Top 10 Malware of Q2 2025: A Deep Dive into the IoCs

Table of Contents

Executive Report

The Center for Internet Security (CIS) Cyber Threat Intelligence (CTI) Team recently published "Top 10 Malware Q2 2025" that not only listed the malware families that took centerstage during the quarter but also their corresponding indicators of compromise (IoCs).

The report identified 62 IoCs for nine of the malware comprising 53 domains and nine IP addresses. Here's a breakdown.

RANK	MALWARE	DESCRIPTION	NUMBER OF DOMAIN IoCs	NUMBER OF IP IoCs
1	SocGholish	Downloader disguised as fake browser updates	12	0
2	ZPHP	Downloader disguised as fake browser updates	5	0
3	AgentTesla	Remote access Trojan (RAT) sold on cybercriminal forums	6	0
4	VenomRAT	RAT distributed via malicious spam	4	0
5	CoinMiner	Cryptocurrency miner either dropped by other malware or distributed via malicious spam	1	0
6	Mirai	Malware botnet for distributed	0	0

		denial-of-service (DDoS) attacks on Internet of Things (IoT) devices		
7	NanoCore	RAT sold on cybercriminal forums distributed via malicious spam	2	3
8	Arechclient2	RAT notable for its evasion tactics	9	6
9	ClearFake	Downloader disguised as fake browser updates	6	0
10	LandUpdate808	Downloader disguised as fake browser updates	8	0

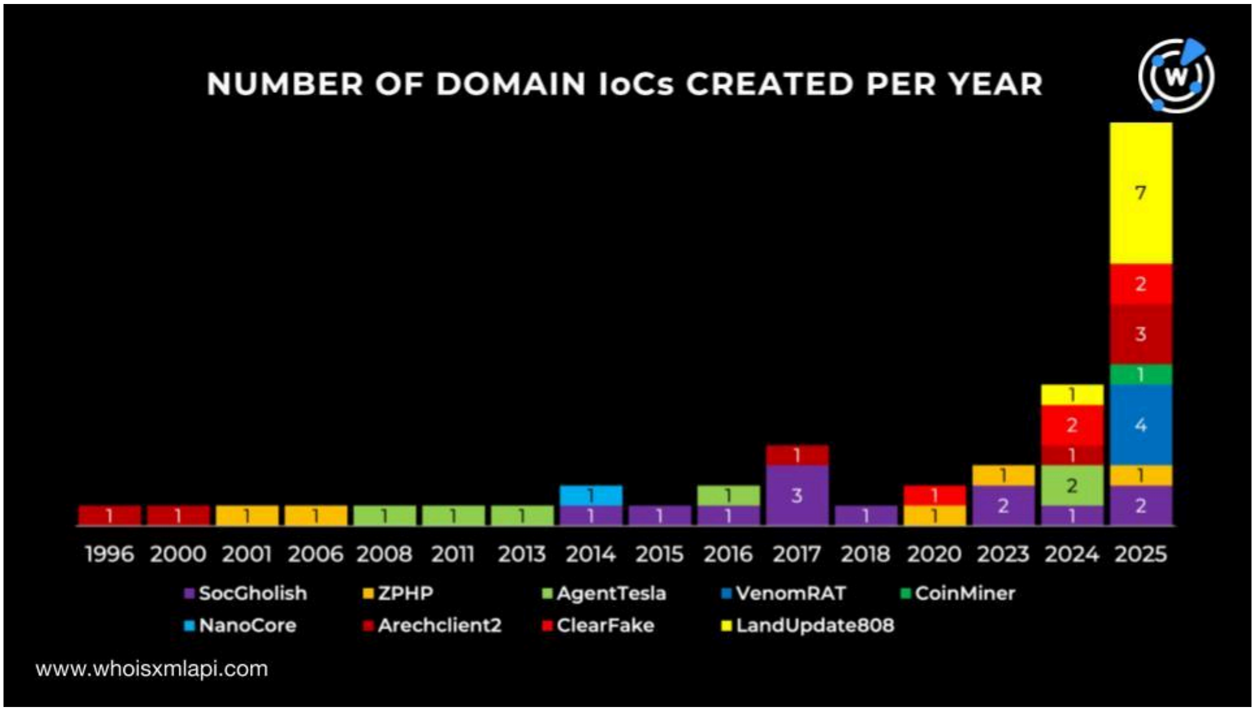
Note that no domains or IP addresses were identified as IoCs for Mirai.

We traced the WHOIS and DNS footprints of the top 10 malware by expanding the list of IoCs. Our in-depth analysis led to the discovery of thousands of new artifacts, namely:

- 72,921 unique client IPs that communicated with some domain IoCs
- Seven domain IoCs appeared on First Watch Malicious Domains Data Feed upon registration
- 34 alleged victim IP records that communicated with some IP IoCs
- 23,996 email-connected domains, 43 were malicious
- 53 additional IP addresses, 33 were malicious
- 431 IP-connected domains, one was malicious
- 1,153 string-connected domains, three were malicious

