DNS Deep Dive: Peeking into Back Doors to Abandoned but Live Backdoors

Table of Contents

Executive Report

watchTowr Labs investigated thousands of abandoned but live backdoors installed on various compromised sites to determine what data the original backdoor owners have stolen. They published their findings in "Backdooring Your Backdoors—Another $20 Domain, More Governments" and, in the process, identified 34 domains as indicators of compromise (IoCs).

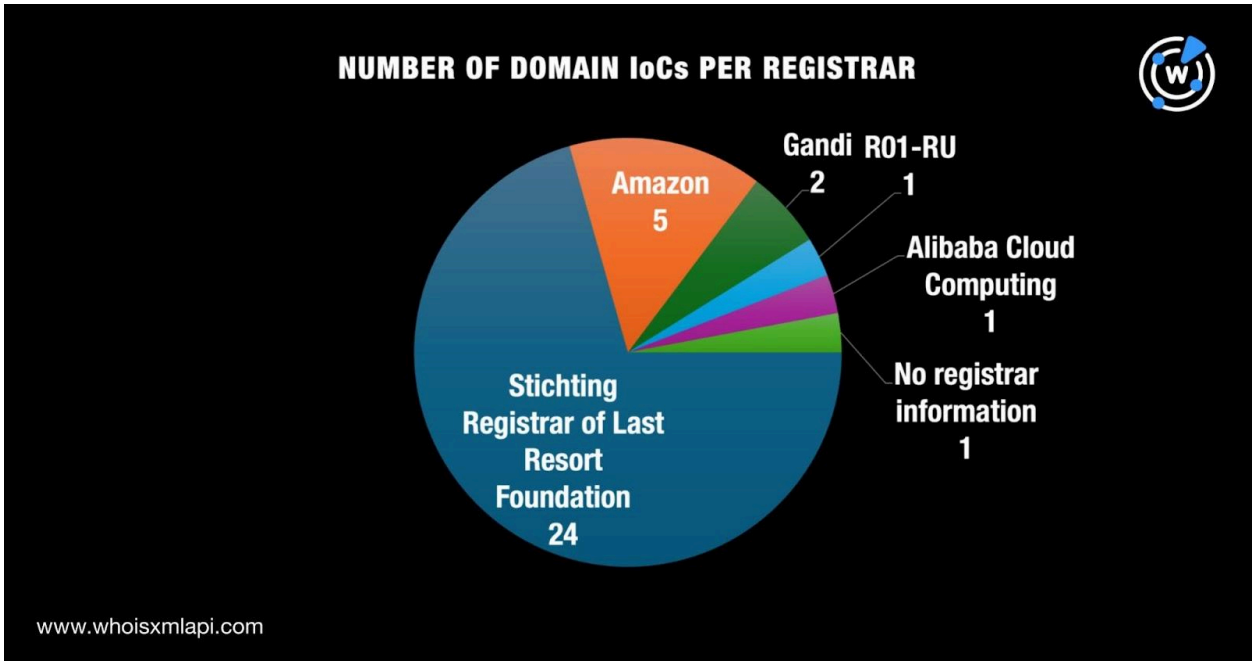
The WhoisXML API research team expanded the list of IoCs through a DNS deep dive and uncovered:

- 498 email-connected domains
- 10 IP addresses, eight of which turned out to be malicious
- 192 IP-connected domains
- 666 string-connected domains

