WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Rounding Up DNS Facts about Operation RoundPress

Table of Contents

Executive Report

The Cybersecurity & Infrastructure Security Agency (CISA) added CVE-2025-32433 and CVE-2024-42009 to the Known Exploited Vulnerabilities (KEV) Catalog on 9 June 2025 after they were reportedly abused by APT28 to hack government webmail servers in an operation dubbed “RoundPress.”

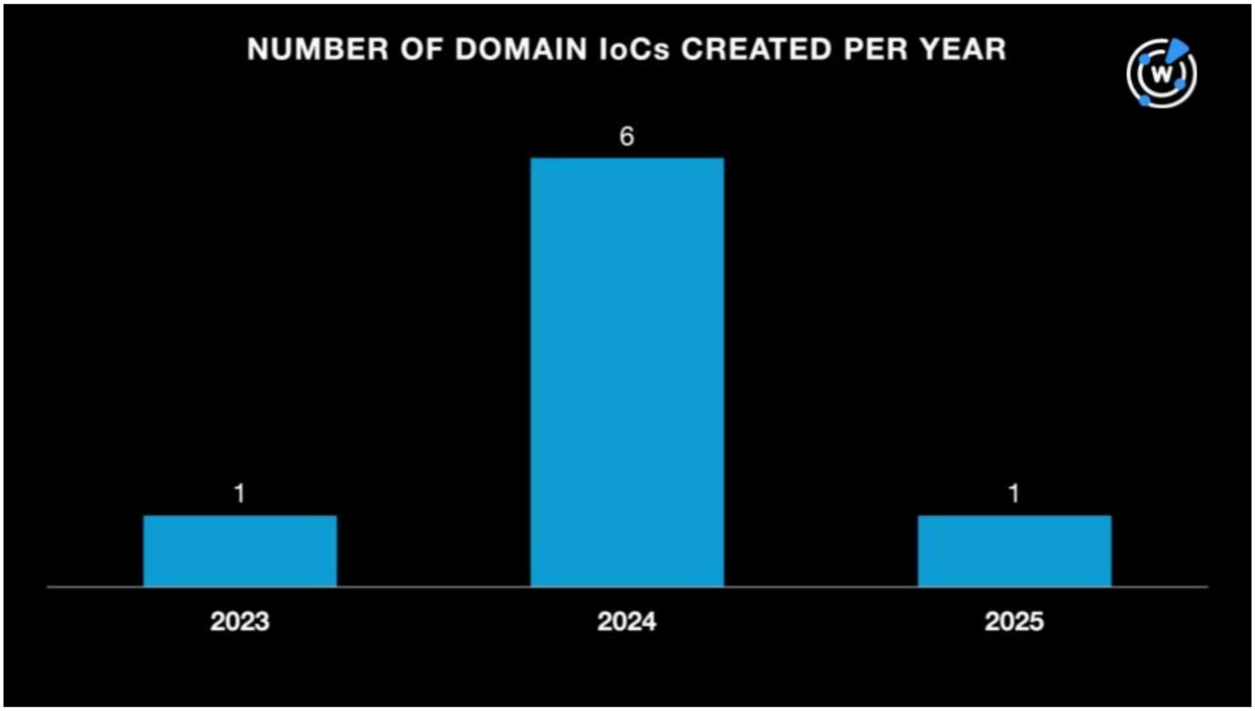
ESET researchers identified 19 indicators of compromise (IoCs) comprising 10 domains and nine IP addresses related to Operation RoundPress. WhoisXML API sought to uncover more potentially connected artifacts using domain and DNS intelligence and found:

- 8,222 email-connected domains, seven of which were malicious
- Two IP addresses, both were malicious
- 102 IP-connected domains
- 580 string-connected domains