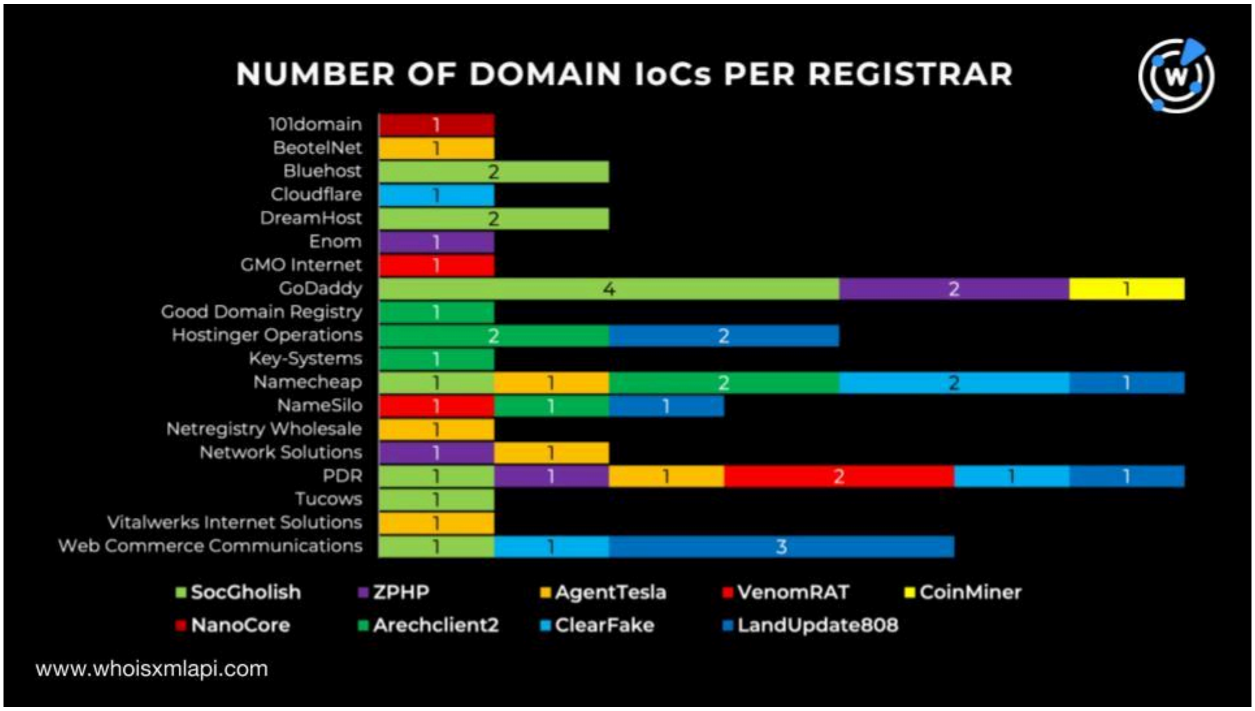
IoC Analysis

We began our investigation by querying each set of domains tagged as IoCs for the nine malware families on Bulk WHOIS API. We discovered that only 49 of the 53 domains tagged as IoCs had current WHOIS records. The 49 domains were created between 26 July 1996 and 25 July 2025. Take a look at their breakdown by year of creation below.

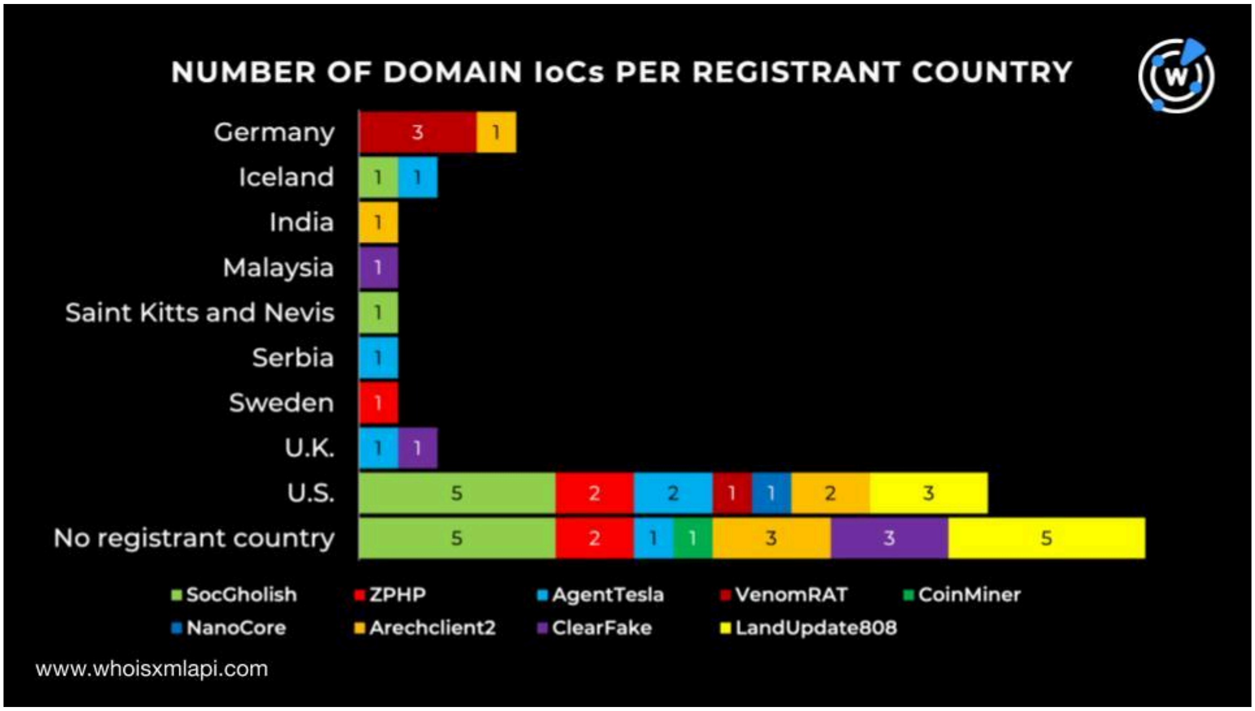


As shown, 20 domains were created in 2025; seven in 2024; four in 2017; three in 2023; two each in 2014, 2016, and 2020; and one each in 1996, 2000, 2001, 2006, 2008, 2011, 2013, 2015, and 2018. The oldest domain—bienvenido[.]com—was associated with Arechclient2 while the newest—xmrminingproxy[.]com—was related to CoinMiner.

