WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

DNS Investigation: Threat Actor TA4922 Goes Global

Threat Report

Table of Contents

Executive Report

TA4922, a highly sophisticated cybercriminal group who rapidly changed tactics and malware, recently used multiple malware, including Atlas RAT, RomulusLoader, SilentRunLoader, and ValleyRAT (Winos4.0), among others, in their campaigns. While they often launched local attacks in nearby regions, they branched out to more countries in Europe and Africa.

Proofpoint published their analysis of the threat and identified seven network IoCs made up of five IP addresses, a domain, and a subdomain in the process. After extracting a unique domain from the subdomain IoC, we collated eight IoCs comprising one subdomain, two domains, and five IP addresses for our own investigation.

Our in-depth IoC investigation led to these discoveries:

- 36 unique IP addresses likely owned by victims that communicated with two of the IP IoCs
- 2,779 email-connected domains, 39 of which were confirmed malicious
- One additional IP address, which was confirmed malicious
- 37 IP-connected domains, 18 of which were confirmed malicious

TA4922 Global Attack Subdomain IoC Study

We began our study by looking more closely at the subdomain IoC.

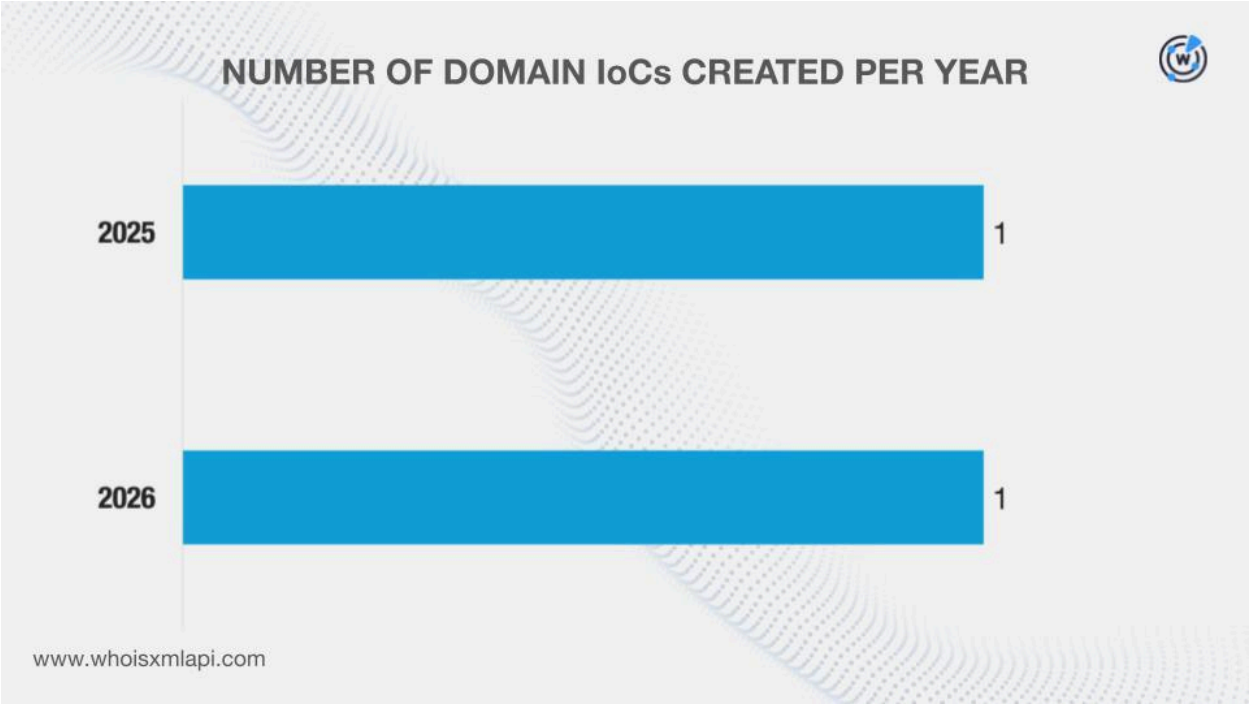
We queried the sole subdomain IoC ws[.]ztts88[.]cyou on the WhoisXML API MCP Server and discovered that its apex domain has the hallmarks of malicious infrastructure, likely a C&C endpoint malware use. Our tools advised users not to visit or interact with it using any browser. And if encountered in logs or traffic, treat any host that contacted it as potentially compromised. Blocking access to it at the DNS or firewall level may also be warranted.

