A Look Back at the Top 10 Ransomware of 2025

Threat Report

Table of Contents

Executive Report

Back in March 2025, we investigated the DNS footprint of what were dubbed 2025's up and coming ransomware families—RansomHub, LockBit 3.0, Play, Akira, Hunters, Medusa, BlackBasta, Qilin, BianLian, and INC Ransom (aka Lynx). We now looked back at last year's actual threat landscape and discovered that six of them actually made Picus Security's top 10 ransomware list—Qilin, Akira, Play, INC Ransom, Lynx, and RansomHub.

Take a look at brief descriptions of the 10 ransomware featured in this report below, along with the links to the reports we obtained lists of network IoCs from below.

RANK	RANSOMWARE	DESCRIPTION	IoC SOURCE	DATE PUBLISHED
1	Qilin	Also known as "Agenda" and uses advanced techniques, cross-platform variants, and alliances with other major threat groups	https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-agenda	12/31/25
2	Akira	RaaS that emerged in March 2023 that targeted 250+ organizations worldwide	https://thedfirreport.com/2025/11/04/from-bing-search-to-ransomware-bumblebee-and-adaptixc2-deliver-akira-2/	08/07/25
3	Cl0p	Often targets the critical infrastructure, financial, and government sectors using encryptionless tactics to steal data and demand ransoms without encrypting files	https://theravenfile.From Bing Search to Ransomware: Bumblebee and AdaptixC2 Deliver Akira - The DFIR Reportcom/2025/11/04/clop-ransomware-dissecting-network/	11/04/25
4	Play	Known for infiltrating companies via exposed RDP servers and exploiting vulnerabilities	https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/	05/18/25
5	INC Ransom	Known for highly	https://www.trendmicr	01/15/26

		aggressive, rapid, and targeted attacks against enterprises in the healthcare, manufacturing, education, and government sectors primarily in North America and Europe	o.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-inc	
6	SafePay	Operates with a centralized non-RaaS model and frequently executes attacks within a 24-hour window using double-extortion tactics	https://www.acronis.com/en/tru/posts/safepay-ransomware-the-fast-rising-threat-targeting-msps/	07/08/25
7	Lynx	Widely considered a rebranded and more advanced variant of INC Ransom that focuses on double extortion tactics targeting SMBs and large organizations across sectors primarily in the U.S. and the U.K.	https://thedfirreport.com/2025/12/17/cats-got-your-files-lynx-ransomware/	11/19/25
8	RansomHub	Known for operating as a cartel, it lets affiliates keep up to 90% of the ransom payment, attracting experienced threat actors	https://thedfirreport.com/2025/06/30/hide-your-rdp-password-spray-leads-to-ransomhub-deployment/	07/01/25
9	DragonForce	Operates by leasing to affiliates who conduct attacks through double-extortion tactics	https://www.acronis.com/en/tru/posts/the-dragonforce-cartel-scattered-spider-at-the-gate/	11/05/25
10	Babuk2	Suspected to be led by the actor known as	https://www.rapid7.com/blog/post/2025/04/	04/02/25

		"Bjorka," it uses the notorious Babuk brand to perpetrate extortion through recycled data	02/a-rebirth-of-a-cursed-existence-the-babuk-locker-2-0/	