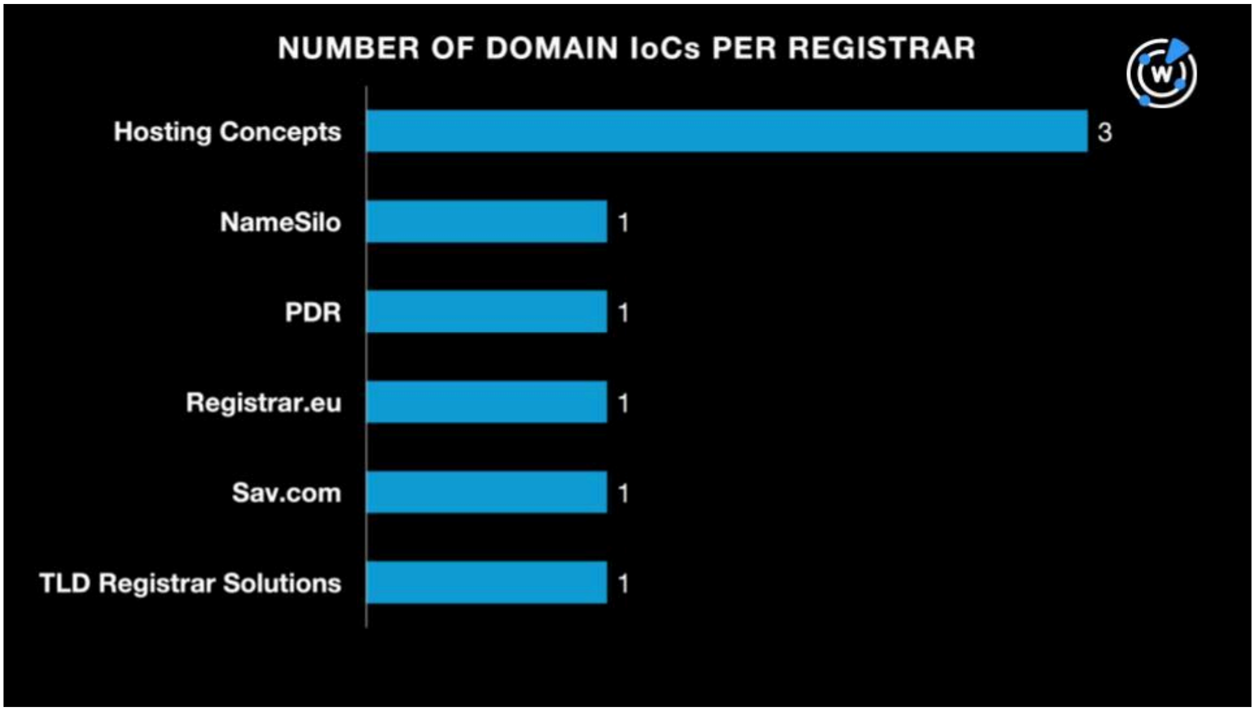
Facts about the RoundPress IoCs

We began our analysis by seeking more information on the 10 domains identified as IoCs through a Bulk WHOIS API query. The results showed that eight of them had current WHOIS records.