TA4922 Global Attack Domain IoC Deep Dive

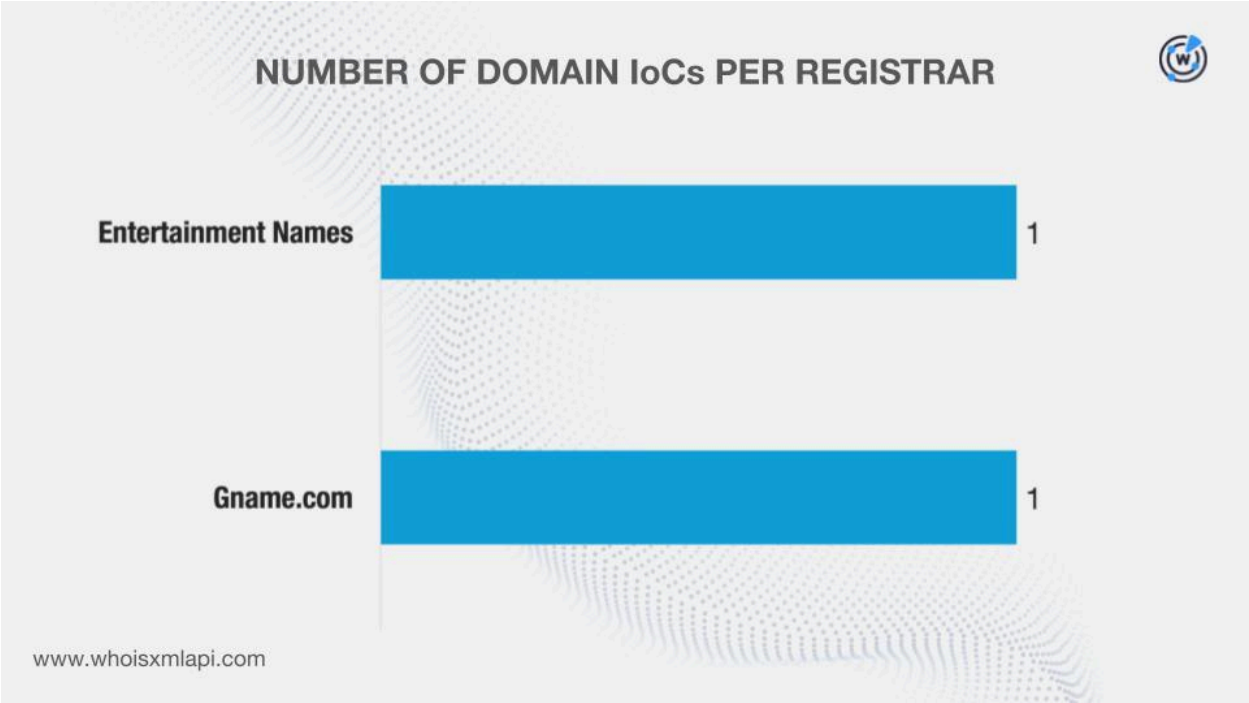
Next, we dove deeper into the two domain IoCs.

First, we queried the domain IoCs on WHOIS API and discovered that:

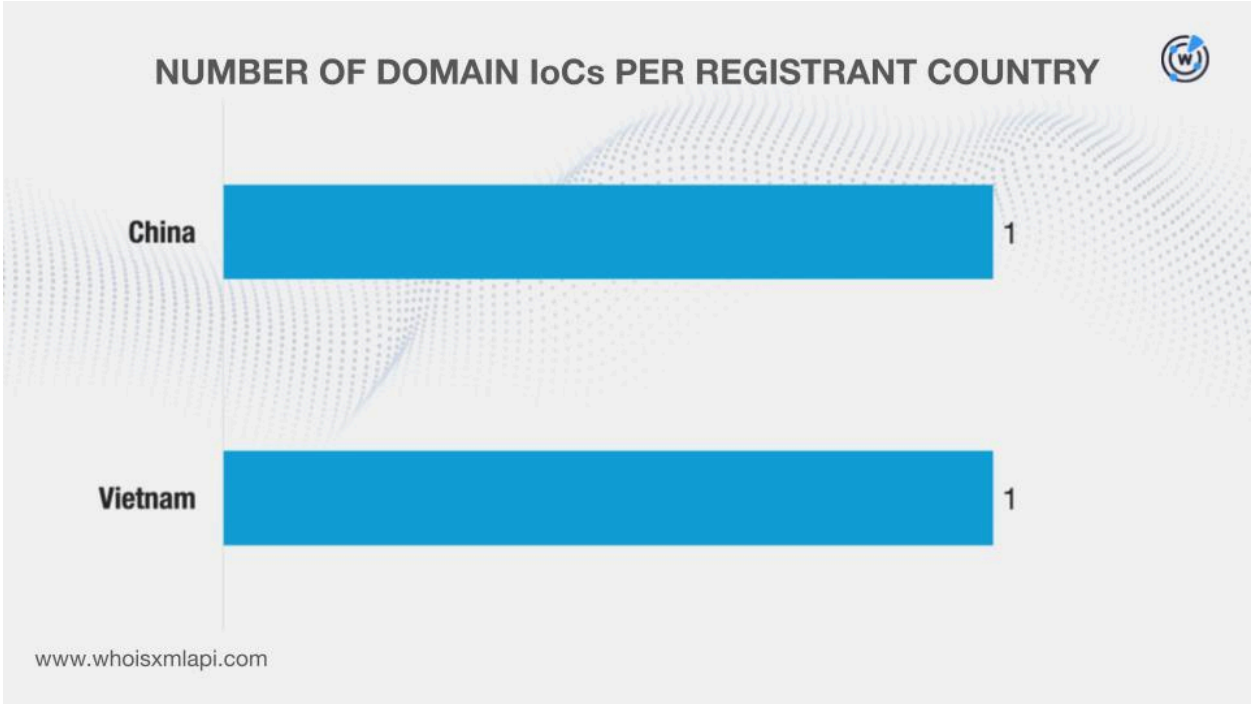
- They were created between 13 June 2025 and 16 March 2026.



- They were administered by different registrars.



- They were also registered in different countries.

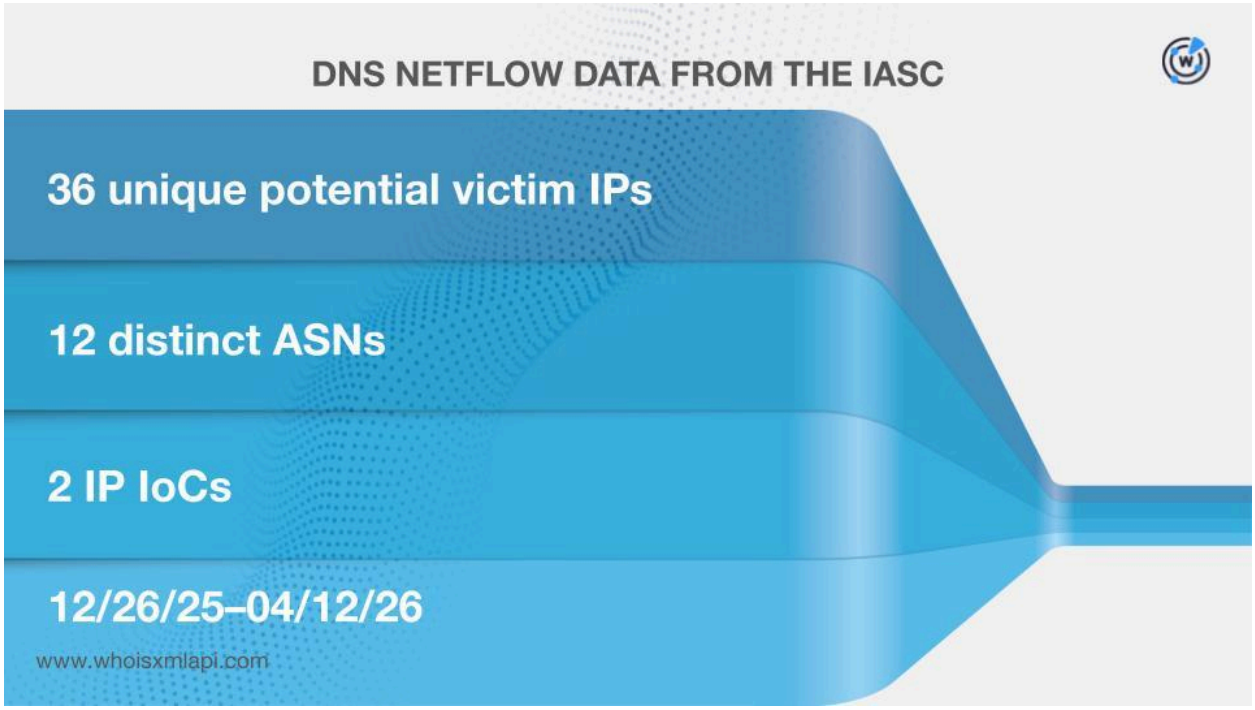


We then queried the domain IoCs on DNS Chronicle API and learned that only one recorded historical domain-to-IP resolutions. The domain IoC nwphotoblog[.]com posted 268 resolutions from 7 February 2017 and 17 May 2026.