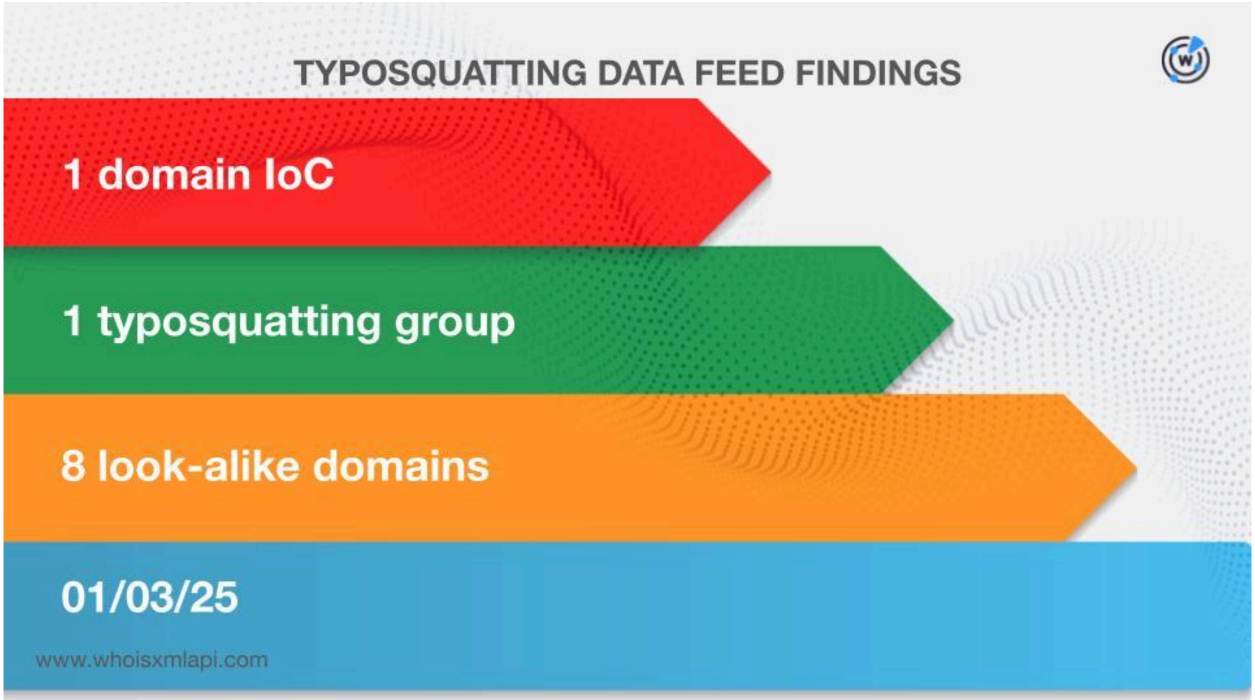
With the aid of the WhoisXML API MCP Server, we extracted domains from the subdomains identified as IoCs and weeded out those that belonged to legitimate entities, did not leave DNS traces behind, and were only accessible via the Dark Web. After that, we were left with 267 network IoCs comprising 28 domains, 236 IP addresses, and three email addresses for our analysis, which led to these discoveries:

- One domain identified as an IoC bulk-registered with eight look-alikes
- Three domains classified as IoCs likely registered with malicious intent
- 2,626 unique potential victim IP addresses communicated with 40 distinct IP addresses tagged as IoCs
- 8,491 email-connected domains, 36 of which were deemed malicious
- Nine additional IP addresses, eight of which were dubbed malicious
- 713 IP-connected domains, 75 of which were named malicious
- 324 string-connected domains, two of which were categorized as malicious

Divulging More Discoveries about the Domain IoCs Related to 6 Ransomware

Note that while we collated 29 domains identified as IoCs for analysis for six of the top 10 ransomware, one domain was tagged as an IoC for two ransomware variants.

We began our investigation by scouring the Typosquatting Data Feed for signs of the 28 domains. We discovered that the domain simplerwebs[.]world connected to INC Ransom was bulk-registered with eight look-alikes on 3 January 2025.

