WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A DNS Investigation of LenAI's ErrTraffic ClickFix Distribution Network

Threat Report

Table of Contents

1. Executive Report
    a. Deep Diving into the ErrTraffic Domain IoCs
    b. New ErrTraffic Artifacts Brought to Light
2. Conclusion
3. Appendix: Sample Artifacts

Executive Report

Sekoia threat researchers recently analyzed a new campaign leveraging the ErrTraffic ClickFix malware distribution framework and identified several network IoCs from which we extracted 71 domains. They believed LenAI who has been gaining notoriety as a MaaS operator in the Dark Web is behind the recent spate of attacks.

The two clusters Sekoia analyzed zoomed in on WordPress servers, had a built-in TDS function, concealed their C&C infrastructure within the blockchain, and utilized fake AI tools (e.g., Google Antigravity and ChatGPT) as lures. Even if MaaS distributor LenAI was implicated, the researchers surmised that the clusters they studied (i.e., Analytics and Beer) were launched by different but unnamed threat actors. Note that LenAI was also behind the Aeternum C&C botnet publicized in February this year, among other threats.

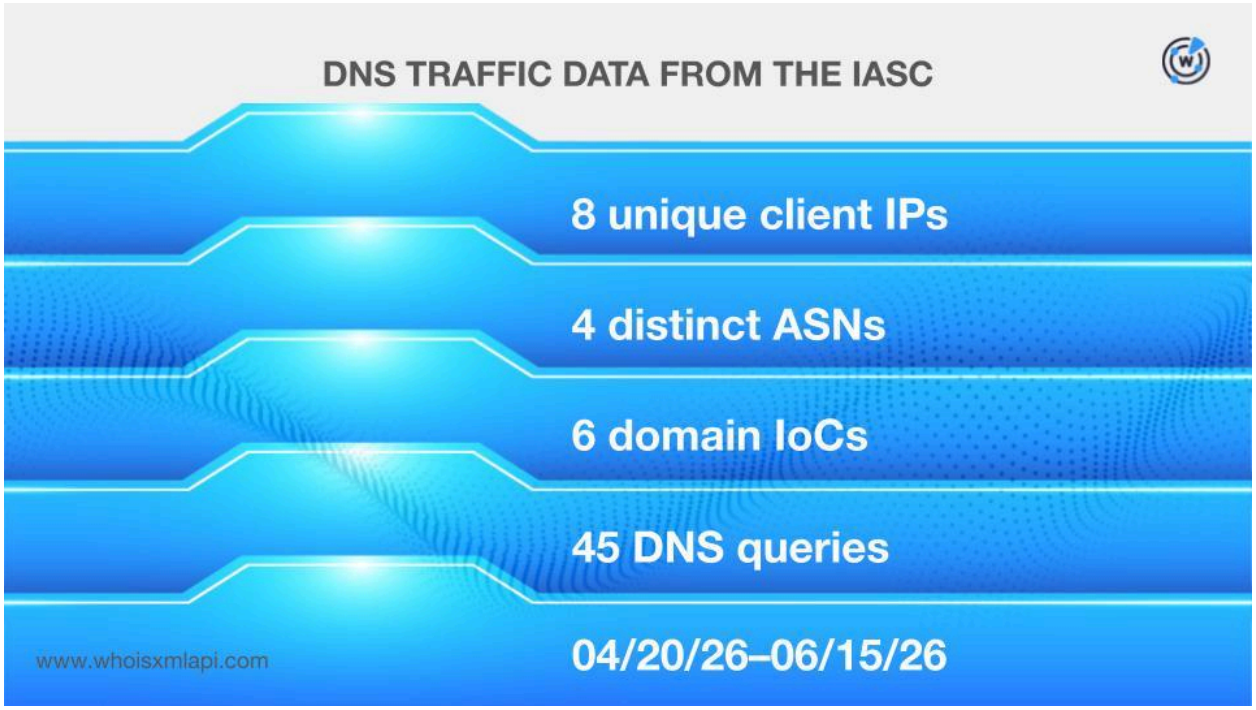
Our own DNS deep dive into the ErrTraffic network IoCs led to these discoveries:

