for 70 of them. Alibaba came in second place with 15 domains. Stichting Registrar of Last Resort Foundation took the third spot with seven domains. NameSilo placed fourth with five domains, followed by Dynadot with four. Cloudflare and Name.com accounted for two domains each. Finally, one domain each was administered by 1API, DNSPod, Gname, and Internet Domain Service.



- Only 85 of the 109 domains had registrant countries on record. They were registered in three countries topped by the U.S., which accounted for 68 domains. China took the second spot with 16 domains. One domain was registered in Germany. Finally, 24 domains did not have registrant countries in their current WHOIS records.



We also queried the 109 domains identified as IoCs on DNS Chronicle API and discovered that 105 had historical domain-to-IP address resolutions. Four of them (i.e., duoduodev[.]com, flyermobi[.]com, motiyu[.]net, and qazwsxedc[.]xyz) posted the oldest resolution date—4 October 2019.

Inside BADBOX 2.0's DNS Strongbox

Our search for more artifacts began with a WHOIS History API query for the 109 domains tagged as IoCs. We found that 61 of them had 101 email addresses in their historical WHOIS records after duplicates were filtered out. Upon closer examination, 45 of the email addresses were public.

Next, we queried the 45 public email addresses on Reverse WHOIS API and discovered that 44 of them appeared in the historical WHOIS records of several domains. A total of 19 public email addresses, however, could belong to domainers (given the large number of connected domains) so they were excluded from further analysis. That said, the 25 email addresses left on our list appeared in the current WHOIS records of 915 domains after those already identified as IoCs and duplicates were filtered out.

We then performed a Threat Intelligence API query for the 915 email-connected domains and found that eight have already been associated with various threats. Take a look at three examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT
fifeaccounts[.]com	Malware distribution
glennborne[.]com	Malware distribution
musicforcause[.]com	Malware distribution

A DNS Lookup API query for the 109 domains identified as IoCs came next. We found that 52 of them resolved to 50 unique IP addresses.

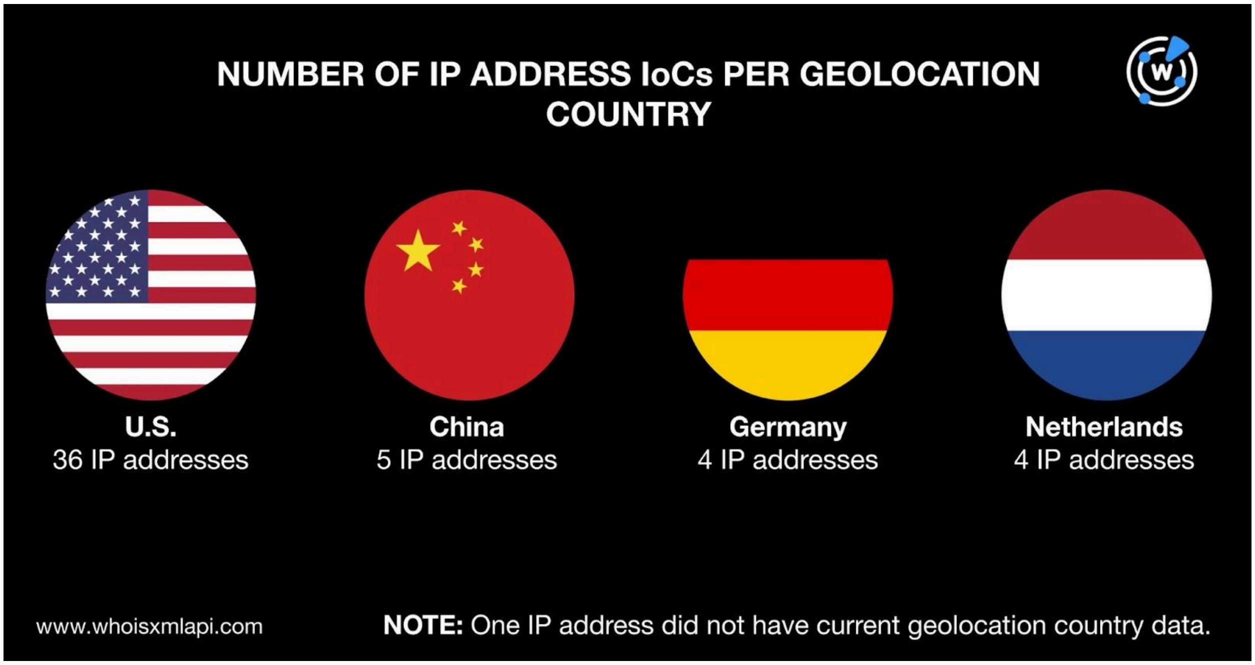
We queried the 50 IP addresses on Threat Intelligence API and discovered that 34 have already been classified as malicious. The following table shows five examples.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT
104[.]21[.]112[.]1	Attack C&C

