WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Unearthing DNS Facts about UAT-8099

Threat Report

Table of Contents

Executive Report

WhoisXML API expands Cisco Talos's findings on the new UAT-8099 campaign that has been active since late 2025 to date, identifying additional associated artifacts.

UAT-8099 is a threat actor that has reportedly targeted vulnerable IIS servers across Asia specifically focusing on Thailand and Vietnam. They used web shells and PowerShell to execute scripts and deploy the GotoHTTP tool, granting them remote access to vulnerable IIS servers. They also utilized new BadIIS variants that came hardcoded with their target region, along with customized features for each variant.

Cisco Talos originally identified 17 network IoCs. Upon further scrutiny (i.e., apex domain extraction from subdomains and exclusion of legitimate domains) aided by the WhoisXML API MCP Server, we ended up with and analyzed 27 IoCs comprising 10 domains and 17 subdomains. Our in-depth investigation led to these discoveries:

- Two unique client IP addresses communicated with two domains tagged as IoCs
- Three domains named as IoCs were deemed likely to turn malicious 545–569 days prior to being dubbed as such
- 12,787 email-connected domains, four of which were classified as malicious
- 13 IP addresses, 12 of which were categorized as malicious
- 76 string-connected domains

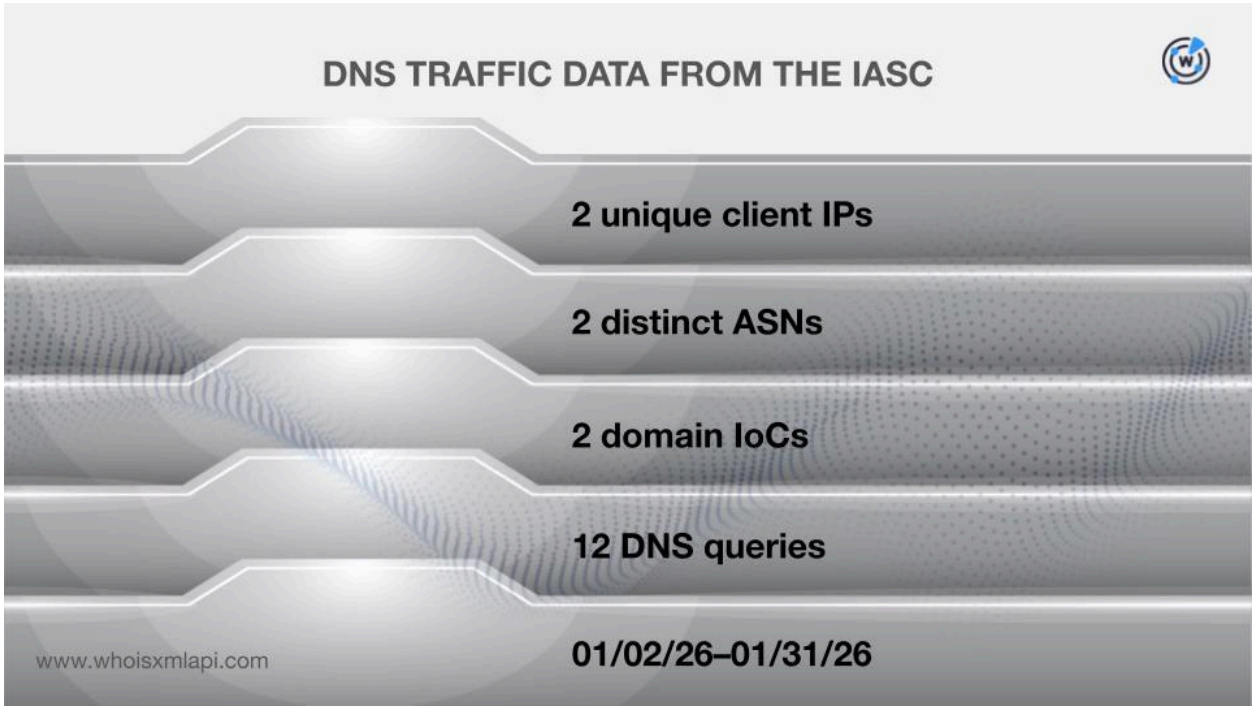
Findings for the Subdomain IoCs

We began our analysis by querying the 17 subdomains identified as IoCs using the WhoisXML API MCP Server.