- Eight unique client IP addresses that communicated with six distinct domain IoCs
- Two domain IoCs that appeared in two typosquatting groups with 3–5 members each
- Four domain IoCs that were likely registered with malicious intent
- 12 email-connected domains
- 16 IP addresses, 12 of which were confirmed malicious
- 156 IP-connected domains, 44 of which were confirmed malicious
- 1,079 string-connected domains

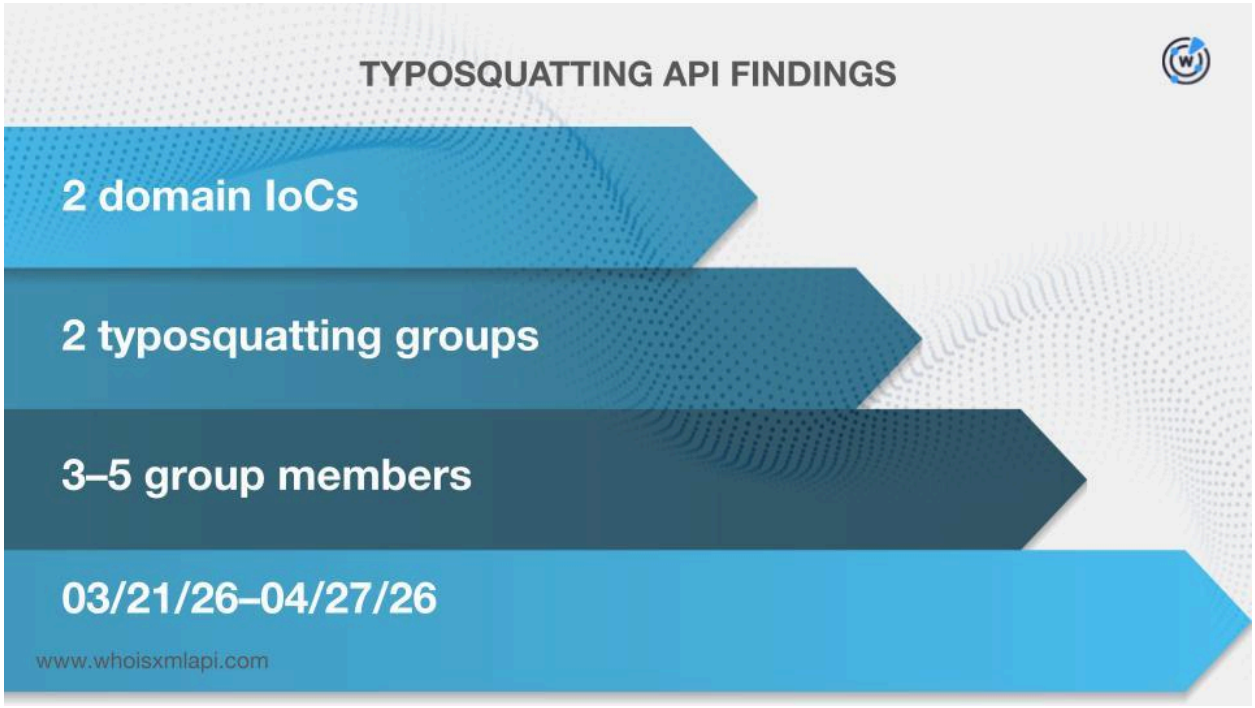
Deep Diving into the ErrTraffic Domain IoCs

We began our investigation by ensuring none of the 71 domain IoCs were owned by legitimate entities aided by the WhoisXML API MCP Server.

Next, we looked at sample network traffic data from the IASC and discovered that eight unique client IP addresses under four distinct ASNs communicated with six of the domain IoCs via 45 DNS queries between 20 April and 15 June 2026.