A closer look at the registrars of the 49 domains tagged as IoCs revealed that GoDaddy, Namecheap, and PDR topped the list of registrars, accounting for seven domains each. Web Commerce Communications came in second place with five domains followed by Hostinger Operations with four domains. NameSilo placed fourth with three domains. Bluehost, DreamHost, and Network Solutions with two domains each placed fifth. Finally, 101domain, BeotelNet, Cloudflare, Enom, GMO Internet, Good Domain Registry, Key-Systems, Netregistry Wholesale, Tucows, and Vitalwerks Internet Solutions with one domain each completed the roster. Here’s their breakdown.



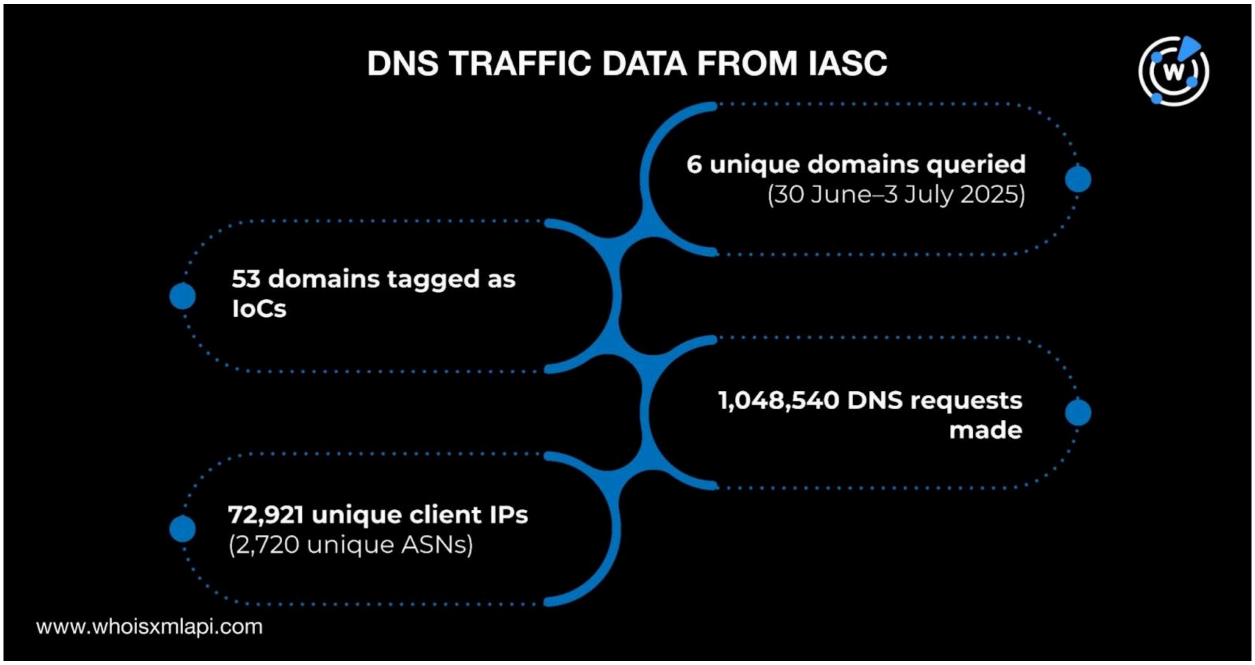
Diving deeper into the 49 domains tagged as IoCs, we found out that while 20 did not have registrant countries on record, the remaining 29 were split across nine nations. The U.S. topped the list, accounting for 16 domains. Germany placed second with four domains followed by Iceland and the U.K. with two each. One domain each was registered in India, Malaysia, Saint Kitts and Nevis, Serbia, and Sweden.



Next, we queried the 53 domains tagged as IoCs on DNS Chronicle API and discovered that only 50 had historical DNS connections. Specifically, the 50 domains posted 8,472 domain-to-IP resolutions from 5 February 2017. Seven domains, in particular, shared this oldest resolution date. Of these seven domains, two each were connected to SocGholish and NanoCore. One domain each, meanwhile, was associated with AgentTesla, Arechclient2, and LandUpdate808. Take a look at more details for five domains below.

DOMAIN IoC	MALWARE	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	FIRST RESOLUTION DATE
cpa2go[.]com	SocGholish	296	23 July 2018
lqsword[.]top	ZPHP	234	3 December 2017
jeepcommerce[.]rs	AgentTesla	292	6 February 2017
xmrminingproxy[.]com	CoinMiner	309	1 January 2018
key-systems[.]net	Arechclient2	498	6 February 2017

We also looked at sample DNS traffic data from the Internet Abuse Signal Collective (IASC) to further analyze the 53 domains tagged as IoCs. The sample data revealed that 72,921 unique client IP addresses tied to 2,720 unique ASNs queried six distinct domains between 30 June and 3 July 2025 via 1,048,540 DNS requests.