We discovered that 13 of them fell under recently registered domains, and several consisted of random characters, which is unusual for legitimate websites. Only one, however, merited complete avoidance since it seemed to be mimicking Google, typical of sites designed for phishing campaigns.

More DNS Infrastructure Details about the Domain IoCs

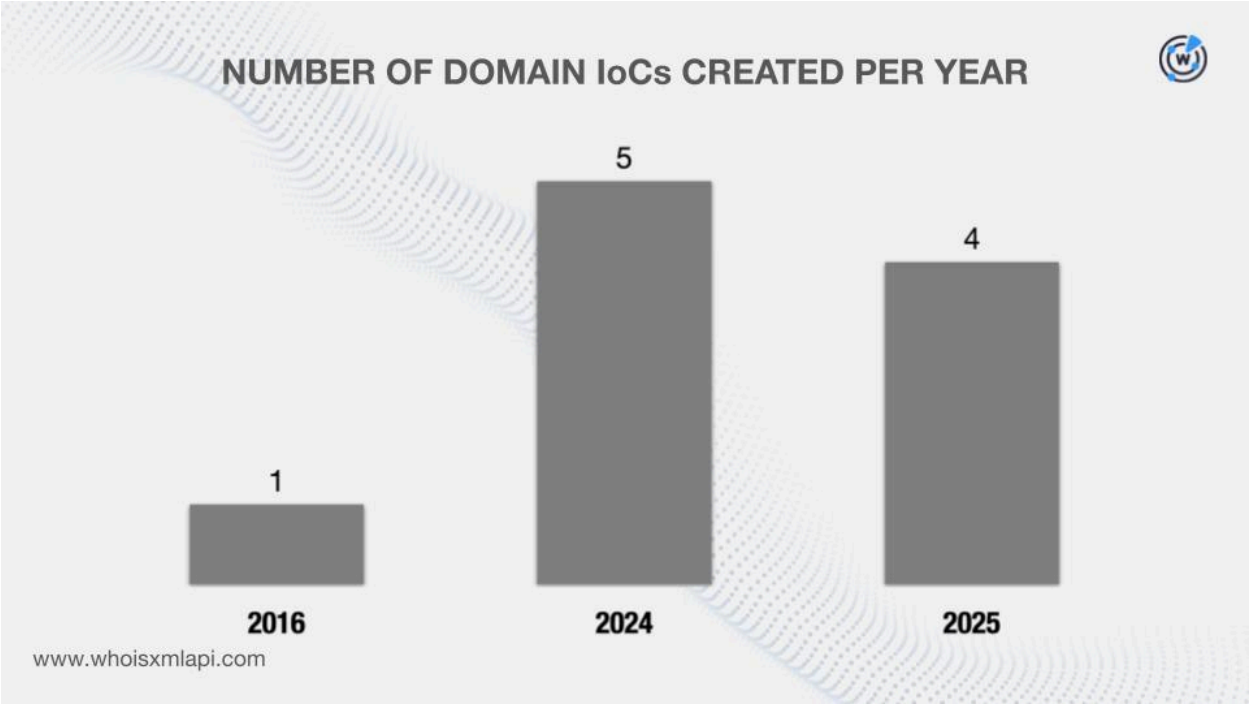
Sample network traffic data from the IASC showed that two unique client IP addresses under two distinct ASNs communicated with two domains identified as IoCs via 12 DNS queries between 2 and 31 January 2026.