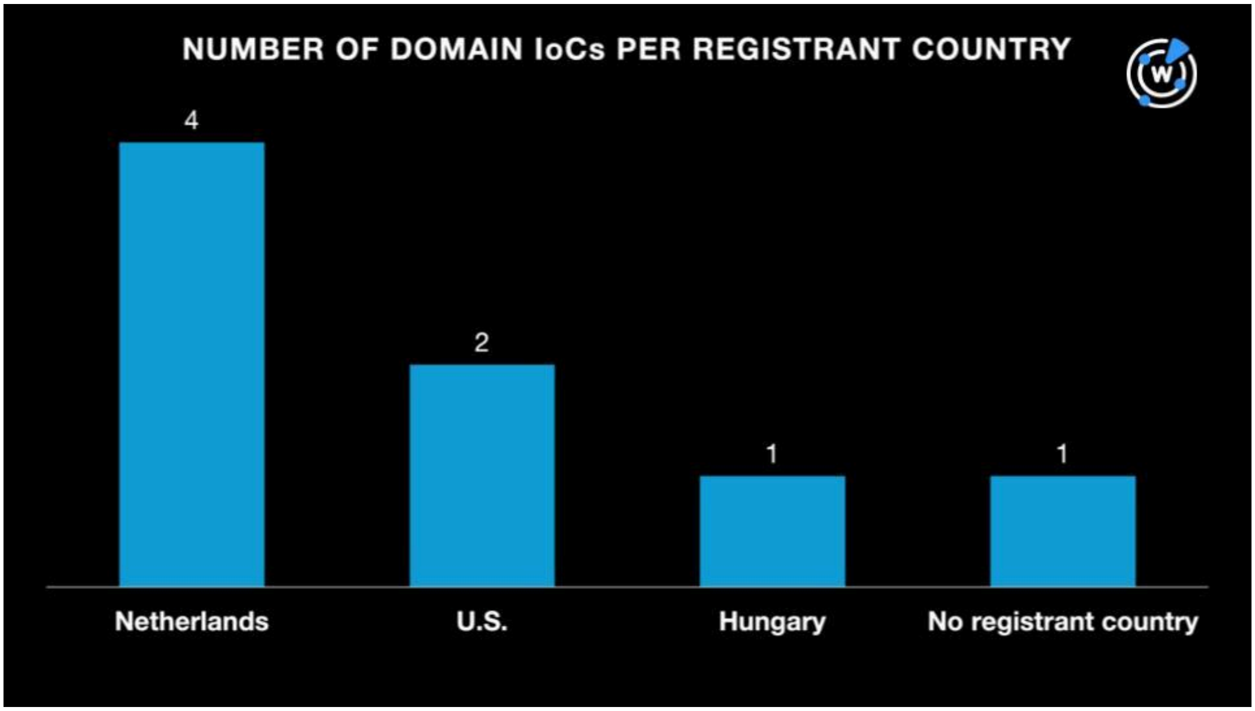
- The eight IoCs were created between 2023 and 2025. A majority of them, six to be exact, were created in 2024 while one each was created in 2023 and 2025.



- Hosting Concepts was the top registrar, accounting for three domains. In addition, one each was administered by NameSilo, PDR, Registrar.eu, Sav.com, and TLD Registrar Solutions.



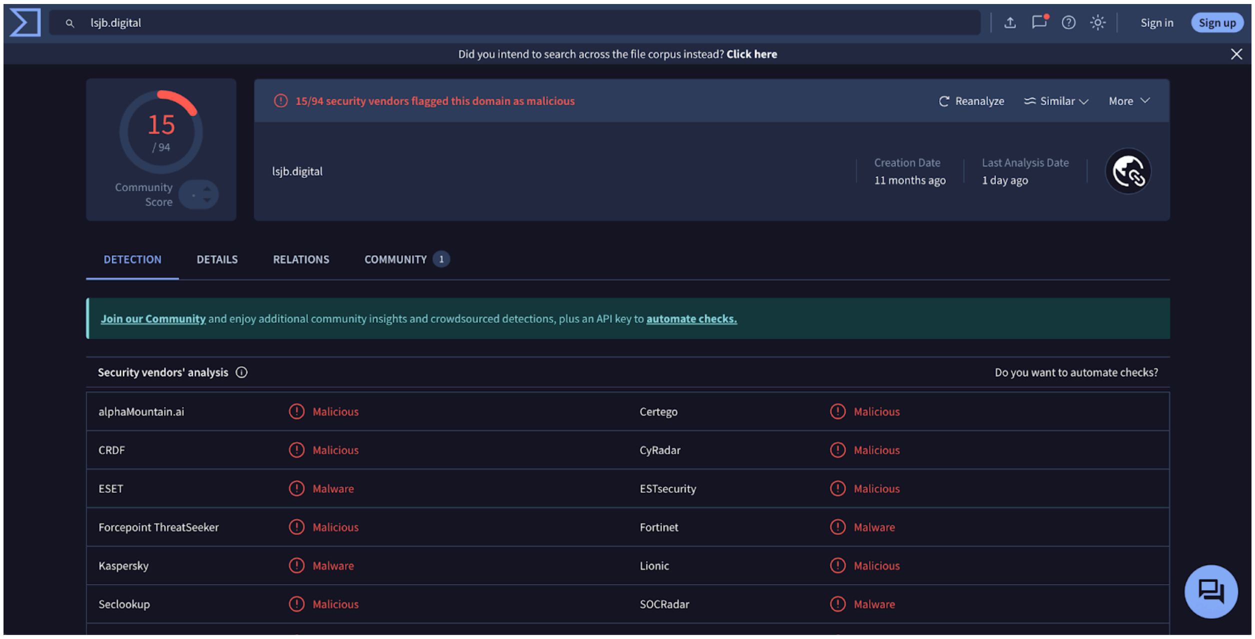
- While one of the eight domains with current WHOIS records did not have a registrant country on record, the remaining seven were registered in three nations led by the Netherlands, which accounted for four domains. The U.S. accounted for two domains while the last one was registered in Hungary.