DNS TRAFFIC DATA FROM IASC

6 unique domains queried (30 June–3 July 2025)

53 domains tagged as IoCs

1,048,540 DNS requests made

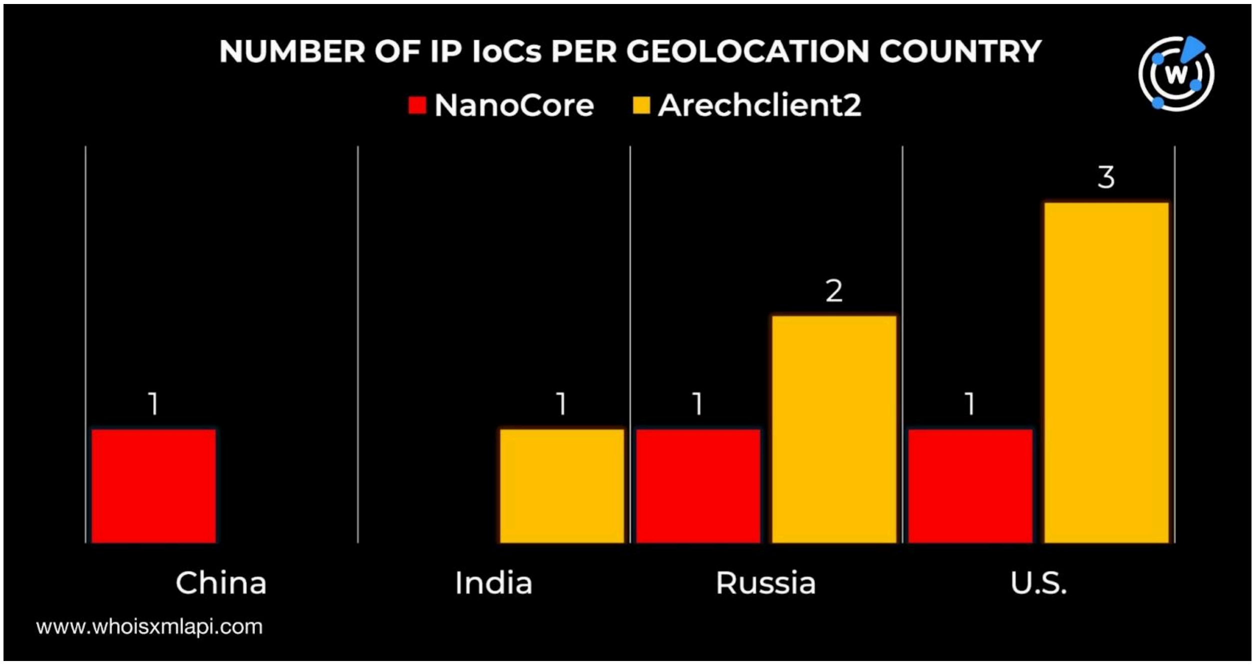
72,921 unique client IPs (2,720 unique ASNs)

www.whoisxmlapi.com

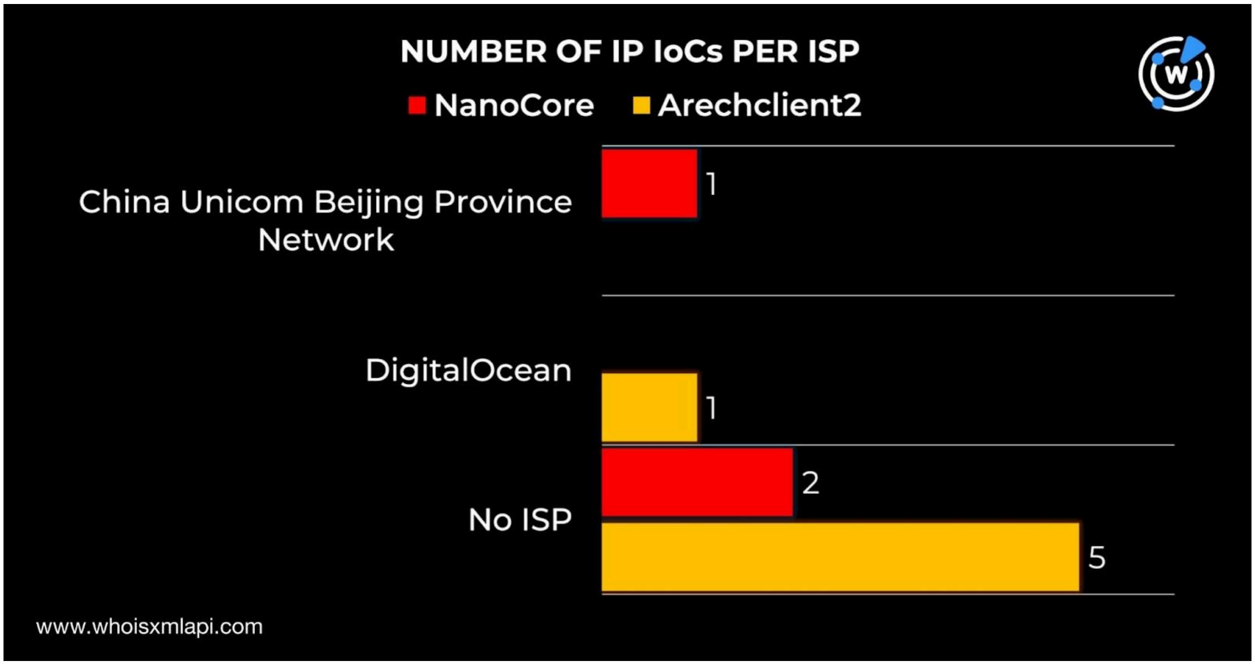
Lastly, we queried the 53 domains tagged as IoCs on First Watch and found that seven appeared on various feeds 31–233 days before they were reported as attack IoCs on 18 July 2025. Take a look at three examples below.