TA4922 Global Attack IP IoC Investigation

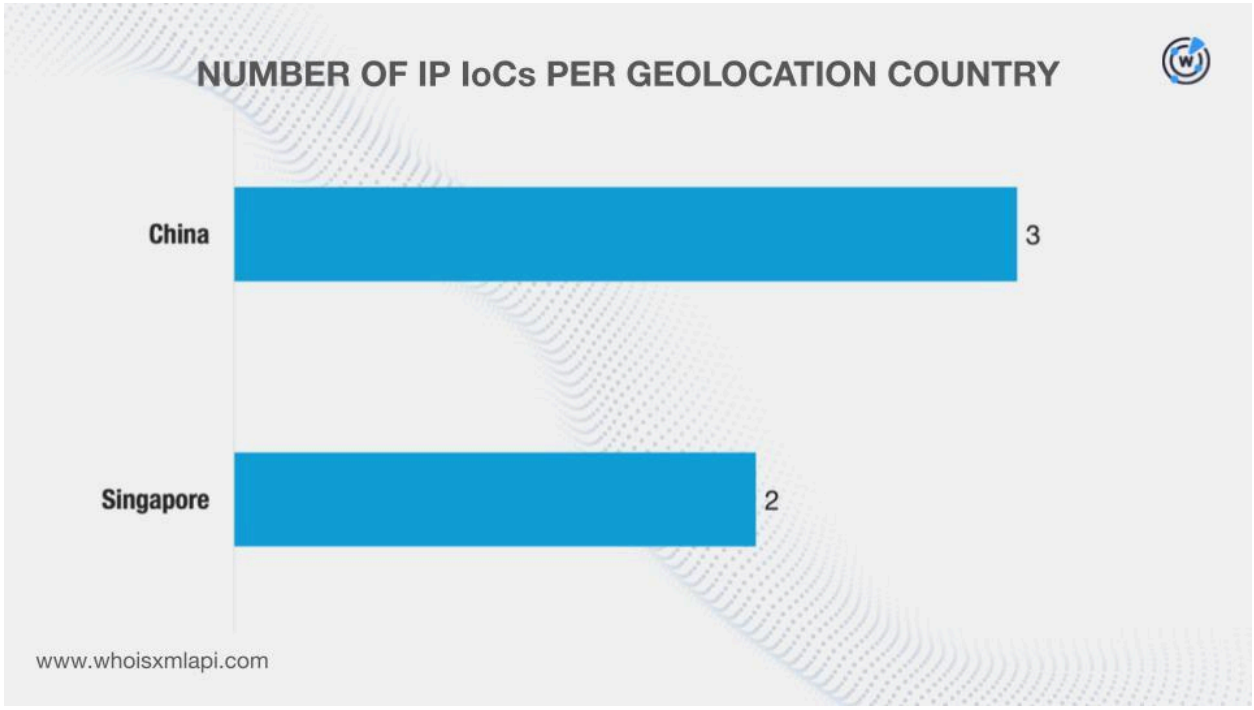
After that, we zoomed in on the five IP IoCs.

Sample network data from the IASC revealed that 36 unique IP addresses that could belong to victims under 12 distinct ASNs communicated with two of the IP IoCs between 26 December 2025 and 12 April 2026.