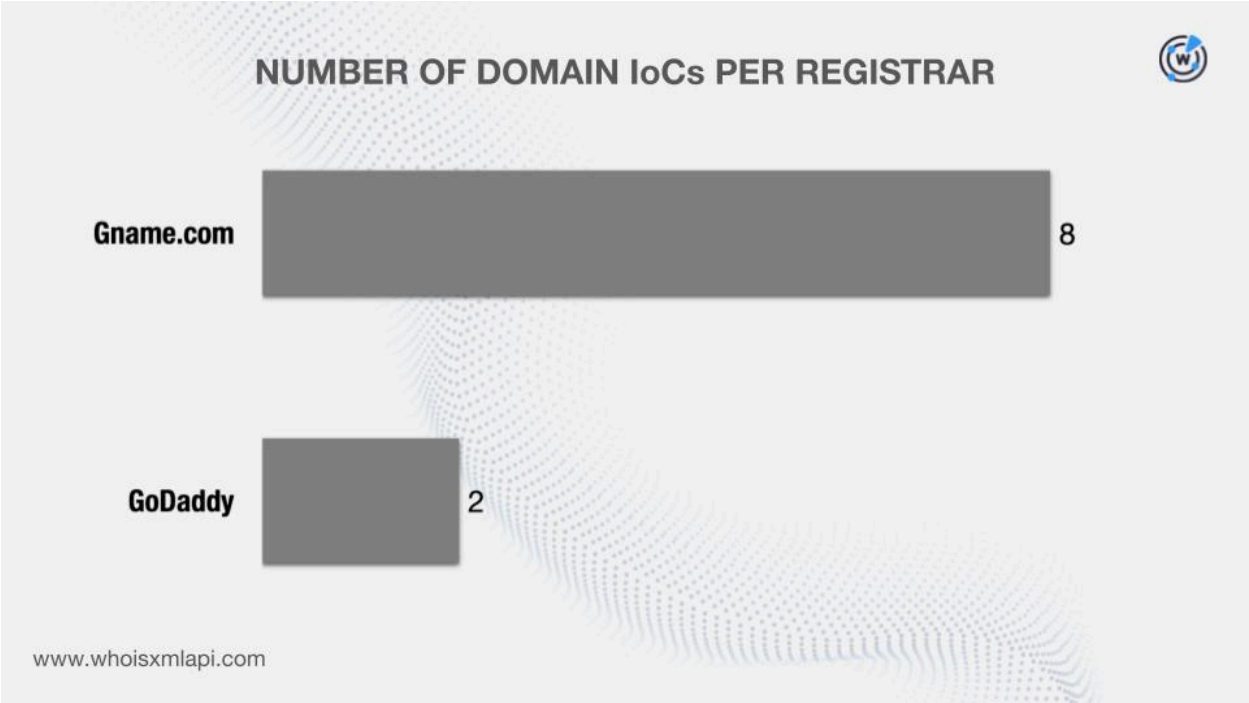
The First Watch Malicious Domains Data Feed revealed that three of the domains tagged as IoCs were deemed likely to turn malicious 545–569 days before they were dubbed as such. An example is the domain gtwql[.]com, which was likely registered with malicious intent 569 days before it was named as an IoC on 29 January 2026.

Next, we queried the 10 domains classified as IoCs on WHOIS API and discovered that:

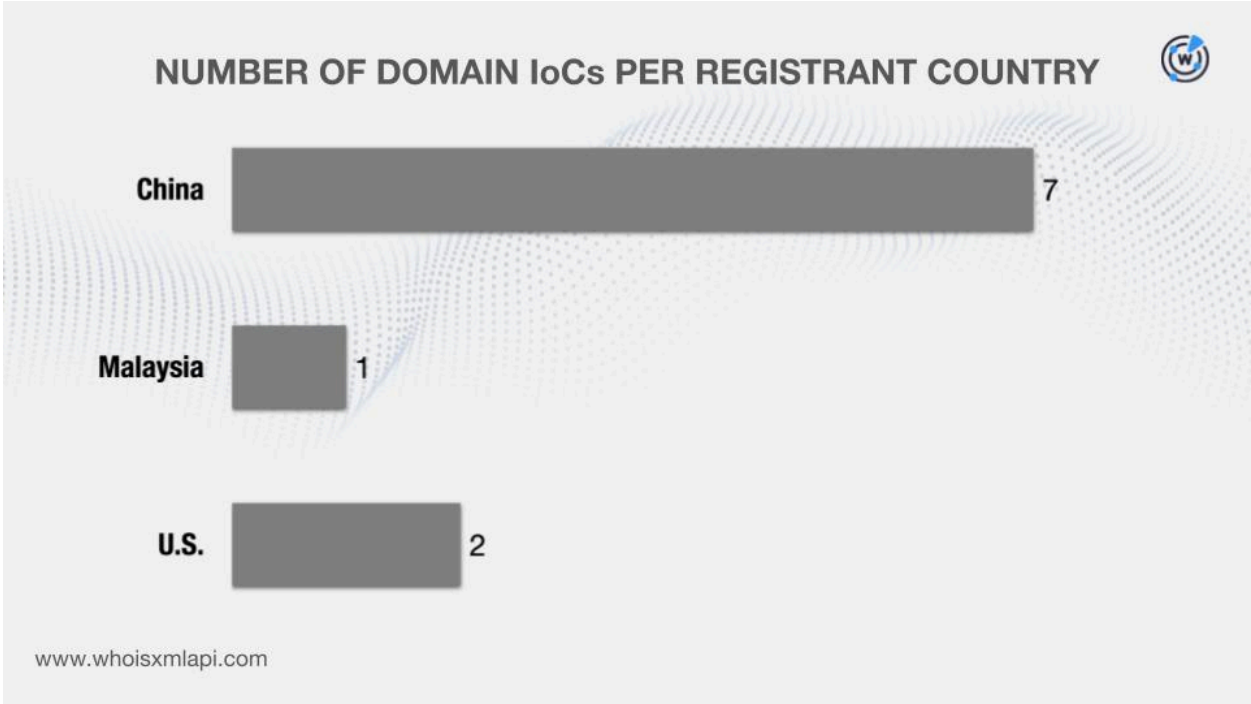
- They were created between 13 May 2016 and 21 July 2025, suggesting that UAT-8099 did not have a specific preference with regard to the age of the domains they weaponized for campaigns.