DOMAIN IoC	MALWARE	FIRST WATCH DATE ADDED	NUMBER OF DAYS PRIOR TO REPORTING DATE
emeraldpinesolutions[.]com	SocGholish	17 June 2025	31
sixfiguredigital[.]group	AgentTesla	27 November 2024	233
candyxpdf[.]com	Arechclient2	26 February 2025	142

Afterward, we queried the nine IP addresses tagged as IoCs for NanoCore and Arechclient2 on Bulk IP Geolocation Lookup. A look at their geolocation countries revealed that they were split across four nations topped by the U.S., which accounted for four IP addresses. Russia took the second spot with three IP addresses while one each were geolocated in China and India. Here’s the breakdown.



Further scrutiny of the ISPs of the nine IP addresses tagged as IoCs, meanwhile, showed that while seven did not have ISPs on record, one each was administered by China Unicom Beijing Province Network and DigitalOcean. Take a look at more details below.



A DNS Chronicle API query for the nine IP addresses tagged as IoCs revealed that only seven had historical IP-to-domain resolutions. Specifically, the seven IP addresses recorded 3,704 resolutions since 4 February 2017. Take a look at details for three IP addresses below.

IP IoC	MALWARE	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	FIRST RESOLUTION DATE
193[.]161[.]193[.]99	NanoCore	1,000	27 February 2017
143[.]110[.]230[.]167	Arechclient2	474	6 December 2020
45[.]129[.]86[.]82	Arechclient2	1,000	27 March 2024

In addition, using sample netflow data from the IASC, we further analyzed nine IP addresses that could point to attack command-and-control (C&C) servers. The sample data revealed 34 alleged victim IP records associated with three unique ISPs operating under six ASNs.

The IP IoC 23[.]172[.]40[.]89 proved most interesting in that it communicated with a potential victim IP 60 times via ICMP.

IoC List Expansion Analysis Findings

After uncovering more information about the IoCs, we sought to find more connected artifacts next. We began by querying the 53 domains tagged as IoCs on WHOIS History API and discovered that only 40 had email addresses in their historical WHOIS records. Specifically, we collated 129 unique email addresses. A closer look at the email addresses showed that only 37 could be public.

While none of the 37 public email addresses showed up on other domains' current WHOIS records based on the results of our Reverse WHOIS API query, 30 did on historical WHOIS records. The 30 public email addresses were found in the historical WHOIS records of 23,996 email-connected domains after duplicates and those already tagged as IoCs were filtered out.

A Threat Intelligence API query for the 23,996 email-connected domains revealed that 43 were already considered malicious. Take a look at five examples below.

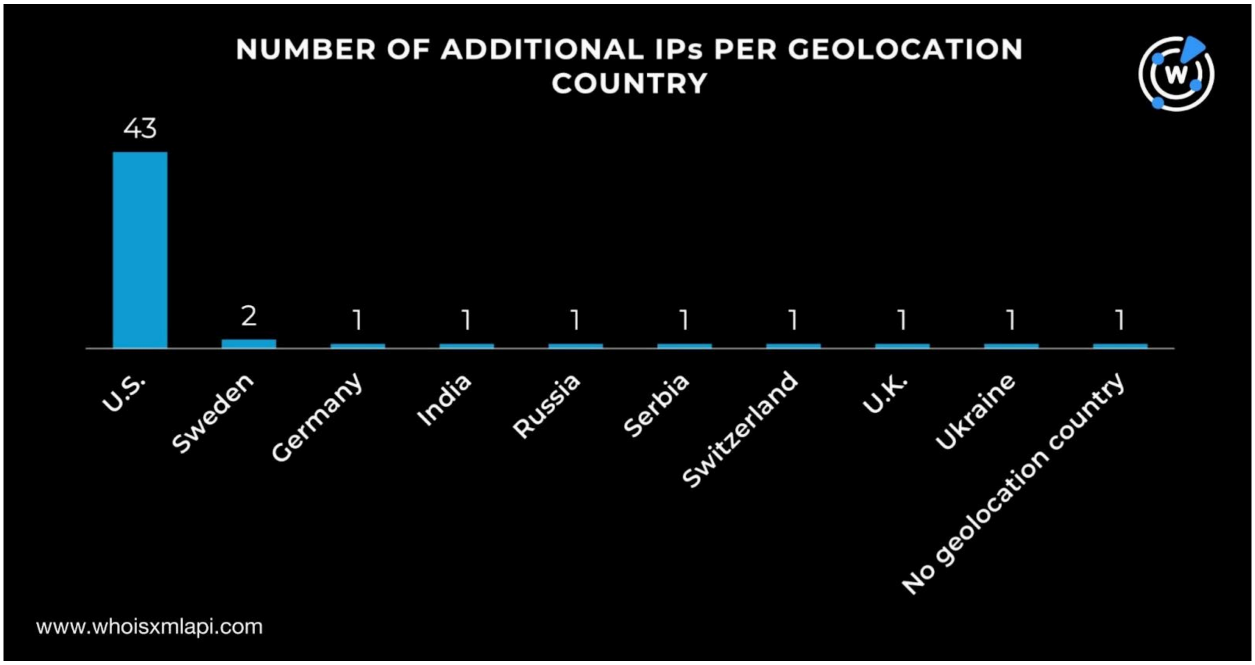
MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREATS
357f[.]com	Malware distribution
akgulemlak[.]com	Malware distribution
biabrasuporte[.]com	Phishing
cdngateway[.]us	Malware distribution
dashboard-aave[.]us	Phishing Generic threat

Next, we queried the 53 domains tagged as IoCs on [DNS Lookup API](). Our search revealed that 42 actively resolved to 53 unique IP addresses after removing duplicates and those already identified as IoCs.