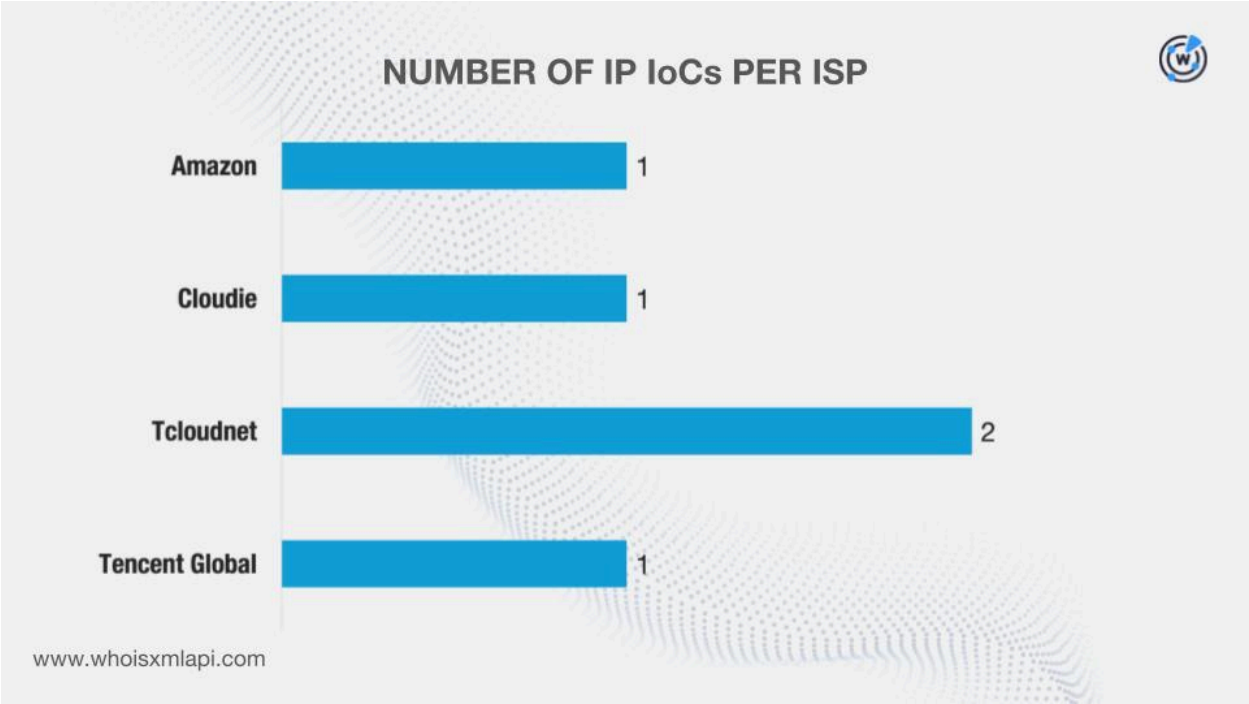


The results of our Bulk IP Geolocation Lookup for the IP IoCs showed that:

- They were geolocated in two countries, one of which—China—was also named a registrant country.



- They were administered by four different ISPs.



We then queried the IP IoCs on DNS Chronicle API and learned that three posted 186 historical IP-to-domain resolutions over time. The IP IoC 18[.]139[.]83[.]110, for instance, recorded 114 resolutions between 4 January 2019 and 30 April 2026.

To date, only two of the three IP IoCs with historical resolutions recorded communications in 2026.

New TA4922 Global Attack Artifacts Found

We kicked off our hunt for new possibly connected artifacts by querying the domain IoCs on WHOIS History API. We discovered nwphotoblog[.]com had eight unique email addresses in its historical records. Further examination revealed that four were public email addresses.

The results of our Reverse WHOIS API queries for the domain IoCs led to the discovery of 2,779 unique email-connected domains after those already dubbed as IoCs were weeded out.

We queried the email-connected domains on Threat Intelligence API and found out that 39 have already been weaponized for various cyber attacks. Take a look at more information for five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
cosmetologycareerguidance[.]com	Phishing Generic threat	04/23/26–06/11/26 04/25/26–05/24/26
annakovaleva[.]com	Phishing	05/13/26–06/11/26
astra-travel[.]com	Phishing	05/04/26–06/11/26
blueoceancode[.]com	Malware distribution	03/19/26–06/11/26
cst-furniture[.]com	Phishing Generic threat	04/22/26–06/11/26 04/22/26–05/21/26

Next, we queried the domain IoCs on DNS Lookup API, which allowed us to identify an additional IP address.

A Threat Intelligence API query for the sole additional IP address—47[.]242[.]39[.]192—revealed that it has already figured in malware distribution between 5 November 2025 and 11 June 2026 and other attacks seen from 21 November 2025 and 11 June 2026.

An IP Geolocation API query for the additional IP address, meanwhile, showed that it was geolocated in China (i.e., named a domain IoC registrant country and an IP IoC geolocation country earlier) under the administration of ISP Alibaba.