Next, we queried the 10 domains identified as IoCs on DNS Chronicle API and found that all of them had a total of 351 historical domain-to-IP resolutions. The IoC rnl[.]world, which accounted for 252 resolutions, recorded the oldest resolution dated 14 September 2018. Take a look at the details for five examples below.

DOMAIN IoC	NUMBER OF HISTORICAL DOMAIN-TO-IP RESOLUTIONS	FIRST HISTORICAL DOMAIN-TO-IP RESOLUTION DATE
hfuu[.]de	5	6 March 2024
ikses[.]net	7	1 December 2024
lsjb[.]digital	12	2 July 2024
sqj[.]fr	7	18 April 2024
tuo[.]world	26	18 March 2023

We also searched First Watch Malicious Domains Data Feed for the 10 domains identified as IoCs and discovered that lsjb[.]digital appeared as a domain likely to turn malicious on 1 July 2024, 318 days before it was classified as an IoC by ESET on 15 May 2025. Today, it is considered malicious by 15 out of 94 engines on VirusTotal.



Did you intend to search across the file corpus instead? **Click here**

15/94 security vendors flagged this domain as malicious

lsjb.digital

Creation Date 11 months ago

Last Analysis Date 1 day ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

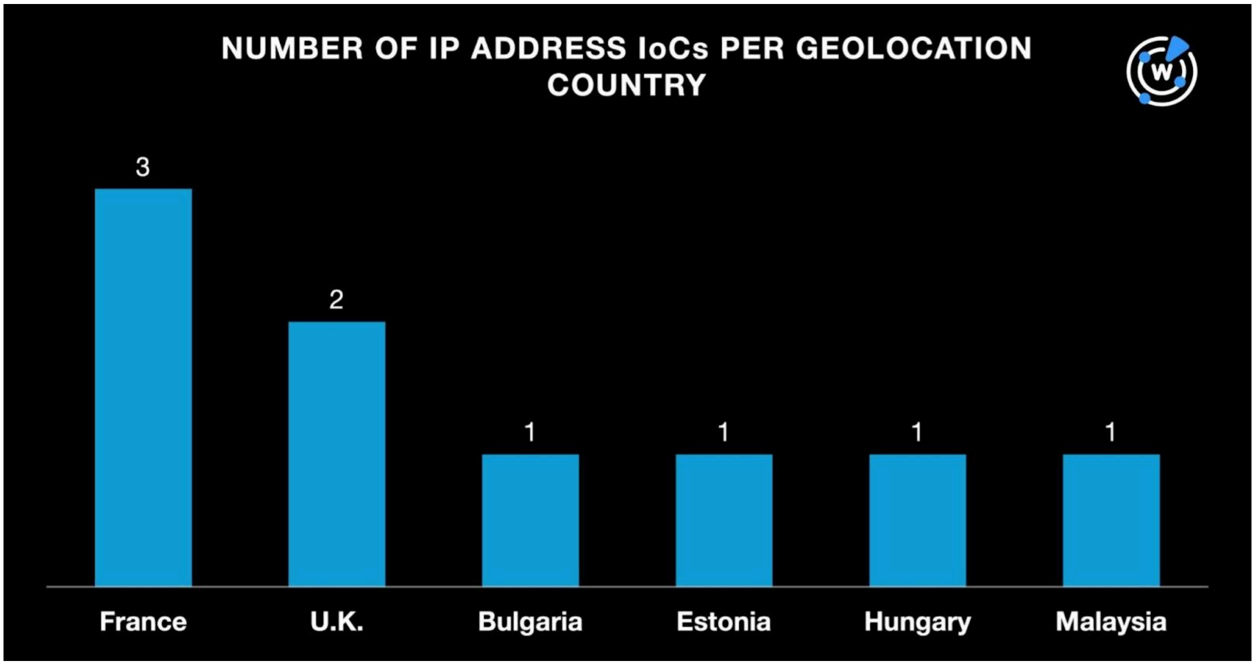
Security vendors' analysis

Do you want to automate checks?