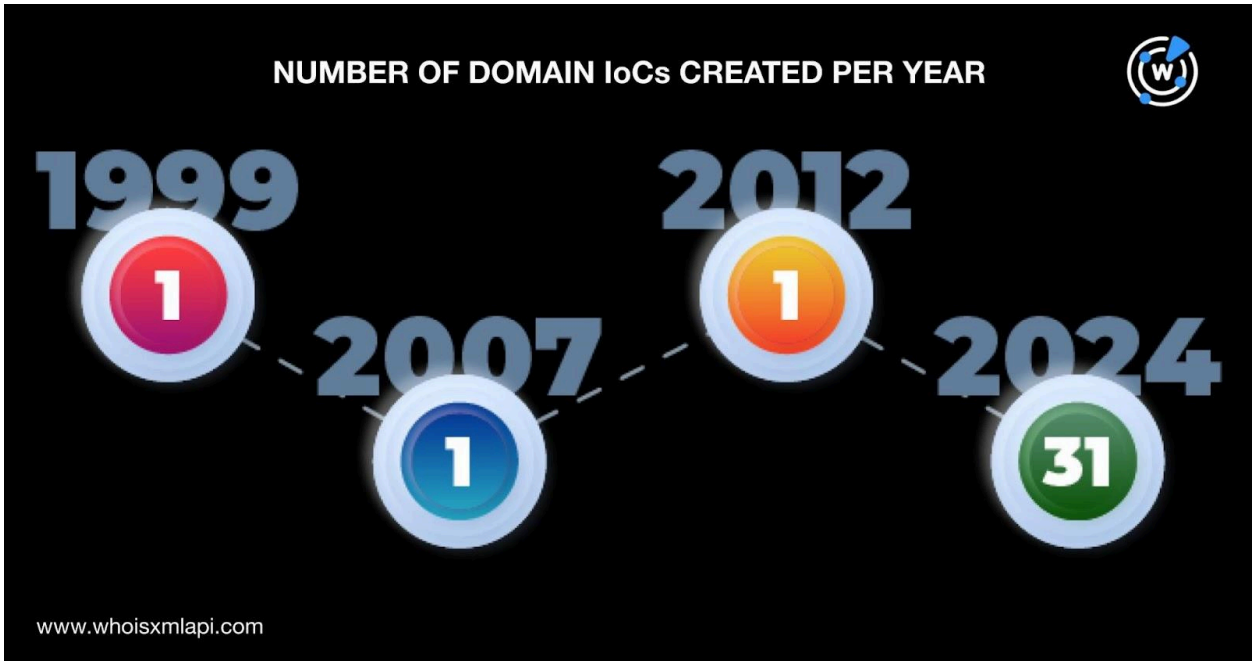
A Closer Look at the IoCs

Before diving into the IoC list expansion, we looked more closely at the 34 domains tagged as IoCs first. We began by querying them on Bulk WHOIS API and found that all of them had current WHOIS records. Here are our findings.

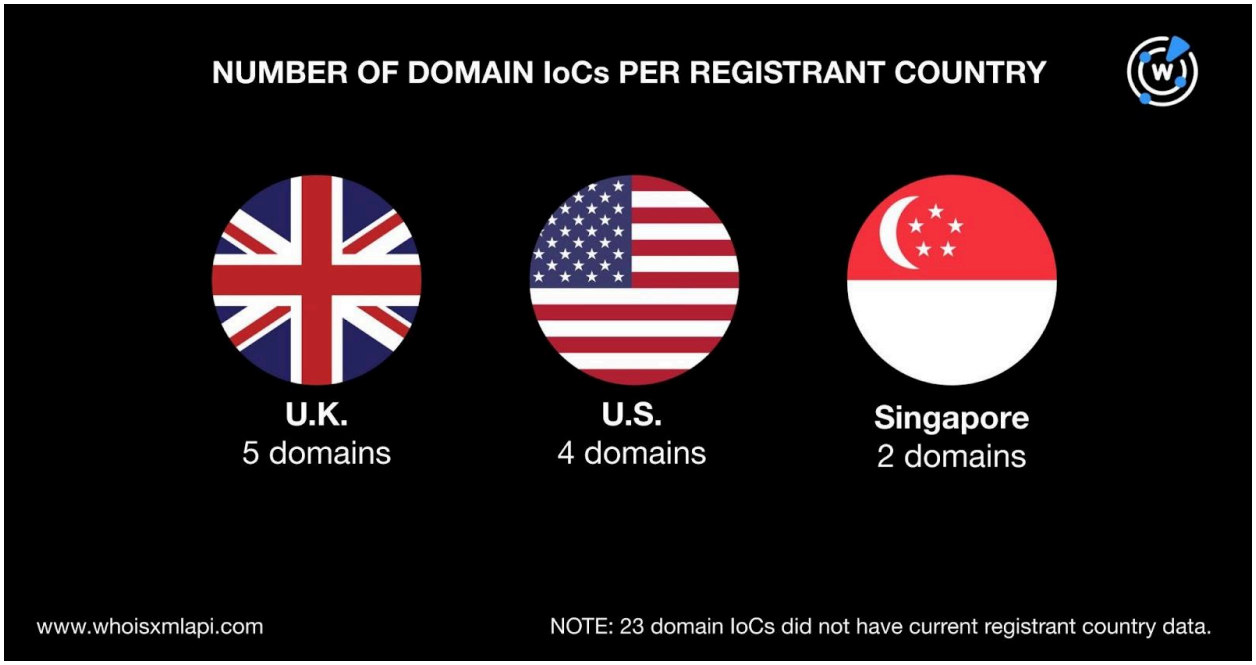
- A majority of the domain IoCs, 24 to be exact, were administered by Stichting Registrar of Last Resort Foundation. Amazon took second place, accounting for five of the total domain IoC volume. Gandi administered two domain IoCs, while R01-RU and Alibaba Cloud Computing accounted for one each. Finally, one domain IoC did not have registrar information in its current WHOIS record.