	Generic threat Malware distribution Phishing Suspicious activity
3[.]33[.]130[.]190	Attack C&C Generic threat Malware distribution Phishing Suspicious activity
5[.]79[.]71[.]205	C&C Generic threat Malware distribution
69[.]16[.]230[.]165	Attack C&C Generic threat Malware distribution Phishing Suspicious activity
76[.]223[.]67[.]189	Attack C&C Generic threat Malware distribution Phishing Suspicious activity

Next, we queried the 50 IP addresses on Bulk IP Geolocation Lookup and found that only 49 had geolocation countries and ISPs on record. Specifically:

- The 49 IP addresses were geolocated in four countries led by the U.S., which accounted for 36 IP addresses. China took the second spot with five IP addresses. Germany and the Netherlands placed third with four IP addresses each. Finally, one did not have a geolocation country on record.



NUMBER OF IP ADDRESS IoCs PER GEOLOCATION COUNTRY

U.S.
36 IP addresses

China
5 IP addresses

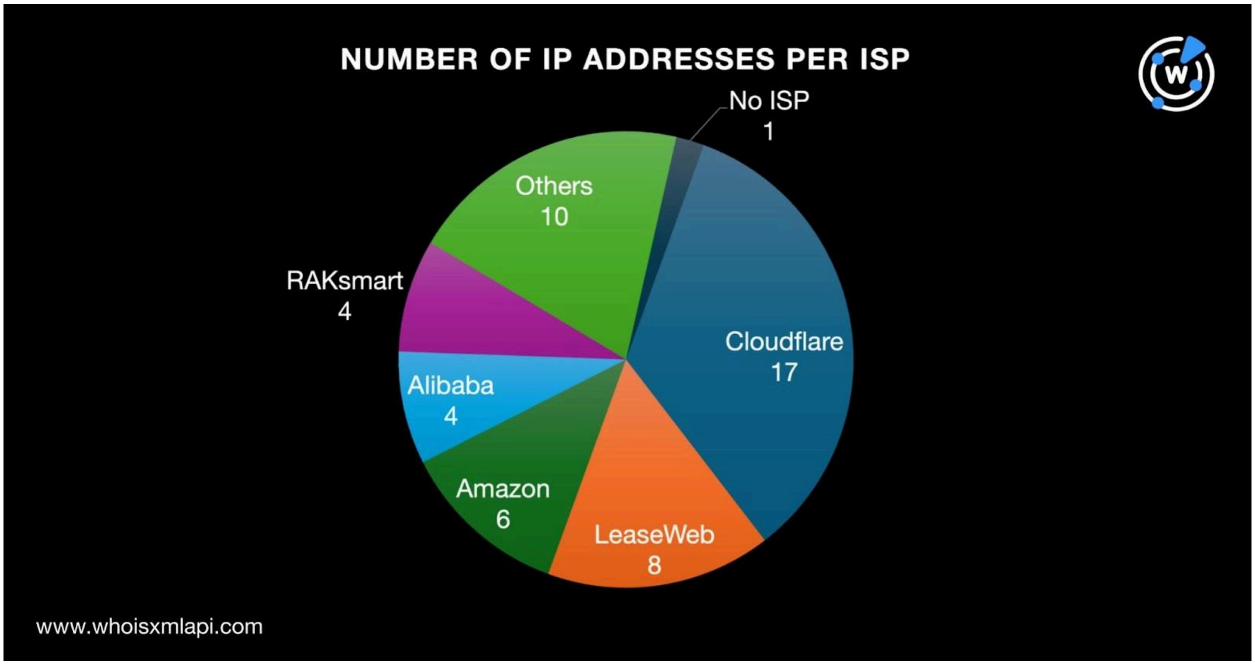
Germany
4 IP addresses

Netherlands
4 IP addresses

www.whoisxmlapi.com

NOTE: One IP address did not have current geolocation country data.

- The 49 IP addresses were split among 13 ISPs topped by Cloudflare, which accounted for 17 IP addresses. LeaseWeb placed second with eight IP addresses. Amazon took the third spot with six. Alibaba and RAKsmart administered four IP addresses each. Google and Zenlayer accounted for two IP addresses each. One IP address each was administered by DigitalOcean, FDCServers.net, Linode, Liquid Web, The Constant Company, and VPSOR-Global. Finally, one IP address did not have an ISP on record.



NUMBER OF IP ADDRESSES PER ISP

www.whoisxmlapi.com

A Reverse IP API query for the 50 IP addresses showed that 49 had active IP address-to-domain resolutions. Only 15 IP addresses could likely support dedicated infrastructure and were good for further analysis. They hosted 211 domains after duplicates, those already tagged as IoCs, and the email-connected domains were filtered out.