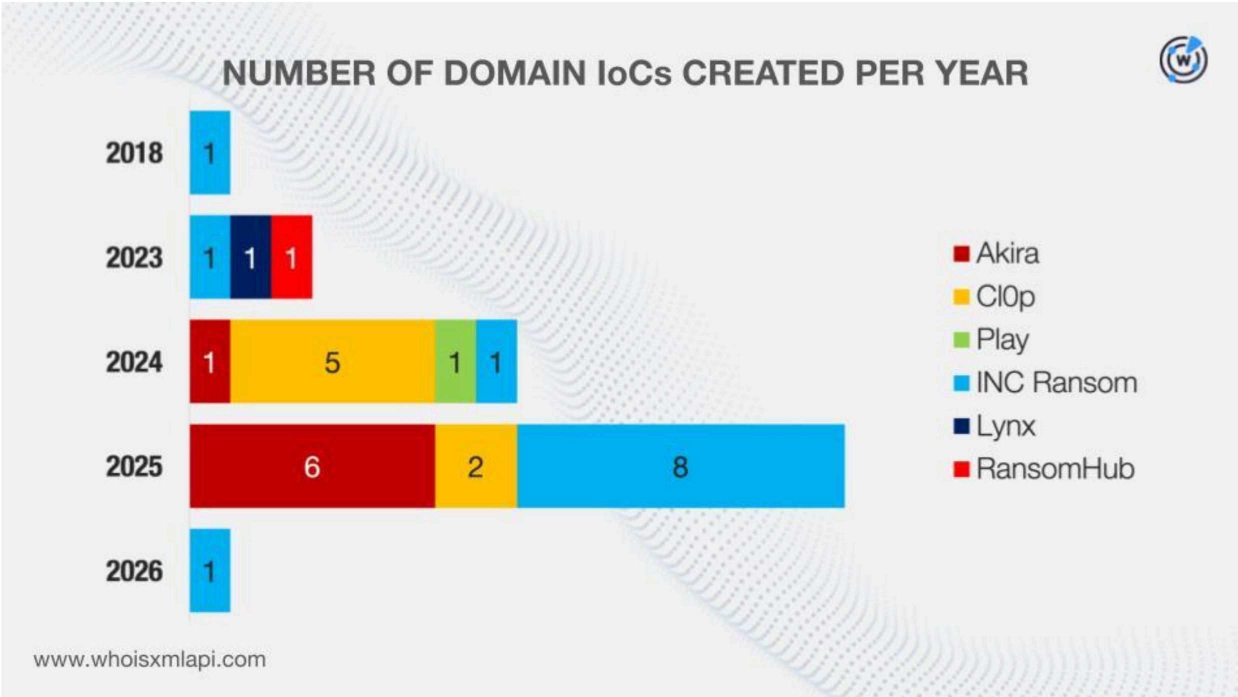


Next, we sought to find out if any of the 28 domains were likely registered with malicious intent from the get-go. We discovered that three domains related to Akira were tagged as malicious 15–37 days before they were reported as such on 7 August 2025. Here are more details about them.