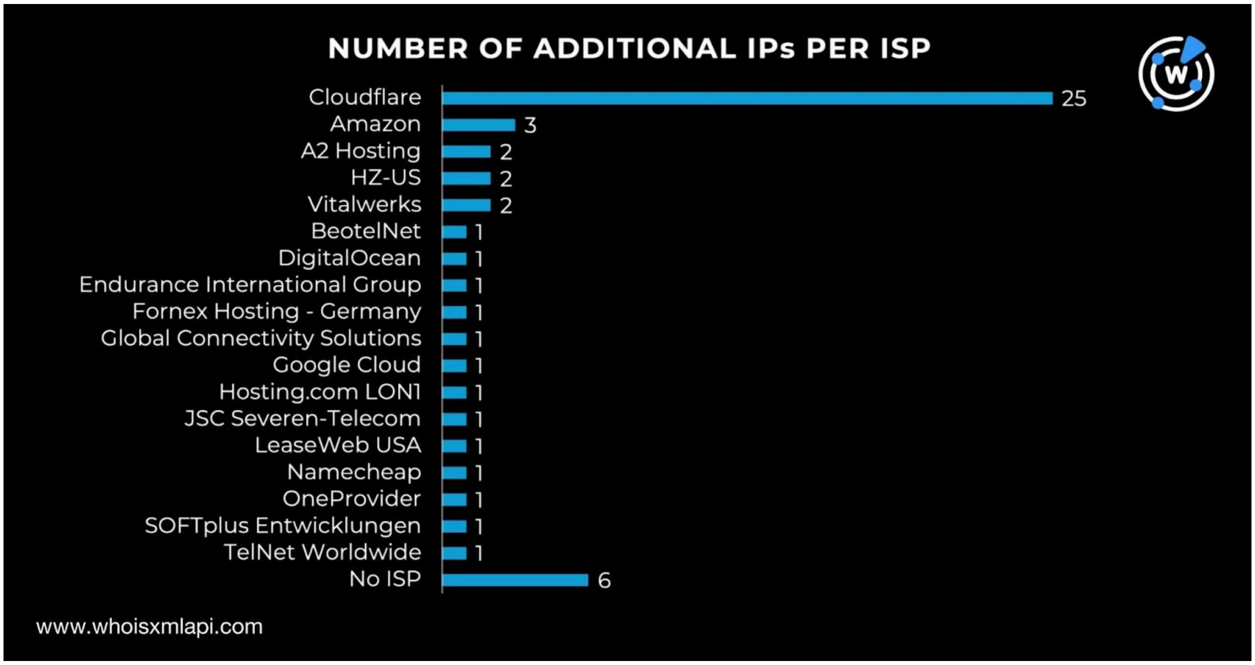
A Threat Intelligence API query for the 53 additional IP addresses showed that 33 have already been weaponized for various attacks. Take a look at five examples below.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREATS
104[.]18[.]21[.]135	Generic threat
15[.]197[.]148[.]33	Phishing Generic threat Malware distribution Suspicious activity Command and control (C&C)
172[.]67[.]128[.]220	Phishing Malware distribution Generic threat
173[.]254[.]31[.]34	Attack Spam campaign Malware distribution
216[.]144[.]210[.]189	C&C

We queried the 53 additional IP addresses on Bulk IP Geolocation Lookup as well and found that while one did not have a geolocation country on record, the 52 remaining IPs were split across nine nations. The U.S. accounted for 43 IP addresses. Sweden took the second spot with two IP addresses. Finally, one IP address each was geolocated in Germany, India, Russia, Serbia, Switzerland, the U.K., and Ukraine.



A closer look at the ISPs, on the other hand, showed that while six IP addresses did not have ISPs on record, the remaining 47 were split across 18 ISPs. Cloudflare took the top spot with 25 IP addresses followed by Amazon with three. Two each were administered by A2 Hosting, HZ-US, and Vitalwerks. Finally, BeotelNet, DigitalOcean, Endurance International Group, Fornex Hosting - Germany, Global Connectivity Solutions, Google Cloud, Hosting.com LON1, JSC Severen-Telecom, LeaseWeb USA, Namecheap, OneProvider, SOFTplus Entwicklungen, and TelNet Worldwide accounted for one IP address each.



Comparing the geolocation country and ISP results for the IP IoCs and additional IP addresses, we noticed these similarities:

- India, Russia, and the U.S.—three of the four geolocation countries of the IoCs—also appeared in the list of origins for the additional IP addresses.
- DigitalOcean—one of the two ISPs for the IoCs—also appeared in the list of administrators for the additional IP addresses.

Adding the 53 IP addresses to the nine already tagged as IoCs, we now had 62 to work with. We queried them on Reverse IP API and discovered that 55 had current domain resolutions. All in all, they resolved 11,499 domains. Further scrutiny also showed that 18 IP addresses could be dedicated hosts. The 18 possibly dedicated IPs hosted 431 IP-connected domains after filtering out duplicates, those already tagged as IoCs, and the email-connected domains.

To date, only one of the 431 IP-connected domains—javascripterhub[.]com—has already figured in malware distribution.

As our last step, we looked more closely at the 53 domains tagged as IoCs and discovered that they had unique text strings. Only 41 of the strings, however, appeared in other domains according to our Domains & Subdomains Discovery searches. The strings were:

- emeraldpinesolutions.
- cpa2go.
- ebuilderssource.
- lanpdt.