- They were administered by two registrars.



- They were registered in three different countries.



DNS Chronicle API queries for the 10 domains categorized as IoCs revealed that seven recorded 566 domain-to-IP resolutions over time. Take a look at more details for three examples below.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
ceye[.]io	354	02/26/17	01/30/26
jmfwy[.]com	58	04/29/17	01/27/26
hunanduodao[.]com	36	06/13/22	01/08/26

A closer look at the historical resolutions of the seven domains revealed as IoCs showed that two first posted resolutions in 2017, one in 2022, and four in 2025.

New Artifacts Found for the UAT-8099 Attack

To unearth new artifacts connected to this UAT-8099 campaign, we queried the 10 domains identified as IoCs on WHOIS History API. We found out that three of them had eight unique email addresses in their historical WHOIS records. Upon further scrutiny, seven were public email addresses.

The results of our Reverse WHOIS API queries for the public email addresses revealed that two could belong to domainers. The remaining five public email addresses, meanwhile, led to the discovery of 12,787 unique email-connected domains after those already named as IoCs were filtered out.

Threat Intelligence API queries for the email-connected domains showed that four have already been weaponized for various attacks. An example is dmnsg[.]com, which has already been associated with malware distribution between 9 March 2023 and 30 January 2026.

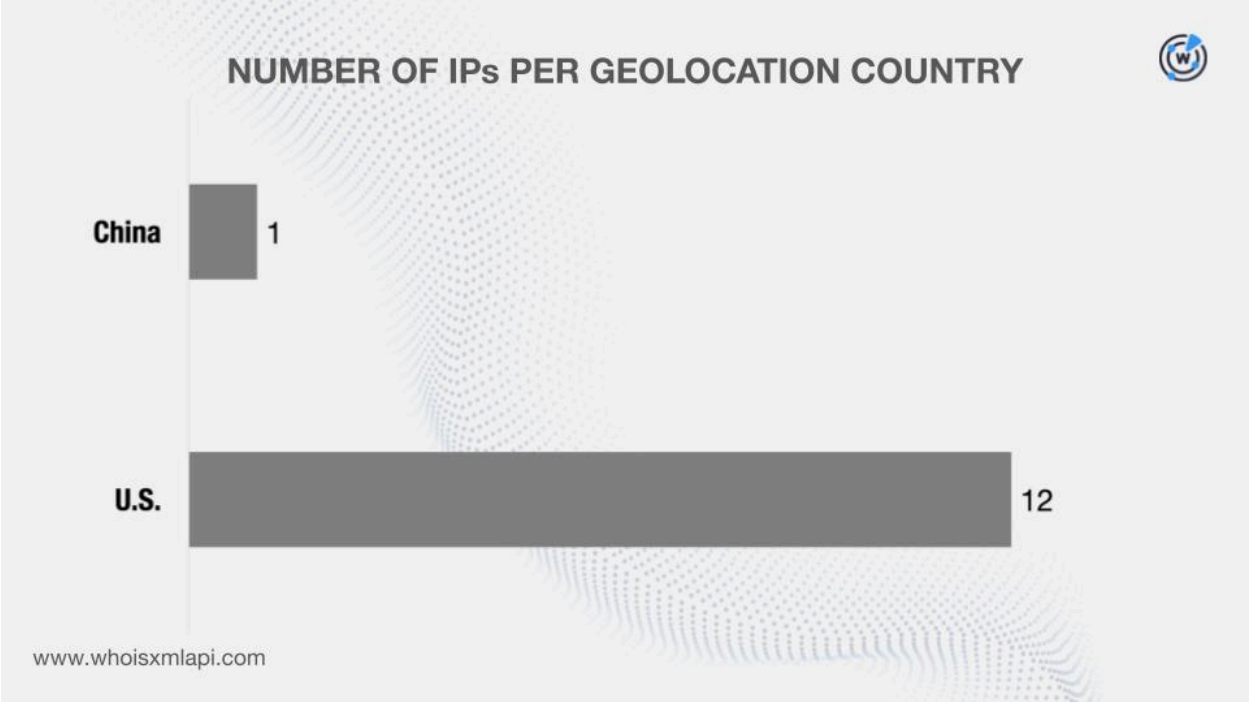
Next, we queried the 10 domains named as IoCs on DNS Lookup API and discovered that seven resolved to 13 unique IP addresses.