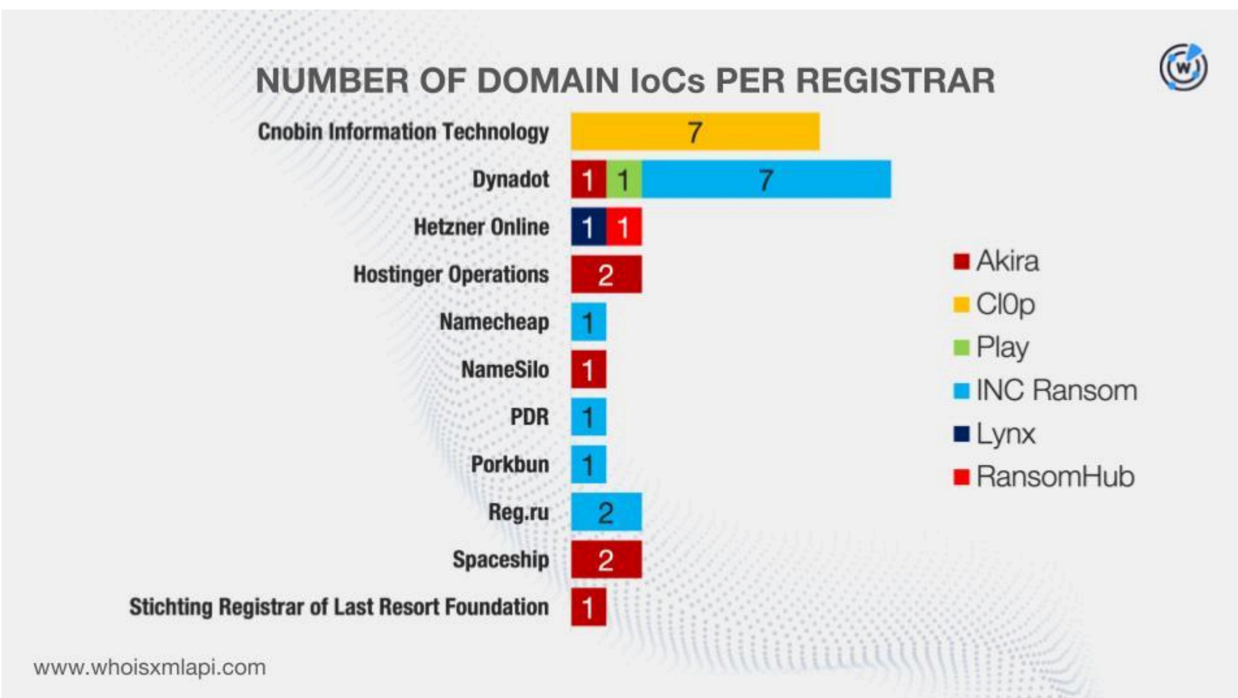
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE THE REPORT DATE
2rxyt9urhq0bgj[.]org	07/01/25	37
ev2sirbd269o5j[.]org	07/09/25	29
ijt0l3i8brit6q[.]org	07/23/25	15

We then queried the 29 domains on WHOIS API and learned that:

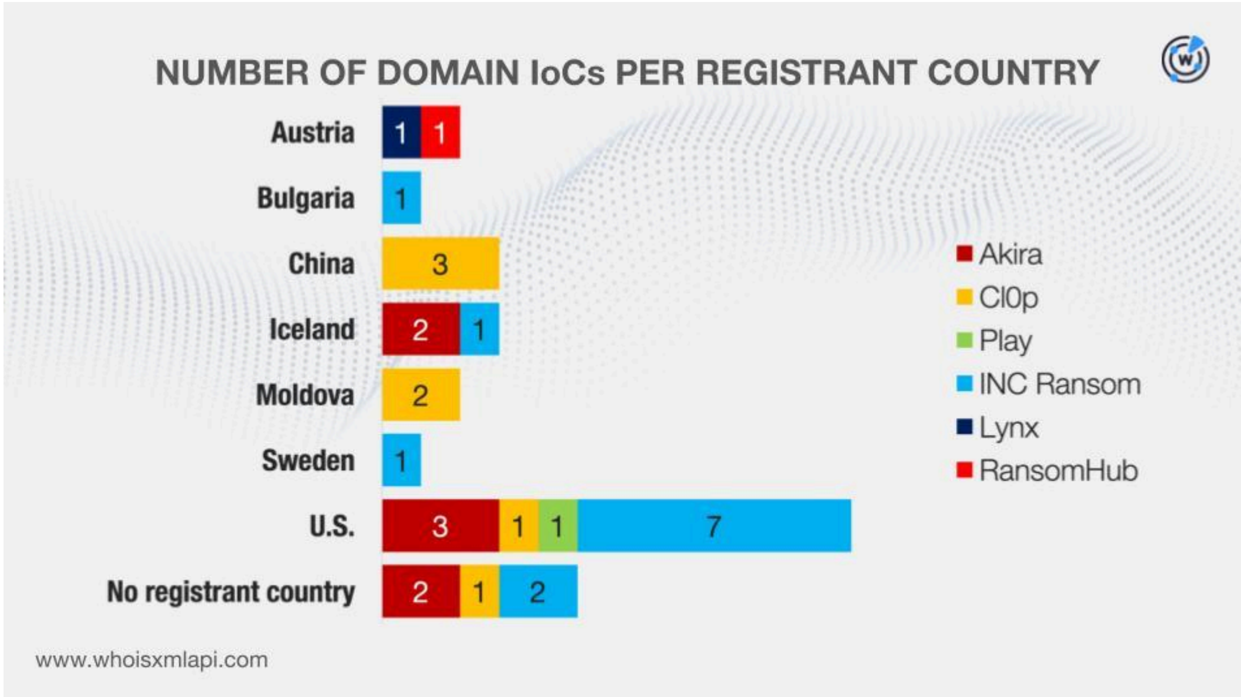
- They were created between 8 November 2018 and 25 February 2026. Note that the oldest and news domains were both associated with a single ransomware—INC Ransom.