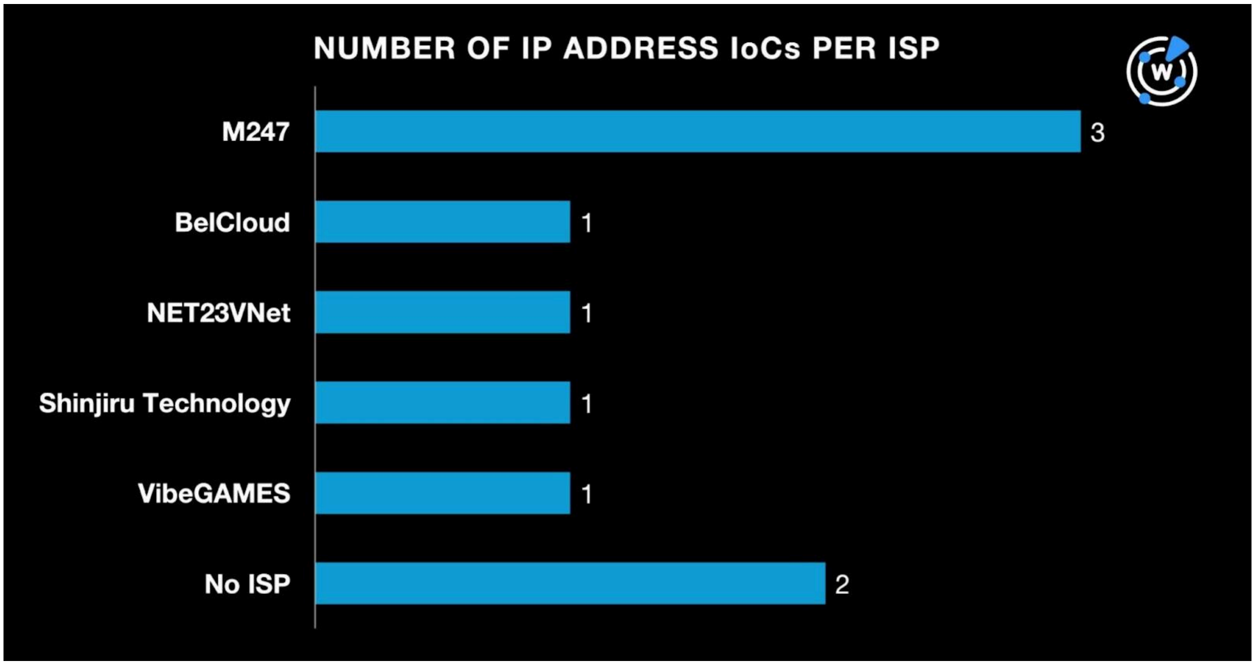
alphaMountain.ai	Malicious	Certego	Malicious
CRDF	Malicious	CyRadar	Malicious
ESET	Malware	ESTsecurity	Malicious
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
Kaspersky	Malware	Lionic	Malicious
Seclookup	Malicious	SOCRadar	Malware

After that, we queried the nine IP addresses identified as IoCs on Bulk IP Geolocation Lookup and found that:

- They were geolocated in six different countries topped by France, which accounted for three IP addresses. Two IPs originated from the U.K. while one each was geolocated in Bulgaria, Estonia, Hungary, and Malaysia.



- While two IP addresses did not have ISPs on record, the seven remaining ones were split among five ISPs led by M247, which accounted for three IPs. BelCloud, NET23VNet, Shinjiru Technology, and VibeGAMES administered one IP address each.



RoundPress IoC DNS Connections

Our search for connected properties began with a WHOIS History API query for the 10 domains identified as IoCs. We discovered that three of them had email addresses in their historical WHOIS records. We uncovered five unique email addresses, three of which were public.

While a Reverse WHOIS API query for the three public email addresses did not turn up email-connected domains via current WHOIS records, we did uncover 8,222 email-connected domains via historical WHOIS records after duplicates and those already identified as IoCs were filtered out. Notably, many of them resembled the IoCs in that they were made up of 3–5 letters or letter-and-number combos.