- micha.
- roofnrack.
- smthwentwrong.
- stirngo.
- suziestuder.
- symphoniabags.
- lqsword.
- eddereklam.
- islonline.
- jeepcommerce.
- fosna.
- hostsailor.
- myddns.
- sixfiguredigital.
- topendpower.
- bitdefender-download.
- royalbanksecure.
- xmrminingproxy.
- anondns.
- gotdns.
- bienvenido.
- candyxpdf.
- key-systems.
- launchapps.
- ninositsolution.
- bandarsport.
- katuj.
- pages.
- ratatui.
- alhasba.
- edveha.
- jimriehls.
- nypipeline.
- rajjas.
- skatkat.
- swedrent.
- waxworkx.

A total of 1,153 string-connected domains started with the 41 strings above. Note that we removed duplicates, those already tagged as IoCs, and the email- and IP-connected domains from the results.

A Threat Intelligence API query for the 1,153 string-connected domains showed that three have already been dubbed malicious. An example would be pages[.]hk, which was associated with malware distribution.

—

Our more in-depth analysis of the WHOIS and DNS footprints of nine of the top 10 malware of Q2 2025 led to the discovery of 25,633 connected artifacts comprising 23,996 email-connected domains, 53 additional IP addresses, 431 IP-connected domains, and 1,153 string-connected domains. To date, 80 have already been weaponized for various attacks.

Sample DNS traffic data from IASC also revealed that 72,921 unique client IP addresses tied to 2,720 unique ASNs queried six distinct domains between 30 June and 3 July 2025 via 1,048,540 DNS requests. Their sample netflow data, meanwhile, uncovered 34 alleged victim IP records associated with three unique ISPs operating under six ASNs.

Interestingly, seven of the 53 domains tagged as IoCs were deemed likely to turn malicious upon registration by First Watch 31–233 days before they were reported as attack IoCs on 18 July 2025.

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

- 1040amended[.]com
- 1040schedulea[.]com
- 1040scheduleb[.]com
- accountingdegree[.]online
- accountingdoctorate[.]com
- accountingdownriver[.]com
- bachelorsdegreeengineering[.]com
- bachelorsdegreenursing[.]com
- bachelorsineconomics[.]com
- cadsoftwaretraining[.]com
- caduse[.]com
- caekoshagurenope[.]com
- dcsx[.]cn
- dctdesign[.]com
- dctrafficcameras[.]com
- eatingbananas[.]com
- ebankcards[.]com
- ebankingsystem[.]com
- familyplanhealth[.]com
- familysupportsystem[.]com
- familysupportsystems[.]com
- gardenplant[.]org
- garesearch[.]com
- garlinghouse[.]us
- happy-forex[.]com
- happy-prince-sigma[.]com
- happy[.]holiday
- idhtml[.]com
- idie[.]net
- idimark[.]com
- japtrix[.]com
- jasongpt[.]com
- jasonsjungle[.]com
- katourlinewigs[.]com
- katserg[.]com
- kavaklidereemlak[.]com
- lanyardz[.]com
- laohen[.]com
- laomatutou[.]cn
- macversions[.]com
- mad[.]pictures
- madcache[.]com
- ncipm[.]com
- ncpennysaver[.]com
- ncuy[.]com
- oannew[.]com
- oanniphoneapp[.]com
- oannnews[.]net
- partnershipreturn[.]com
- partnershipreturns[.]com
- partnershipstructure[.]com
- qrfactorization[.]com
- qrrr[.]net
- qrups[.]com
- rankedmba[.]com
- rankings[.]best
- ranneymethod[.]com
- sailorshost[.]net
- sailorshosting[.]com
- sailorshosting[.]net
- tasciogluinsaat[.]com
- tascioglutekstil[.]com
- tasdemirinsaat[.]com
- ukxj[.]com
- uky[.]info
- ulasemlak[.]com
- vcoip[.]com
- vcplayer[.]com
- vcqf[.]com
- w7irs[.]com
- w7ojdb[.]cn
- w811[.]com

- xbkvrfn[.]com
- xbookvrf[.]com
- xboxcloudgaming[.]net
- yildizdesign[.]com
- yilmazdegirmenci[.]com
- yilmazemlak[.]net
- zpvf[.]com
- zrfv[.]com
- zrnmm[.]com

Sample Additional IP Addresses

- 104[.]18[.]20[.]135
- 127[.]0[.]0[.]1
- 143[.]110[.]187[.]231
- 146[.]148[.]93[.]148
- 15[.]197[.]148[.]33
- 158[.]247[.]7[.]206
- 172[.]66[.]160[.]99
- 173[.]254[.]31[.]34
- 193[.]111[.]208[.]2
- 195[.]252[.]110[.]253
- 216[.]144[.]210[.]189
- 23[.]105[.]163[.]27
- 3[.]33[.]130[.]190
- 5[.]181[.]161[.]82
- 68[.]65[.]122[.]221
- 77[.]95[.]113[.]182
- 79[.]132[.]141[.]22
- 8[.]23[.]224[.]108
- 85[.]118[.]206[.]137
- 91[.]193[.]19[.]32