Next, closer scrutiny of the 109 domains identified as IoCs revealed that they contained 104 unique text strings. We queried the 104 strings on Domains & Subdomains Discovery and found that only the 71 listed below appeared in other domains.

- 99soya.
- ad3g.
- admoyu.
- ai-goal.
- apotube.
- astrolink.
- bluefish.
- catmore88.
- catmos99.
- cbphe.
- clickby.
- coslogdydy.
- cxlcyy.
- cxzyr.
- dazzl.
- dqmop.
- duoduodev.
- easyjoy.
- echojoy.
- finemob.
- firehub.
- flyermobi.
- g1ee.
- giddy.
- goologer.
- heygames.
- huuww.
- ipforyou.
- ipmoyu.
- jasmine.
- jolted.
- jutux.
- long.
- meiboot.
- meisvip.
- moonhub.
- motiyu.
- moyix.
- moyu88.
- msohu.
- mtcprogram.
- mymoyu.
- navnow.
- net-goal.
- pccyy.
- pcxrl.
- pixelscast.
- pixlo.
- qazwsxedc.
- randomhow.
- shanhulan.
- simplekds.
- soyatea.
- sparkjoy.
- sustat.
- swiftcode.
- sysbinder.
- tuding.
- veezy.
- vividweb.

- vmud.
- ycxad.
- ycxrl.
- yeyeyeye.
- yxcrl.
- yydsma.
- yydsmb.
- yydsmd.
- ziyemy.
- ztword.
- zxcvbnmasdfghjkl.

The 71 text strings particularly appeared in 2,078 domains after duplicates, those already tagged as IoCs, and the email- and IP-connected domains were filtered out.

A Threat Intelligence API query for the 2,078 string-connected domains showed that two—dazzl[.]ink and qazwsxedc[.]tech—have already been tied to generic threats, malware distribution, and phishing.

—

Our IoC list expansion analysis for BADBOX 2.0 led to the discovery of 3,254 additional artifacts comprising 915 email-connected domains, 50 IP addresses, 211 IP-connected domains, and 2,078 string-connected domains. We also discovered that 44 of these artifacts, specifically 10 domains and 34 IP addresses, have already figured in various cyber attacks.