The results of our Threat Intelligence API queries for the IP addresses revealed that 12 have already figured in various malicious campaigns. Here are five examples.

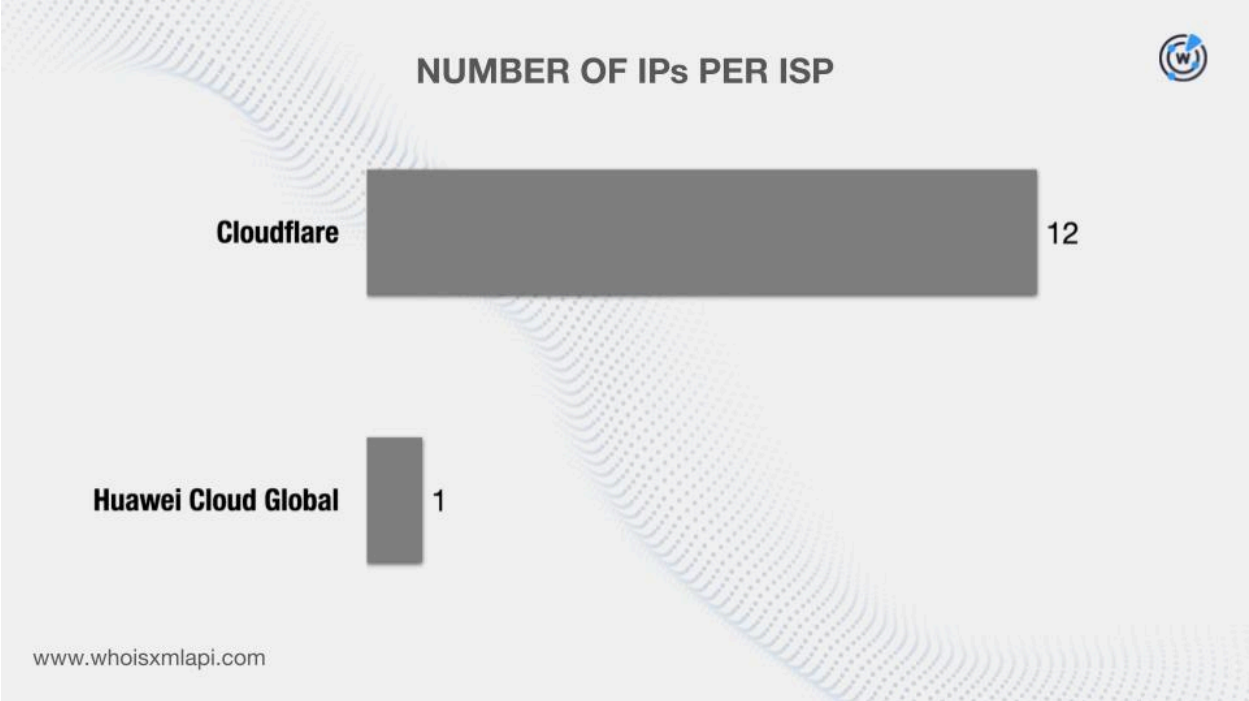
IP ADDRESS	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
104[.]21[.]50[.]194	Phishing Malware distribution Generic threat	03/28/23 10/17/24 04/04/23	01/31/26 01/31/26 11/27/25
104[.]21[.]51[.]85	Malware distribution Phishing Generic threat	05/09/24 07/04/23 12/01/23	01/31/26 01/09/26 11/25/25
104[.]21[.]53[.]75	Malware distribution Generic threat Phishing	12/06/23 04/29/25 03/30/23	01/31/26 11/15/25 11/10/25
104[.]21[.]70[.]225	Suspicious activity Phishing Malware distribution	05/13/25 06/22/24 03/29/23	01/31/26 01/30/26 01/29/26
172[.]67[.]140[.]39	Suspicious activity Phishing Malware distribution	05/13/25 06/22/24 03/29/23	01/31/26 01/30/26 01/29/26

We then sought to find more information on the 13 IP addresses by querying them on Bulk IP Geolocation Lookup and found out that:

- They were geolocated in two countries. Note that both were also on the list of registrant countries.