A Threat Intelligence API query for the 8,222 email-connected domains showed that seven have already figured in cyber attacks. Take a look at three examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT
006700[.]xyz	Generic threat
097170[.]com	Malware distribution
arkt[.]xyz	Malware distribution

We also queried the 10 domains identified as IoCs on DNS Lookup API and found that five of them had current IP resolutions. We uncovered two unique IP addresses after those already identified as IoCs were filtered out.

According to the results of our Bulk IP Geolocation Lookup query for the two additional IP addresses, both were geolocated in the U.S., which incidentally is not included in the list of IoCs' geolocation countries. Both were also administered by Amazon, also not one of the IoCs' ISPs.

A Threat Intelligence API query for the two additional IP addresses revealed they have already been weaponized for attacks. The IP address 13[.]248[.]169[.]48, for instance, has already been associated with phishing, generic threats, malware distribution, command and control (C&C), suspicious activity, and attacks.

After that, we queried the 11 IP addresses (nine identified as IoCs and two additional from our DNS Lookup API query) on Reverse IP API and discovered that seven of them had IP-to-domain resolutions. Four of the seven IP addresses could be dedicated hosts. Altogether, the four possibly dedicated IP addresses hosted 102 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

As our final step, we looked more closely at the 10 domains identified as IoCs and collated 10 unique text strings. We used these strings as Domains & Subdomains Discovery search terms along with the **Starts with** parameter:

- hfuu.
- hijx.
- ikses.
- jiaw.
- lsjb.
- raxia.
- rnl.
- sqj.
- tgh24.
- tuo.

We uncovered 580 string-connected domains in all that only differed from those identified as IoCs in terms of TLD.

—

Overall, our in-depth analysis of the Operation RoundPress IoCs led to the discovery of 8,906 connected artifacts comprising 8,222 email-connected domains, two IP addresses, 102 IP-connected domains, and 580 string-connected domains. It is also worth noting that nine of these 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 Domains

- 0000088[.]xyz
- 00002222[.]xyz
- 00003333[.]xyz
- aavc[.]xyz
- abcje[.]com
- abcoj[.]com
- babfor[.]com
- bailihexiang[.]com
- baky[.]xyz
- cangdai[.]xyz
- canggou[.]xyz
- canxing[.]xyz
- daawoo[.]com
- dachuangjia[.]com
- daihou[.]xyz
- eaok[.]xyz
- ebxyz[.]com
- ecosoulife[.]net
- fafafa[.]xyz
- fafang[.]xyz
- faky[.]xyz
- gaar[.]xyz
- gaky[.]xyz
- gaok[.]xyz
- hackthon[.]com
- hafury[.]xyz
- haiao[.]xyz
- iaok[.]xyz
- ibaft[.]com
- ibaimu[.]com
- jadetown[.]com
- jaky[.]xyz
- jaok[.]xyz
- kafeisi[.]com
- kaifei[.]xyz
- kajl[.]xyz
- laishiju[.]com
- lamando[.]net
- landmarkbank[.]cn
- mache[.]xyz
- mady[.]xyz
- mainiuzai[.]com
- nabcd[.]com
- naky[.]xyz
- nancai[.]xyz
- oaok[.]xyz
- obcg[.]xyz
- ocok[.]xyz
- pangko[.]com
- paok[.]xyz
- pbai[.]xyz
- qaok[.]xyz
- qbai[.]xyz
- qbar[.]xyz
- raok[.]xyz
- rbai[.]xyz
- rbar[.]xyz
- saian[.]xyz
- saiao[.]xyz
- saicheyi[.]com
- tabb[.]xyz
- tabx[.]xyz
- tadu[.]xyz
- uaok[.]xyz
- ubok[.]xyz
- udok[.]xyz
- vady[.]xyz
- vaky[.]xyz
- vany[.]xyz
- waky[.]xyz
- wanao[.]xyz
- wanchen[.]xyz

- xacbank[.]net
- xapq[.]com
- xapw[.]xyz
- yaah[.]xyz
- yaaj[.]xyz
- yaat[.]xyz
- zabg[.]xyz
- zabm[.]xyz
- zadh[.]xyz