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

- 028123[.]com
- 0769jiudianjiaju[.]info
- 0buxiugangcanju[.]com
- aacxb[.]xyz
- abba[.]me
- adaptorx[.]com
- b1abber[.]com
- b4ngkok[.]com
- b4rcelona[.]net
- c1oaked[.]com
- c21propertymogul[.]com
- c4ncun[.]com
- d4[.]com[.]cn
- d4llas[.]com
- dadona[.]net
- e-devletgirisi[.]org
- e1ectrician[.]com
- e1ectricians[.]com
- f-ing[.]net
- f-ing[.]org
- f1ab[.]com
- g0sh[.]com
- gameonline[.]club
- gameonline[.]pro
- h-fun[.]com
- h0ttie[.]com
- h0tty[.]com
- i3nc[.]nyc
- iajtc[.]xyz
- ichexun[.]com
- jddyq[.]xyz
- jea1ous[.]com
- jea1ousy[.]com
- kaonai[.]com
- kepti[.]xyz
- kewwf[.]xyz
- l4ndon[.]com
- l4svegas[.]com
- laann[.]xyz
- m4drid[.]com
- m4nhattan[.]com
- m4rbella[.]com
- n4shville[.]com
- n4ssau[.]com
- n4wyorkcity[.]com
- oco[.]com[.]cn
- oidjm[.]xyz
- oleed[.]xyz
- p00ch[.]com
- p1ayed[.]com
- p1umber[.]com
- q3[.]cn
- qarant[.]pro
- qilbz[.]xyz
- rack[.]click
- re1ief[.]com
- realrealmccoy[.]com
- s1ide[.]com
- s1lver[.]com
- s4les[.]net
- t4mpa[.]com
- taduino[.]com
- tanmoxi[.]com
- u9[.]com[.]cn
- ubdmw[.]xyz
- ubestbuyprice[.]com
- v4cation[.]com
- v4cations[.]com
- v4lue[.]com
- w4shdc[.]com
- w4shingtondc[.]com
- wai[.]com[.]cn

- xadee[.]xyz
- xavierzhu[.]top
- xiaow[.]com
- ye11[.]org
- yearofthedomino[.]com
- yearofthedomino[.]net
- zavvi[.]net
- zcvvr[.]xyz
- zeeboard[.]com

Sample IP Addresses

- 103[.]133[.]179[.]219
- 104[.]21[.]112[.]1
- 127[.]0[.]0[.]1
- 128[.]14[.]153[.]82
- 13[.]248[.]213[.]45
- 137[.]175[.]27[.]19
- 149[.]248[.]1[.]23
- 15[.]197[.]148[.]33
- 161[.]35[.]229[.]239
- 172[.]105[.]156[.]15
- 178[.]162[.]203[.]202
- 192[.]74[.]237[.]135
- 23[.]237[.]233[.]171
- 3[.]33[.]130[.]190
- 34[.]132[.]102[.]6
- 38[.]177[.]196[.]242
- 39[.]96[.]197[.]79
- 42[.]96[.]169[.]232
- 5[.]79[.]71[.]205
- 52[.]41[.]176[.]125
- 54[.]85[.]87[.]184
- 59[.]110[.]19[.]6
- 69[.]16[.]230[.]165
- 76[.]223[.]67[.]189
- 8[.]210[.]106[.]113
- 85[.]17[.]31[.]122

Sample IP-Connected Domains

- 3gallery[.]biz
- admin[.]wildpettykiwi[.]xyz
- b1qn[.]cn
- config[.]wildpettykiwi[.]xyz
- dashboard[.]petrel-ip[.]com
- en[.]ipmoyu[.]com
- fantasyoriginsg[.]com
- gamesla[.]xyz
- h5fun[.]xyz
- informati[.]xyz
- johnandaudrey[.]at
- keep[.]proximocentauri[.]com
- la[.]firehub[.]work
- mail[.]equitytrustcrunion[.]com
- nglmqw[.]cn
- passivhaus-links[.]at
- q5j4[.]cn
- res[.]wildpettykiwi[.]info
- smtp[.]envsilver[.]com
- tengseo[.]cn
- ucgrow[.]com
- vemedi[.]com
- webdisk[.]moyix[.]cn