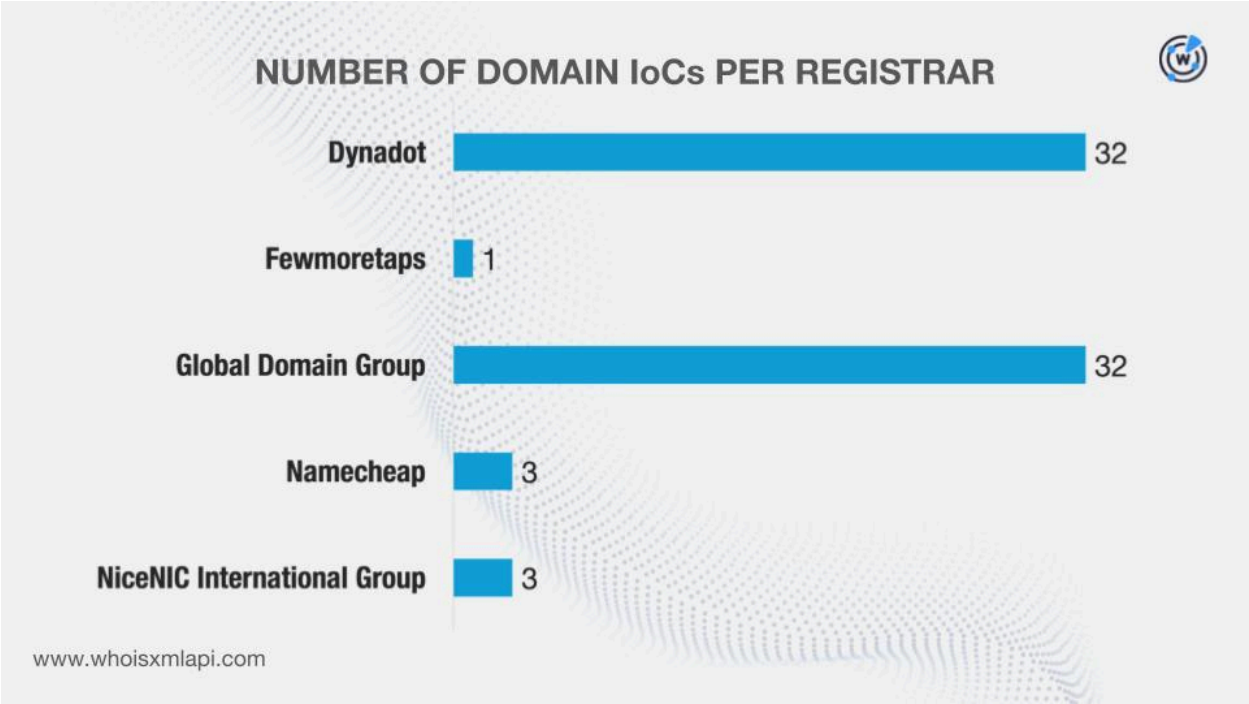
We then queried the domain IoCs on Typosquatting API and learned that two of them appeared in two typosquatting groups. The IoC finework[.]top was bulk-registered with four look-alike domains, three of which were created on 22 March 2026. Note that one of its look-alikes did not have a creation date on record. The domain sandman[.]bond, meanwhile, was bulk-registered with two look-alikes between 26 and 27 April 2026.



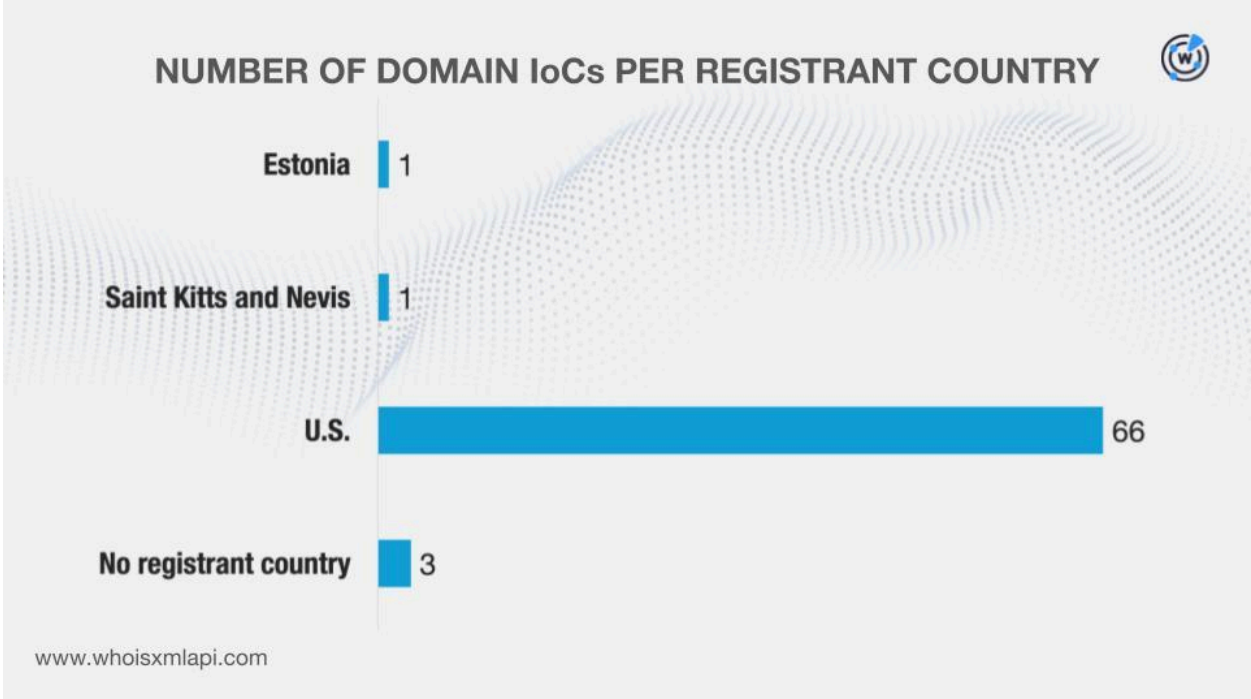
Next, we discovered that four of the domain IoCs appeared on the First Watch Malicious Domains Data Feed. They were likely registered with malicious intent 118–127 days before they were dubbed as IoCs. The domain cloud-safe[.]click, for instance, was registered on 9 February 2026, 127 days before the Sekoia report's publication on 16 June 2026.