- They were administered by 11 registrars.



- While six domains did not have registrant countries on record, the remaining 23 were registered in seven countries.



DNS Chronicle API queries for the 28 domains revealed that they recorded 2,728 historical domain-to-IP resolutions over time. Take a look at more information on five domains with the oldest resolution dates below.

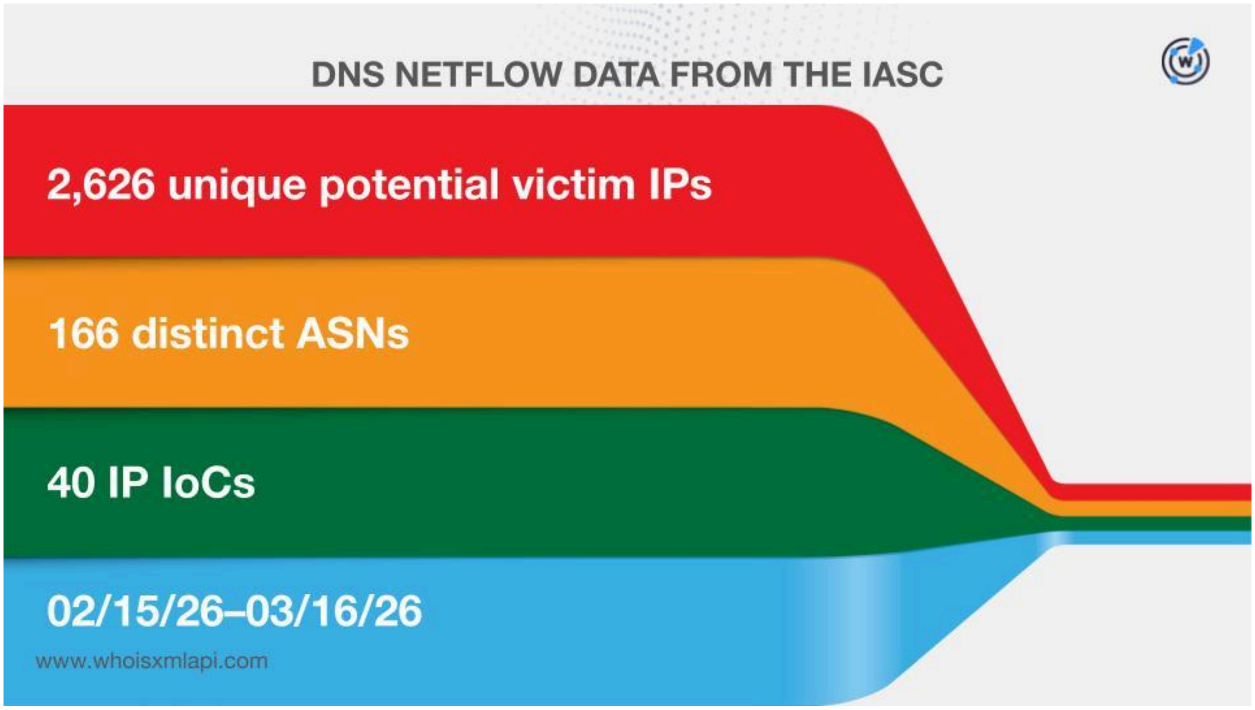
RANSOMWARE	DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
Cl0p	in2pay[.]com	229	02/06/17–03/12/26
Cl0p	pubstorm[.]com	116	02/06/17–01/25/26
Akira	angryipscanner[.]org	114	06/02/17–06/04/25
Cl0p	he1p-center[.]com	61	11/04/17–05/06/25
Akira	opmanager[.]pro	59	08/24/18–06/16/25