- They were created between 1999 and 2024. Specifically, 31 domain IoCs were created in 2024 while one each was created in 1999, 2007, and 2012.



- Only 11 of them had registrant country data in their current WHOIS records. Of these, five were registered in the U.K., four in the U.S., and two in Singapore.



Next, we queried the 34 domains tagged as IoCs on DNS Chronicle API and found that they had 518 IP address resolutions over time. Ccteam[.]ru recorded the oldest IP resolution date—9 October 2019. Take a look at the DNS histories of five other domain IoCs below.

DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST RESOLUTION DATE
csthis[.]com	22	20 October 2019
h4cks[.]in	3	5 September 2024
imhabirligi[.]com	22	13 October 2019
odayexp[.]com	23	29 September 2021
w2img[.]com	22	14 November 2019

Expanding the List of IoCs

Our search for possibly connected artifacts began with a WHOIS History API query for the 34 domains tagged as IoCs. We found that their historical records contained 168 email addresses after duplicates were removed. Of these, 65 turned out to be public email addresses.

Next, we queried the 65 public email addresses on Reverse WHOIS API and discovered that 33 of them appeared in the current WHOIS records of other domains. However, 15 of the 33 public

email addresses present in other domains' current WHOIS records could belong to domainers so they were excluded from further investigation.

The 18 public email addresses left on our list appeared in the current WHOIS records of 498 email-connected domains after duplicates and those already identified as IoCs were filtered out.

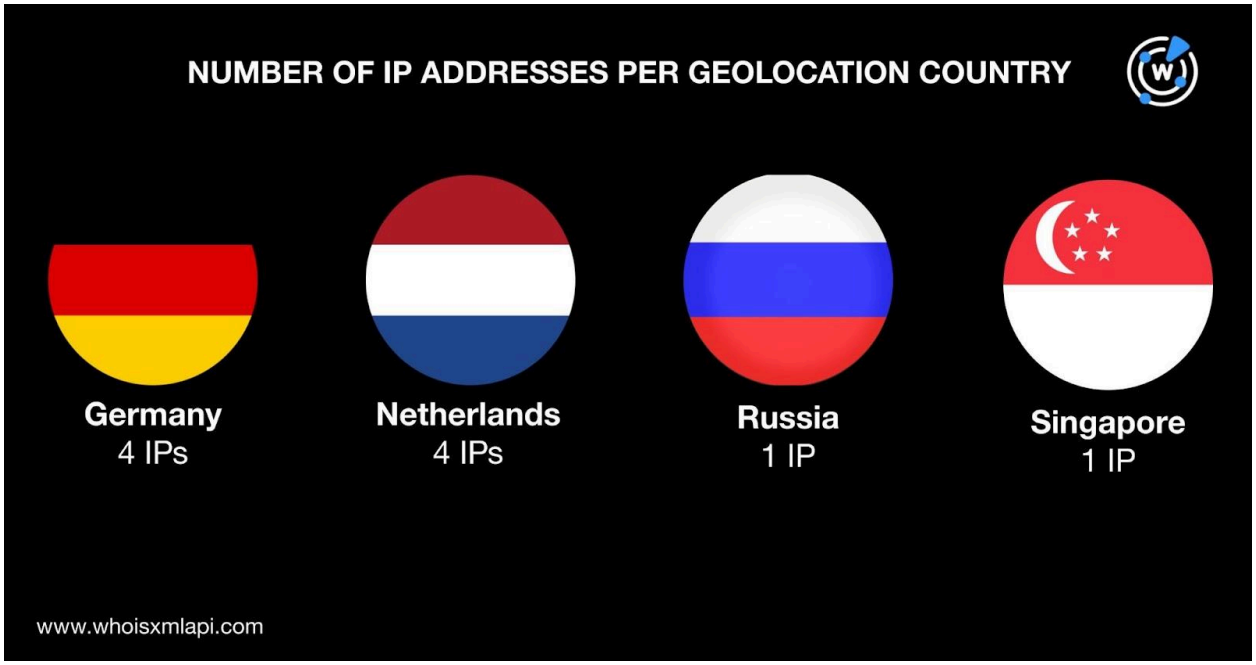
We then queried the 34 domains tagged as IoCs on DNS Lookup API and found that 32 of them actively resolved to 10 unique IP addresses after duplicates were filtered out.