Sample IP-Connected Domains

- 88446d14-9ad8-4550-a5bf-9d576316c843[.]random[.]islonline[.]org
- 88clbbiz[.]com
- 938052fb-23c3-4cbb-bacd-05cce73b2cc5[.]random[.]buylocksetsonline[.]com
- admin2[.]seriouslysimplehosting[.]com
- aebbf21e-8b29-43b7-bb9f-7cb1d7c4afe4[.]random[.]enthuse-test[.]com
- akw[.]enthuse-test[.]com
- bbs[.]buyelectricstrikesonline[.]com
- blackhorsecanyon[.]com
- blog[.]buydoorlitesandlouvers[.]com
- cpanel[.]enthuse-test[.]com
- cpanel[.]islonline[.]org
- cpanel[.]securewifiworks[.]com
- dev[.]securewifiworks[.]com
- die[.]ucu[.]edu[.]uy
- dns-service[.]sudo[.]host
- elections[.]danecounty[.]gov
- email[.]pandaexpress[.]com[.]cdn[.]cloudflare[.]net
- enthuse-test[.]com
- ftp[.]ebuildingsource[.]net
- ftp[.]enthuse-test[.]com
- ftp[.]islonline[.]org
- git[.]futa[.]gg
- howfun[.]futa[.]gg
- hsrxnweaworker[.]enthuse-test[.]com
- i[.]futa[.]gg
- javascripterhub[.]com
- kgsewrqzworker[.]enthuse-test[.]com
- kiyvehgbworker[.]enthuse-test[.]com
- ksysuqiaworker[.]enthuse-test[.]com
- laetbjztworker[.]enthuse-test[.]com
- lgd1[.]mira[.]gmk[.]cl
- lgd2[.]mira[.]gmk[.]cl

- momijicf[.]futa[.]gg
- monit[.]seriouslysimplehosting[.]com
- mostynlyons[.]co[.]uk
- n11[.]enthuse-test[.]com
- ncdr[.]futa[.]gg
- newbalancesport[.]top
- onlyfinder[.]co
- order-events-prd[.]pandaexpress[.]com[.]cdn[.]cloudflare[.]net
- order[.]pandaexpress[.]com[.]cdn[.]cloudflare[.]net
- pop[.]seriouslysimplehosting[.]com
- pplex[.]sudo[.]host
- preprod[.]mlj[.]ma
- qlrxspksworker[.]enthuse-test[.]com
- qppfmixiworker[.]enthuse-test[.]com
- quickpoint[.]me
- ralph[.]sudo[.]host
- random[.]securewifiworks[.]com
- remboursementreclamation[.]com
- stats[.]admin[.]buyexitdevicesonline[.]com
- status[.]futa[.]gg
- syncthings[.]sudo[.]host
- thelauniuresidences[.]com
- theteamrobotics[.]com
- thkxyhytworker[.]enthuse-test[.]com
- u[.]enthuse-test[.]com
- uiservices[.]com
- uyqwilhsworker[.]enthuse-test[.]com
- venthoodcleaningtexas[.]com
- vital[.]sh
- vpn1[.]islonline[.]org
- wallabag[.]futa[.]gg
- water[.]futa[.]gg
- webdisk[.]blackhorsecanyon[.]com
- youtubevideo[.]top

Sample String-Connected Domains

- alhasba[.]gifts
- alhasba[.]ws
- anondns[.]ch
- anondns[.]com
- anondns[.]eu
- bandarsport[.]cc
- bandarsport[.]club
- bandarsport[.]co
- bienvenido[.]ai
- bienvenido[.]al
- bienvenido[.]app
- bitdefender-download[.]org
- candyxpdf[.]ph
- cpa2go[.]biz
- cpa2go[.]ca
- cpa2go[.]net
- ebuilderssource[.]net
- eddereklam[.]se
- edveha[.]eu
- edveha[.]nl
- edveha[.]ph
- emeraldpinesolutions[.]ws
- fosna[.]bike
- fosna[.]com
- fosna[.]com[.]cn
- gotdns[.]biz
- gotdns[.]cf
- gotdns[.]cn
- hostsailor[.]accountant
- hostsailor[.]ae
- hostsailor[.]agency
- islonline[.]asia
- islonline[.]at
- islonline[.]be
- jeepcommerce[.]co[.]rs
- jeepcommerce[.]com

- jeepcommerce[.]ga
- jimriehls[.]ph
- katuj[.]info
- katuj[.]link
- katuj[.]tk
- key-systems[.]ac
- key-systems[.]ae
- key-systems[.]af
- lanpdt[.]info
- lanpdt[.]life
- launchapps[.]co
- launchapps[.]co[.]uk
- launchapps[.]com
- lqsword[.]com
- lqsword[.]me
- lqsword[.]net
- micha[.]africa
- micha[.]amsterdam
- micha[.]app
- myddns[.]app
- myddns[.]asia
- myddns[.]be
- ninositsolution[.]sg
- nypipeline[.]org
- nypipeline[.]ph
- pages[.]ab[.]ca
- pages[.]ac
- pages[.]academy
- rajjas[.]co[.]uk
- rajjas[.]loan
- rajjas[.]uk
- ratatui[.]ac[.]ug
- ratatui[.]by
- ratatui[.]cf
- roofnrack[.]com
- roofnrack[.]ph
- royalbanksecure[.]com
- royalbanksecure[.]info
- royalbanksecure[.]sbs
- skatkat[.]ph
- skatkat[.]ws
- smthwentwrong[.]xyz
- stirngo[.]bg
- stirngo[.]eu
- stirngo[.]shop
- suziestuder[.]ws
- swedrent[.]ru
- swedrent[.]se
- topendpower[.]co[.]uk
- topendpower[.]com
- topendpower[.]eu
- waxworkx[.]co[.]uk
- waxworkx[.]ph
- waxworkx[.]ws
- xmrminingproxy[.]ph
- xmrminingproxy[.]ws