We then queried the domain IoCs on WHOIS API, completed missing data points with the help of Domain Info API, and found out that:

- They were all created in 2026, hinting at the threat actors' preference for using NRDs in their campaigns.
- They were administered by five registrars.



- While three domains did not have registrant countries on record, the remaining 68 were registered in three countries.



Next, we queried the domain IoCs on DNS Chronicle API and learned that 70 recorded 566 historical domain-to-IP resolutions over time. Here are more details for five examples.

DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
webanalytics-cdn[.]sbs	150	02/21/26–04/21/26
finework[.]top	56	06/11/21–05/22/26
abrikos[.]xyz	32	03/16/22–05/16/26
anakondabob[.]club	12	05/08/26–05/26/26
bobik[.]cfd	12	05/05/26–05/26/26

All 70 domains with historical results continue to post resolutions in 2026.

New ErrTraffic Artifacts Brought to Light

After all that, we started our hunt for new ErrTraffic artifacts.

First, we queried the domain IoCs on WHOIS History API and discovered that four had four unique email addresses in their historical records. Further scrutiny revealed that two were public email addresses.

Reverse WHOIS API queries for the public email addresses led to the discovery of 12 unique email-connected domains after those already identified as IoCs were filtered out.

Next, we queried the domain IoCs on DNS Lookup API and learned that 30 resolved to 16 unique IP addresses.