Sample IP-Connected Domains

- 03b7904b-1b48-4e21-b4c6-b54c69f2ef8c[.]random[.]login-inobxservice[.]com
- 054b1a90-9146-4481-9633-3b80824d3ca2[.]random[.]login-inobxservice[.]com
- 0ad1bd76-66b5-459e-ba4e-6d70b7daabd5[.]random[.]login-inobxservice[.]com
- alexandra[.]login-inobxservice[.]com
- api[.]login-inobxservice[.]com
- argo[.]login-inobxservice[.]com
- b6642a76-5d4a-461f-8f35-ac6a6db5f56e[.]random[.]login-inobxservice[.]com
- b6da028a-7057-44bc-b6e2-363318c06f74[.]random[.]login-inobxservice[.]com
- b89f9d66-edca-4eb8-8aee-82ca9beced15[.]random[.]login-inobxservice[.]com
- c31be329-c497-4570-bcaa-1911d22c3073[.]random[.]login-inobxservice[.]com
- c739d84f-d21e-4059-890d-041e53870f37[.]login-inobxservice[.]com
- cacti[.]login-inobxservice[.]com
- desiflicks[.]com
- e371b9af-8a45-4b4d-affe-2bd57fb53f64[.]random[.]login-inobxservice[.]com
- ec846778-7b6d-4e21-907f-4aec020fd4f0[.]random[.]login-inobxservice[.]com
- email[.]login-inobxservice[.]com
- f3d30855-b968-48c0-ab87-623e96d7b7be[.]random[.]login-inobxservice[.]com
- f4d960a7-07d0-4efd-b47c-47af26cac309[.]random[.]login-inobxservice[.]com
- fjewkwqkevq[.]login-inobxservice[.]com
- get[.]login-inobxservice[.]com
- git[.]login-inobxservice[.]com
- gzolottdlfo[.]login-inobxservice[.]com
- home[.]login-inobxservice[.]com
- hostmaster[.]login-inobxservice[.]com
- i[.]login-inobxservice[.]com
- imagecollection[.]net
- images[.]login-inobxservice[.]com
- jasper[.]login-inobxservice[.]com
- l443barfymc5987oh[.]login-inobxservice[.]com
- localhost[.]login-inobxservice[.]com
- login-inobxservice[.]com
- m[.]login-inobxservice[.]com
- m5[.]login-inobxservice[.]com
- mail[.]login-inobxservice[.]com
- new[.]login-inobxservice[.]com
- ns1[.]login-inobxservice[.]com

- old[.]login-inobxservice[.]com
- pay[.]login-inobxservice[.]com
- pdf-filereviewonline[.]login-inobxservice[.]com
- pop[.]login-inobxservice[.]com
- random[.]login-inobxservice[.]com
- remote[.]login-inobxservice[.]com
- secure[.]login-inobxservice[.]com
- server[.]login-inobxservice[.]com
- sip[.]waybig9[.]gleeze[.]com
- tkwf6g6qc5gsyge7a0[.]login-inobxservice[.]com
- wap[.]login-inobxservice[.]com
- webdisk[.]login-inobxservice[.]com
- webmail[.]login-inobxservice[.]com
- xfjlrx5iki[.]login-inobxservice[.]com

Sample String-Connected Domains

- hfuu[.]audnedaln[.]no
- hfuu[.]cc
- hfuu[.]cf
- hijx[.]cc
- hijx[.]cn
- hijx[.]com
- ikses[.]nl
- ikses[.]pw
- ikses[.]ru
- jiaw[.]aquila[.]it
- jiaw[.]cc
- jiaw[.]club
- lsjb[.]bid
- lsjb[.]biz
- lsjb[.]cc
- raxia[.]ai
- raxia[.]cn
- raxia[.]co[.]kr
- rnl[.]academy
- rnl[.]adv[.]br
- rnl[.]aero
- sqj[.]aero
- sqj[.]airport[.]aero
- sqj[.]am
- tgh24[.]com
- tgh24[.]de
- tgh24[.]ir
- tuo[.]adult
- tuo[.]aero
- tuo[.]agency