Sample String-Connected Domains

- 99soya[.]com
- ad3g[.]cn
- ad3g[.]it
- ad3g[.]net[.]ws

- ai-goal[.]cn
- apotube[.]de
- apotube[.]dk
- apotube[.]net
- astrolink[.]ai
- astrolink[.]app
- astrolink[.]biz
- bluefish[.]academy
- bluefish[.]ad
- bluefish[.]ae
- catmore88[.]ph
- catmore88[.]ws
- catmos99[.]ph
- catmos99[.]ws
- cbphe[.]loan
- clickby[.]ca
- clickby[.]click
- clickby[.]club
- coslogdydy[.]ws
- cxlcyy[.]ws
- cxzyr[.]cn
- dazzl[.]ai
- dazzl[.]app
- dazzl[.]au
- dqmop[.]icu
- dqmop[.]tk
- duoduodev[.]club
- easyjoy[.]be
- easyjoy[.]cloud
- easyjoy[.]club
- finemob[.]tk
- firehub[.]ae
- firehub[.]ai
- firehub[.]app
- flyermobi[.]ph
- g1ee[.]fm
- g1ee[.]net[.]au
- g1ee[.]ph
- giddy[.]agency
- giddy[.]ai
- giddy[.]app
- goologer[.]ph
- heygames[.]cn
- heygames[.]co
- heygames[.]com
- huuww[.]loan
- ipforyou[.]com
- ipforyou[.]com[.]br
- ipforyou[.]ru
- ipmoyu[.]net
- ipmoyu[.]top
- jasmine[.]ac[.]cn
- jasmine[.]academy
- jasmine[.]ae
- jolted[.]accountant
- jolted[.]agency
- jolted[.]app
- jutux[.]com
- jutux[.]com[.]cn
- jutux[.]info
- long[.]abudhabi
- long[.]ac
- long[.]ac[.]cn
- meiboot[.]ph
- meiboot[.]ws
- meisvip[.]cn
- meisvip[.]net
- moonhub[.]ai
- moonhub[.]app
- moonhub[.]be
- moyix[.]net
- moyix[.]store
- moyix[.]top
- moyu88[.]cn
- moyu88[.]com
- moyu88[.]tk
- msohu[.]cn
- msohu[.]com
- msohu[.]ga
- mtcprogram[.]org

- mymoyu[.]cn
- mymoyu[.]com
- mymoyu[.]top
- navnow[.]app
- navnow[.]co[.]uk
- navnow[.]com
- net-goal[.]hk
- pccyy[.]cn
- pccyy[.]loan
- pcxrl[.]cn
- pcxrl[.]win
- pixelscast[.]ph
- pixlo[.]ai
- pixlo[.]cf
- pixlo[.]ch
- qazwsxedc[.]app
- qazwsxedc[.]asia
- qazwsxedc[.]at
- randomhow[.]to
- shanhulan[.]com
- simplekds[.]app
- simplekds[.]com
- simplekds[.]vip
- soyatea[.]com
- sparkjoy[.]africa
- sparkjoy[.]ai
- sparkjoy[.]app
- sustat[.]date
- sustat[.]shop
- sustat[.]win
- swiftcode[.]ai
- swiftcode[.]app
- swiftcode[.]be
- sysbinder[.]info
- tuding[.]app
- tuding[.]art
- tuding[.]bid
- veezy[.]africa
- veezy[.]app
- veezy[.]ca
- vividweb[.]agency
- vividweb[.]co
- vividweb[.]co[.]kr
- vmud[.]aquila[.]it
- vmud[.]buzz
- vmud[.]cc
- ycxad[.]cn
- ycxad[.]ws
- ycxrl[.]net
- ycxrl[.]ph
- ycxrl[.]wang
- yeyeyeye[.]cf
- yeyeyeye[.]click
- yeyeyeye[.]club
- yxcrl[.]cn
- yxcrl[.]tk
- yydsma[.]net
- yydsmb[.]loan
- yydsmb[.]ltd
- yydsmd[.]ph
- yydsmd[.]ws
- ziyemy[.]com
- ziyemy[.]xyz
- ztword[.]cn
- zxcvbnmasdfghjkl[.]cn
- zxcvbnmasdfghjkl[.]com
- zxcvbnmasdfghjkl[.]info