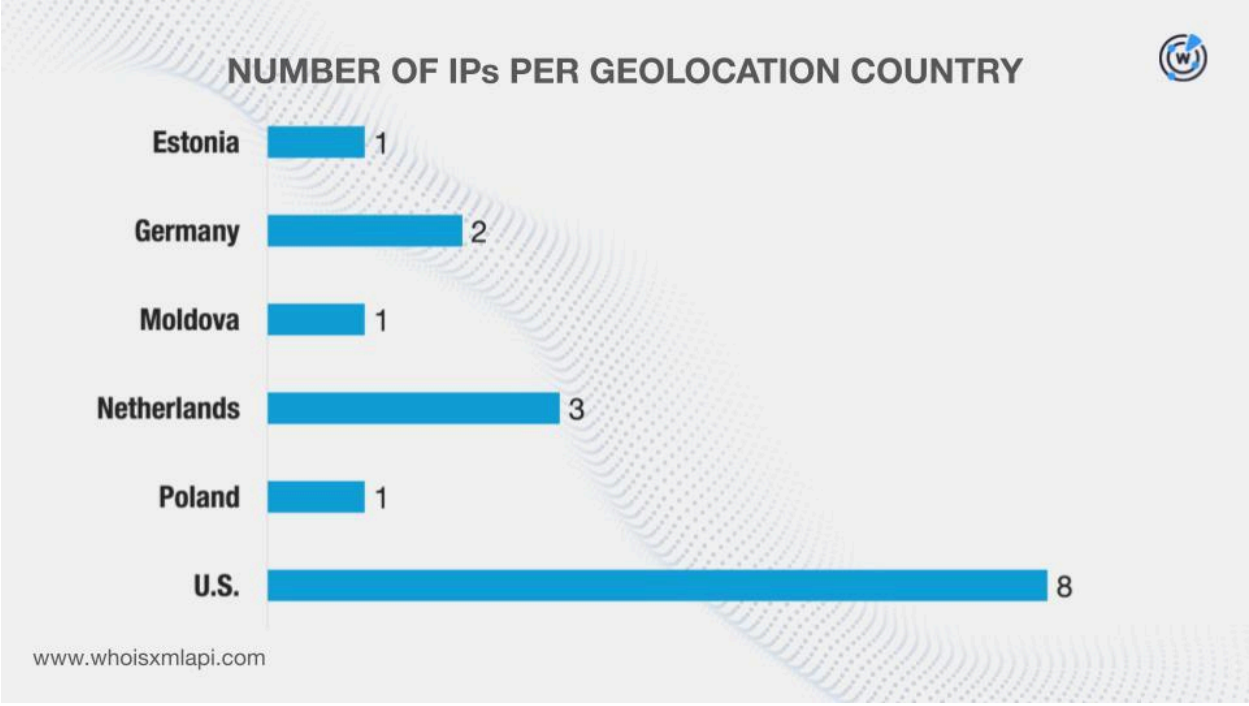
Threat Intelligence API queries for the IP addresses showed that 12 have already been weaponized for various malicious campaigns. Take a look at more information for five examples below.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
178[.]16[.]52[.]101	Malware distribution Phishing Attack Spam campaign	03/15/26–06/18/26 05/06/26–06/17/26 08/23/25–06/17/26 08/22/25–06/17/26

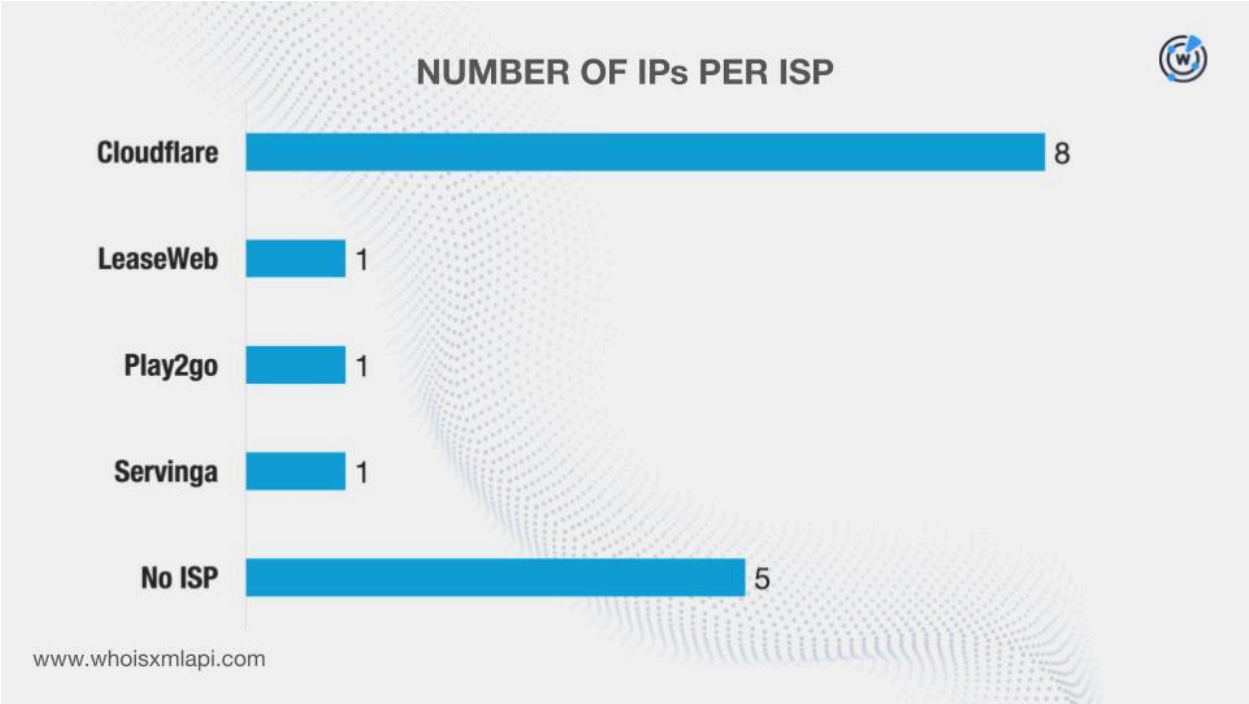
	Generic threat	03/26/26–06/16/26
104[.]21[.]49[.]125	Phishing Generic threat Malware distribution	03/29/23–06/17/26 05/12/23–06/16/26 09/19/24–06/16/26
104[.]21[.]31[.]113	Malware distribution Phishing	08/10/24–06/16/26 12/11/24–05/05/26
104[.]21[.]61[.]51	Malware distribution	08/05/23–06/16/26
172[.]67[.]206[.]124	Malware distribution	08/05/23–06/16/26