A Threat Intelligence API query for the 10 IP addresses showed that eight of them have already been weaponized for various attacks. Here are three examples.

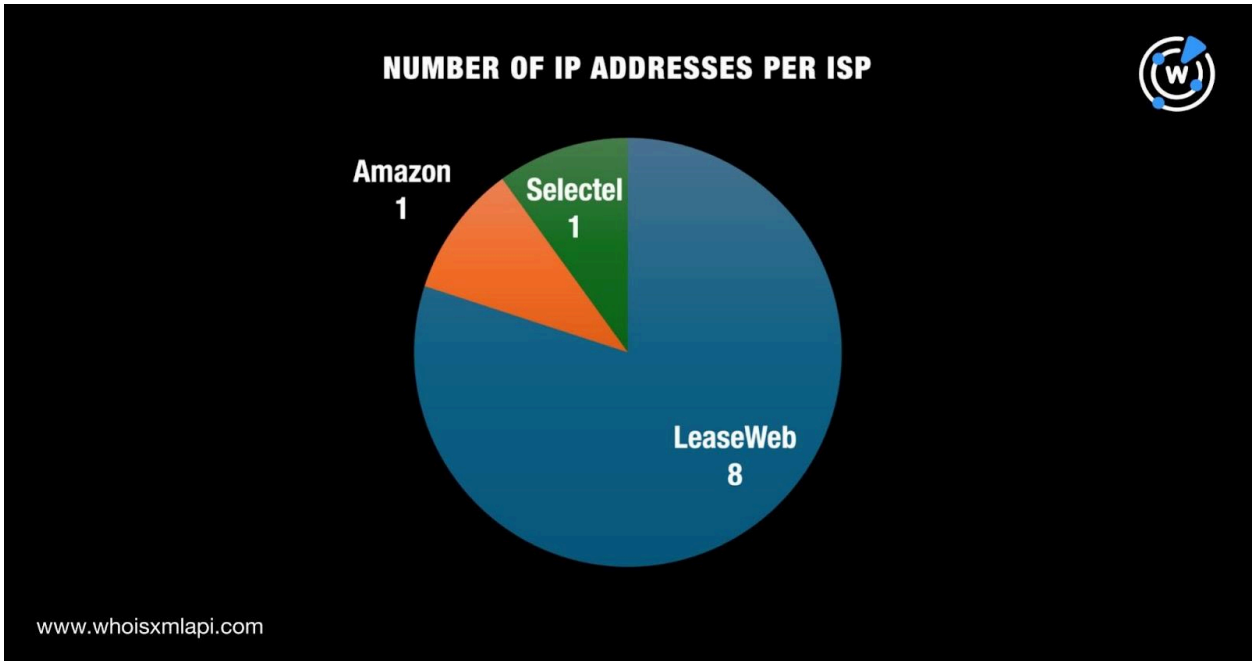
MALICIOUS IP ADDRESS	ASSOCIATED THREATS
178[.]162[.]203[.]202	Command and control (C&C) Generic threats Malware distribution
5[.]79[.]71[.]205	C&C Generic threats Malware distribution
85[.]17[.]31[.]122	C&C Generic threats Malware distribution

Next, a Bulk IP Geolocation Lookup query for the 10 IP addresses revealed that:

- They were geolocated in four countries. Specifically, four IP addresses each originated from Germany and the Netherlands, while one each hailed from Russia and Singapore.



- They were spread across three ISPs led by LeaseWeb, which accounted for eight IP addresses. One IP address each was administered by Amazon and Selectel.