At this point, we had six IP addresses in all—five named as IoCs and one additional. We queried them on Reverse IP API. Further scrutiny revealed that three could be dedicated hosts. Together, they hosted 37 unique IP-connected domains after those already tagged as IoCs and the email-connected domains were filtered out.

The results of our Threat Intelligence API queries for the IP-connected domains showed that 18 have already been weaponized for various cyber attacks. Here are more details for five examples.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
bpsalpe[.]cn	Malware distribution	03/19/26–06/10/26
ccgzbts[.]cn	Malware distribution	03/19/26–06/10/26
cocdex[.]cn	Malware distribution	03/19/26–06/10/26
foeo[.]cn	Malware distribution	03/19/26–06/10/26
fwqjwhe[.]cn	Malware distribution	03/19/26–06/10/26

The Final Word

Our investigation into the global TA4922 attack revealed that 36 unique IP addresses that could belong to victims communicated with two of the IP IoCs based on sample network traffic data from the IASC.

Our deep dive also led to the discovery of 2,817 new artifacts comprising 2,779 email-connected domains, one additional IP address, and 37 IP-connected domains. It is also worth noting that as of this writing, 58 of the newly uncovered artifacts have already been weaponized for 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

- 019699[.]com
- 1-800-newroof[.]com
- 100kpass[.]com
- a-benterprisenig[.]com
- a1cebucarrental[.]com
- a1leakdetection[.]com
- babilinsaatmekatronik[.]com
- baby-golightly[.]com
- bacenglish[.]com
- c-jtransportation[.]com
- c-rayment[.]com
- c4qatar[.]com
- daddycoding[.]com
- daetria[.]com
- dafontlab[.]com
- e-bandaosports[.]cn
- e-bikeservices[.]com
- e-cathaya[.]com
- fabscleanings[.]com
- fabulousfinances[.]com
- fabulouskidsbooks[.]com
- g17climatechange[.]com
- g4gamer[.]com
- gabapentinneurontininfo[.]com
- h2omen[.]com
- hajer-co[.]com
- halfbeds[.]com
- i-cortexi[.]com
- iamigoschool[.]com
- iatehealthy[.]com
- jadedpictures[.]com
- jaglance[.]com
- jaipurmurti[.]com
- k-forceu[.]com
- k1cars[.]com
- kabirsalunkhe[.]com
- laced569[.]com
- lagoslagos[.]com
- lahcenart[.]com
- macretailsolutions[.]com
- madaat[.]com
- madisonvalleycandle[.]com
- naddparty[.]com
- nadiapn[.]com
- naganoleantonic-us[.]com
- ocean-field59[.]com
- oceancitybeachfronts[.]com
- oceanwildlifebracelet[.]com
- p-j-s[.]com
- p-shaddel[.]com
- p50natca[.]com
- qazishaharyar[.]com
- qethurah[.]com
- qiroqo[.]com
- radianthen[.]com
- radiomakonline[.]com
- radirus[.]com
- s2tours[.]com
- sabinasalon[.]com
- sabrinaroeschley[.]com
- t-ikeda[.]com
- t-lebosports[.]cn
- tackwalls[.]com
- ubiquitousinnovationlabs[.]com
- ubiquitousstrategicinsight[.]com
- ucompile[.]com
- vagabondtrails[.]com
- valenti-agency[.]com
- valkyriago[.]com
- waatrnaqqe[.]com
- wableins[.]com
- walkercontemporaryart[.]com
- xannder[.]com
- xebec-urabari-cutter[.]com

- xebecconsultants[.]com
- y00tspin[.]com
- yahtscvisionary[.]com
- yallakoraegy[.]com
- zaynjoshua[.]com
- zebestgames[.]com
- zelustoken[.]com

Additional IP Address

- 47[.]242[.]39[.]192

Sample IP-Connected Domains

- 888888vip[.]live
- aappp[.]vip
- bpsalpe[.]cn
- ccgzbts[.]cn
- dusdt[.]vip
- foeo[.]cn
- gnbqmrr[.]cn
- heo88[.]top
- ixznpri[.]cn
- kezida[.]vip
- letsvpnchina[.]com
- mitgiied[.]vip
- oygzbtc[.]cn
- pdf-gtds[.]com
- unionpayintll[.]vip
- vyhjmi[.]cn
- wps-hakjgyu[.]top
- xdappxz[.]vip
- yunlifang[.]vip
- zszsz[.]vip