After that, we queried the IP addresses on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in six countries.



- While five did not have ISPs on record, the remaining 11 were administered by four ISPs.



Next, we queried the IP addresses on Reverse IP API and discovered that eight were likely dedicated hosts. Together, they hosted 156 unique IP-connected domains after those already dubbed as IoCs and the email-connected domains were filtered out.

Threat Intelligence API queries for the IP-connected domains revealed that 44 have already figured in various cyber attacks. Take a look at more information for five examples below.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
framework-css-styles-js[.]beer	Generic threat Phishing	06/12/26–06/17/26 06/11/26–06/17/26
ai-nexora[.]sbs	Malware distribution	04/14/26–06/17/26
bnnsbdsdn-js[.]beer	Malware distribution	04/14/26–06/17/26
bnsclod[.]beer	Malware distribution	04/14/26–06/17/26
capcha-cdn-js[.]beer	Malware distribution	04/14/26–06/17/26

We then took a closer look at the domain IoCs and extracted 67 unique text strings. According to the results of our Domains & Subdomains Discovery searches for strings

that appeared at the start of domains not yet tagged as IoCs or email- or IP-connected, we obtained results for 38 strings including but not limited to the following:

- abrikos.
- babybon.
- chatgpt-web.
- defi-xstocks.
- etomoe.
- finework.
- gdedengikarlos.
- jogosdecarrobr.
- mambet.
- ponikas.
- robodomain.
- sandman.
- testerlau.
- vsactivens.
- web-protection.
- yoshicity.

We also collated 1,079 unique string-connected domains after those already classified as IoCs and the email- and IP-connected domains were filtered out.

Note that the string-connected domains only serve to reflect the overall popularity of the strings extracted from the IoCs. As such, determining their legitimacy may require further investigation.

Conclusion

Our DNS deep dive into the ErrTraffic IoCs revealed that eight unique client IP addresses communicated with six of the domain IoCs. We also learned that two of the domain IoCs appeared in two typosquatting groups with 3–5 members each. In addition, four of the domain IoCs were likely registered with malicious intent.

Our in-depth investigation also uncovered 1,263 new artifacts comprising 12 email-connected domains, 16 IP addresses, 156 IP-connected domains, and 1,079 string-connected domains. It is worth noting that 56 artifacts have already been weaponized for 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 Domains

- balashow[.]xyz
- hardbass[.]xyz
- mobbi[.]xyz
- narkoman[.]xyz
- pizdabol[.]xyz
- tehnomag[.]xyz
- vgovno[.]xyz
- xn--80akpks[.]xn--p1acf
- zc101wx[.]com

Sample IP Addresses

- 104[.]21[.]31[.]113
- 158[.]94[.]209[.]253
- 172[.]67[.]162[.]254
- 178[.]16[.]52[.]101
- 185[.]122[.]171[.]103
- 194[.]76[.]227[.]172
- 2[.]27[.]5[.]153
- 80[.]96[.]109[.]54
- 94[.]154[.]35[.]161