We then queried the 10 IP addresses on Reverse IP API and found that altogether, they hosted at least 2,624 domains. Two of them could also be dedicated hosts. These two IP addresses

hosted 192 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

Lastly, we scoured the DNS for domains containing the same text strings found in the 34 domains tagged as IoCs using Domains & Subdomains Discovery. The results revealed that these 18 text strings had connections:

- aljazeera7.
- ccteam.
- ciscosoft.
- csthis.
- dcvi.
- emp3ror.
- flyphoto.
- h4cks.
- hackru.
- imhabirligi.
- localshell.
- lpl38.
- precision-gaming.
- rootshell-security.
- shellci.
- templatez.
- void.
- yywjw.

The 18 text strings above appeared in 666 string-connected domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

—

Our in-depth analysis of the 34 domains identified as IoCs in relation to the featured campaign led to the discovery of 1,366 potentially connected threat artifacts. Altogether, we uncovered 498 email-connected domains, 10 IP addresses, 192 IP-connected domains, and 666 string-connected domains. It is also worth noting that eight of these connected artifacts have already figured in various malicious campaigns.

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 Artifacts

- 00849[.]com[.]cn
- 0086bj[.]com[.]cn
- 0535ad[.]cn
- 21746[.]com[.]cn
- 517ts[.]cn
- bestautojobs[.]info
- betwixttheknits[.]com
- bjbtel[.]com
- bjcqc01[.]net
- bljwhbsc[.]com
- boisbande[.]org
- botocms[.]com
- branscome-inc[.]com
- bring-mir-den-burger[.]com
- bvwkyzj[.]com
- c-medina[.]info
- caipiaonu[.]cn
- cao3b9w4[.]com
- carolcostaauthor[.]com
- cbooffsite[.]com
- cbscuttack[.]org
- ccoo-sanostra[.]com
- cdzhcc[.]com
- chengxiangchaishao[.]com
- chericouture[.]com
- chinahuijin[.]net
- chinamianxi[.]com
- chonglangv[.]com
- christina-hiroshima[.]com
- chuangdianpp[.]com
- chuangxinex[.]com
- chunqiubas[.]com
- cingenieros[.]com
- citiesoftomorrow-me[.]com
- clgmc[.]com
- crsmats[.]com
- csmingtai[.]com
- ctbkc[.]com
- cyywy[.]com
- cztiesen[.]com
- dadikushop[.]com
- danzhaohn[.]com
- devsemahadev[.]org
- dfqssc[.]com
- dianmei[.]cn
- dianshouwang[.]com
- divistyles[.]com
- diyarbakirescort[.]work
- dlworldgo[.]com
- donc88[.]com
- donghecun[.]com
- donghuobi[.]cn
- donglaile[.]com
- dsn[.]cn
- duoduoxinfang[.]com
- dzfty[.]com
- e3youth[.]net
- e8casino[.]top
- edy[.]systems
- egfgg[.]com
- eyicao[.]com
- facoshop[.]com
- fantasticbooklist[.]com
- faytou[.]com
- feiyubox[.]com
- feng-shui-realestate[.]com
- fexexpresscourier[.]com
- ff6601[.]cn
- ff6602[.]cn
- ff6603[.]cn
- ff6604[.]cn
- ff6605[.]cn

- ff6606[.]cn
- ff6607[.]cn
- ff6608[.]cn
- ff6609[.]cn
- ff6610[.]cn
- fjlanfeng[.]com
- flexiblepackaging[.]biz
- fortune00[.]net
- fpv-drone-racing[.]com
- frannycoop[.]com
- fttianyi[.]com
- futurespaceonline[.]com
- fvy1[.]com
- fzasda[.]com
- g--t[.]com
- g-shock-mens-watches[.]com
- gaacx[.]com
- gaacy[.]com
- gaaeb[.]com
- gaaek[.]com
- gaaew[.]com
- getmojonow[.]com
- gkp[.]cn
- globalcryptrading[.]com
- gnzhongzi[.]com
- godfatherdesigns[.]com
- goodlliving[.]com
- gospelnewsmedia[.]org

Sample IP Addresses

- 13[.]212[.]199[.]188
- 178[.]162[.]203[.]202
- 178[.]162[.]203[.]211
- 178[.]162[.]203[.]226
- 178[.]162[.]217[.]107