- They were administered by two ISPs.



Next, we queried the 13 IP addresses on Reverse IP API and discovered that none could be dedicated hosts. That said, we did not find any IP-connected domain.

We then took a closer look at the 10 domains classified as IoCs and identified these eight unique text strings:

- ceye.
- gtwql.
- imxzq.
- jmfwy.
- ohtcm.
- sneaws.
- suucx.
- westooo.

These strings appeared at the start of 76 unique string-connected domains after those already categorized as IoCs and the email-connected domains were filtered out.

The Final Word

Our more detailed analysis of the latest UAT-8099 campaign revealed that two unique client IP addresses communicated with two of the domains identified as IoCs. In addition, three of the domains tagged as IoCs could have been registered with malicious intent from the get-go.

We also uncovered 12,876 new artifacts comprising 12,787 email-connected domains, 13 IP addresses, and 76 string-connected domains. It is also worth noting that 16 of them have already been weaponized for various threats.

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

- 01bc[.]cc
- 02083318888[.]com
- 020autocar[.]com
- a8d1[.]com
- aahelios[.]com
- abeexpo[.]net
- baby-garments[.]com
- bacaiart[.]com
- baihepaper[.]com
- c-zqzk[.]com
- cabrtechsz[.]com
- cabrxm[.]com
- dachengart[.]com
- dafengelec[.]com
- dahexing[.]com
- e-daikudogu[.]com
- eacscm[.]com
- eastoptician[.]com
- fa88888[.]cn
- faeku[.]cn
- fandianjj[.]com
- gaago[.]cn
- gaiche[.]wang
- gairin[.]com
- hai-dian[.]cn
- hailianelectron[.]com
- hainangangqin[.]com
- i-webidea[.]com
- iabcs[.]cn
- iabvua[.]cn
- jazbw91[.]com
- jbasp[.]com
- jbdpx[.]cn
- kabangchem[.]com
- kafyva[.]cn
- kaiertesuoju[.]com
- lamolinamaka[.]cn
- langmeiadv[.]com
- langtingh[.]com
- m-powder[.]com
- ma-shpt[.]com
- maihongtz[.]com
- naixi[.]wang
- namomei[.]net
- nancybarnet[.]com
- oa-huichen[.]com
- oaj158[.]com
- oassqb[.]cn
- paiban[.]wang
- palofoot[.]com
- paogame[.]net
- qarui[.]cn
- qbhgc[.]com
- qbmmlg[.]cn
- rayjingreal[.]com
- rbbdm[.]com
- rbcdm[.]com
- s-bid[.]com
- saclouisvuittonvente[.]com
- sailai-machine[.]com
- tabobosi[.]com
- taglpj[.]com
- taiunji[.]com
- uaaof[.]cn
- udxfv[.]cn
- ueymp[.]cn
- v-topcctv[.]com
- vasentar[.]com
- vffbs[.]cn
- w-ri[.]com
- wagy518[.]com
- wananmachine[.]com
- xaclmy[.]com
- xagdj[.]com

- xalianxiang[.]com
- ya-yuan[.]com
- yahami[.]com
- yahengsteel[.]com
- z-plus-intl[.]com
- zakmmi[.]com
- zanazanv[.]com

Sample IP Addresses

- 104[.]21[.]50[.]194
- 104[.]21[.]51[.]85
- 104[.]21[.]53[.]75
- 104[.]21[.]70[.]225
- 172[.]67[.]140[.]39
- 172[.]67[.]177[.]247

Sample String-Connected Domains

- ceye[.]ai
- ceye[.]app
- ceye[.]bid
- gtwql[.]xyz
- imxzq[.]cn
- jmfwy[.]cn
- jmfwy[.]icu
- ohtcm[.]cn
- ohtcm[.]org[.]au
- ohtcm[.]site
- sneaws[.]bayern
- suucx[.]cn
- suucx[.]shop
- suucx[.]xyz
- westooo[.]ph
- westooo[.]ws