Sample IP-Connected Domains

- ai-nexora[.]sbs
- anlytic-js-cloud[.]beer
- awesomeisojs[.]beer
- bbdsnssserver[.]beer
- bhfgtrns-js[.]beer
- bigddeaf[.]monster
- canva-web[.]org
- capcha-cdn-js[.]beer
- capt-stash[.]beer
- darndcs-js[.]beer
- dncloteam[.]beer
- dreff-nsdns[.]beer
- ethercdnns[.]beer
- exdanteam[.]beer
- fijscdn[.]beer
- fontawesome-js-cdn[.]beer
- fonts25-save[.]sbs
- gdnssljs[.]beer
- ghdnsserverns[.]beer
- gppcdnns[.]beer
- hasmeverdcdn[.]beer
- hftplcnsns[.]beer
- hpscdn[.]beer
- ilivewp[.]com
- istounscnnd[.]beer
- jsframeworkns[.]beer
- kapitaljetzt[.]com
- kroger[.]today
- l3cdnns[.]beer
- ladydosug[.]live
- ladydosug[.]love
- mandare[.]life
- menards[.]click
- merkari[.]digital
- neiwteamcdn[.]beer
- nexus-server[.]click
- nfsclaudecdn[.]beer
- olnsclaud[.]beer
- packshotedits[.]com
- planetfitness[.]life
- polygon-cnd-stats[.]sbs
- rpc-cloud[.]beer
- rpc-polygon[.]beer
- sdhscndnssl[.]beer

- sherepunjabpipeband[.]com
- shssshdscn[.]beer
- teamcss[.]beer
- tescdnlast[.]beer
- testapi34726[.]sbs
- unacerveza[.]beer
- vaidyanat[.]monster
- verification-code-js[.]beer
- verification-js-cdn[.]boats
- web-safety[.]beer
- web-security[.]beer
- winecdn[.]sbs
- xdavnode[.]pro
- yinava[.]monster

Sample String-Connected Domains

- abrikos[.]agency
- abrikos[.]app
- abrikos[.]biz
- adzeta[.]co
- adzeta[.]com
- adzeta[.]eu
- antigravity[.]academy
- antigravity[.]ad
- antigravity[.]ae
- babybon[.]be
- babybon[.]cn
- babybon[.]co[.]il
- bobik[.]app
- bobik[.]aquila[.]it
- bobik[.]at
- bulletpop[.]com
- chatgpt-web[.]asia
- chatgpt-web[.]bio
- chatgpt-web[.]club
- chubrik[.]by
- chubrik[.]com
- chubrik[.]ml
- clip-stash[.]com
- cloud-safe[.]ai
- cloud-safe[.]ca
- cloud-safe[.]cfd
- comicstar[.]cn
- comicstar[.]com
- comicstar[.]com[.]tw
- defi-xstocks[.]com
- devltd[.]cn
- devltd[.]co[.]uk
- devltd[.]com
- etomoe[.]com
- etomoe[.]fun
- etomoe[.]info
- etomoidomen[.]tk
- finework[.]app
- finework[.]be
- finework[.]biz
- gdedengikarlos[.]net[.]bb
- jogosdecarrobr[.]com
- js-server[.]cfd
- js-server[.]click
- js-server[.]cloud
- mambet[.]ai
- mambet[.]aquila[.]it
- mambet[.]arab
- marmelad[.]am
- marmelad[.]asia
- marmelad[.]bar
- mhaskins[.]com
- microchlen[.]bond
- microchlen[.]ru
- mnepohui[.]com
- mnepohui[.]de
- mnepohui[.]ru
- ponikas[.]buzz
- ponikas[.]co[.]bb
- ponikas[.]com
- robodomain[.]com
- robodomain[.]net
- robodomain[.]ru
- sandman[.]ae

- sandman[.]ag
- sandman[.]ai
- smackit[.]africa
- smackit[.]ai
- smackit[.]app
- spartanec[.]com
- spartanec[.]com[.]ua
- spartanec[.]info
- superpooper[.]app
- superpooper[.]club
- superpooper[.]co
- testerlau[.]net[.]bb
- traffadmin[.]com
- traffadmin[.]ru
- vsactivens[.]com
- vsactivens[.]sbs
- web-protection[.]co[.]uk
- web-protection[.]com
- web-protection[.]de
- web-safe[.]cc
- web-safe[.]cn
- web-safe[.]co[.]uk
- webflare[.]ai
- webflare[.]app
- webflare[.]blog
- yoshicity[.]com