Sample IP-Connected Domains

- 3bl[.]ru
- aisedorashop[.]ru
- artiart[.]ru
- attacker[.]ru
- basepicker[.]com
- biocenose[.]ru
- bugcafe[.]3bl[.]ru
- bugcafe[.]ru
- centrnko[.]ru
- chkg[.]ru
- confucianism[.]ru
- copernicus[.]ru
- cpanel[.]caspian-pirates[.]org
- cpanel[.]csthis[.]com
- cpanel[.]dcvi[.]net
- cpanel[.]drakdandy[.]net
- cpanel[.]f4ck[.]org
- cpanel[.]flyphoto[.]us
- cpanel[.]fonts4u[.]org
- cpanel[.]h0ld-up[.]info
- cpanel[.]h4cks[.]in
- cpanel[.]hackru[.]info
- cpanel[.]localshell[.]net
- cpanel[.]templatez[.]org
- cpanel[.]zone-t[.]org
- deception[.]ru
- descartes[.]ru
- duft[.]ru
- ebio[.]ru
- ebon[.]ru
- esoul[.]ru
- f4ck[.]org
- fonts4u[.]org
- ftp[.]caspian-pirates[.]org
- ftp[.]csthis[.]com
- ftp[.]dcvi[.]net

- ftp[.]drakdandy[.]net
- ftp[.]f4ck[.]org
- ftp[.]flyphoto[.]us
- ftp[.]fonts4u[.]org
- ftp[.]h0ld-up[.]info
- ftp[.]h4cks[.]in
- ftp[.]hackru[.]info
- ftp[.]localshell[.]net
- ftp[.]templatez[.]org
- ftp[.]zone-t[.]org
- galaxies[.]ru
- game[.]f4ck[.]org
- glossary[.]ccteam[.]ru
- goldmama[.]ru

Sample String-Connected Domains

- aljazeera7[.]tk
- ccteam[.]at
- ccteam[.]bar
- ccteam[.]be
- ccteam[.]ca
- ccteam[.]cc
- ccteam[.]ch
- ccteam[.]club
- ccteam[.]cn
- ccteam[.]co
- ccteam[.]co[.]uk
- ciscosoft[.]cn
- ciscosoft[.]com
- ciscosoft[.]com[.]br
- ciscosoft[.]net
- csthis[.]pw
- dcvi[.]agency
- dcvi[.]club
- dcvi[.]cn
- dcvi[.]com
- dcvi[.]com[.]br
- dcvi[.]com[.]ph
- dcvi[.]de
- dcvi[.]dk
- dcvi[.]eu
- dcvi[.]fr
- emp3ror[.]ml
- emp3ror[.]pw
- emp3ror[.]tk
- emp3ror[.]xyz
- flyphoto[.]au
- flyphoto[.]bid
- flyphoto[.]biz
- flyphoto[.]ca
- flyphoto[.]cn
- flyphoto[.]co
- flyphoto[.]co[.]kr
- flyphoto[.]co[.]uk
- flyphoto[.]co[.]za
- flyphoto[.]com
- h4cks[.]art
- h4cks[.]cf
- h4cks[.]cn
- h4cks[.]com
- h4cks[.]de
- h4cks[.]eu
- h4cks[.]ga
- h4cks[.]gq
- h4cks[.]icu
- h4cks[.]info
- hackru[.]cf
- hackru[.]com
- hackru[.]net
- hackru[.]nl
- hackru[.]org
- hackru[.]ru
- imhabirligi[.]org
- localshell[.]biz
- localshell[.]com
- lpl38[.]top

- precision-gaming[.]co[.]uk
- precision-gaming[.]de
- precision-gaming[.]net
- precision-gaming[.]org
- precision-gaming[.]rocks
- precision-gaming[.]us
- rootshell-security[.]com
- shellci[.]com
- shellci[.]net
- shellci[.]online
- shellci[.]tk
- templatez[.]app
- templatez[.]bot
- templatez[.]cf
- templatez[.]club
- templatez[.]cn
- templatez[.]co
- templatez[.]co[.]uk
- templatez[.]com
- templatez[.]com[.]br
- templatez[.]com[.]ng
- void[.]ac
- void[.]ac[.]cn
- void[.]ac[.]nz
- void[.]academy
- void[.]ad
- void[.]ae
- void[.]af
- void[.]africa
- void[.]ag
- void[.]agency
- yywjw[.]cn
- yywjw[.]com[.]cn
- yywjw[.]icu
- yywjw[.]loan
- yywjw[.]net
- yywjw[.]top
- yywjw[.]xyz