It is interesting to note that the five domains with the oldest resolution dates above were also affiliated with two of the oldest ransomware variants that made the top 10. Cl0p has been around since 2019 while Akira has been active since 2023.

Investigating the IP IoCs Connected to 8 Ransomware

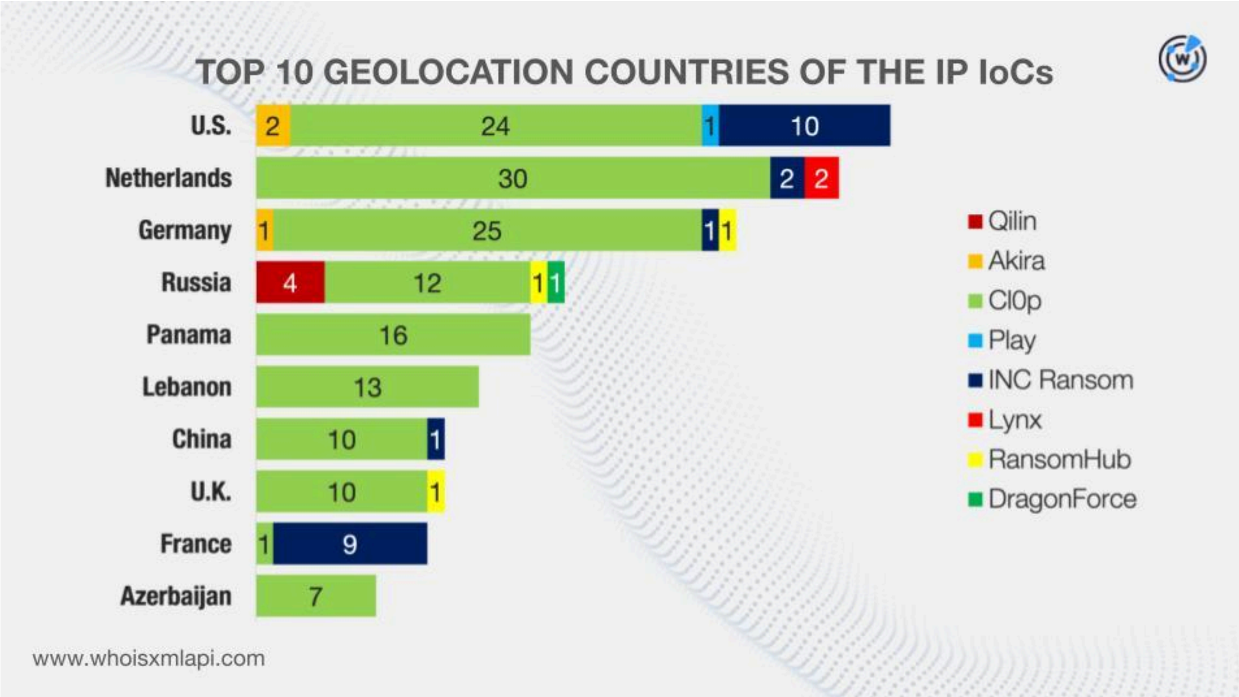
The reports connected to eight of the top 10 ransomware also identified 236 IP addresses as IoCs.

Sample network traffic data from the IASC revealed that 2,626 unique potential victim IP addresses under 166 distinct ASNs communicated with 40 of the IP IoCs between 15 February and 16 March 2026.

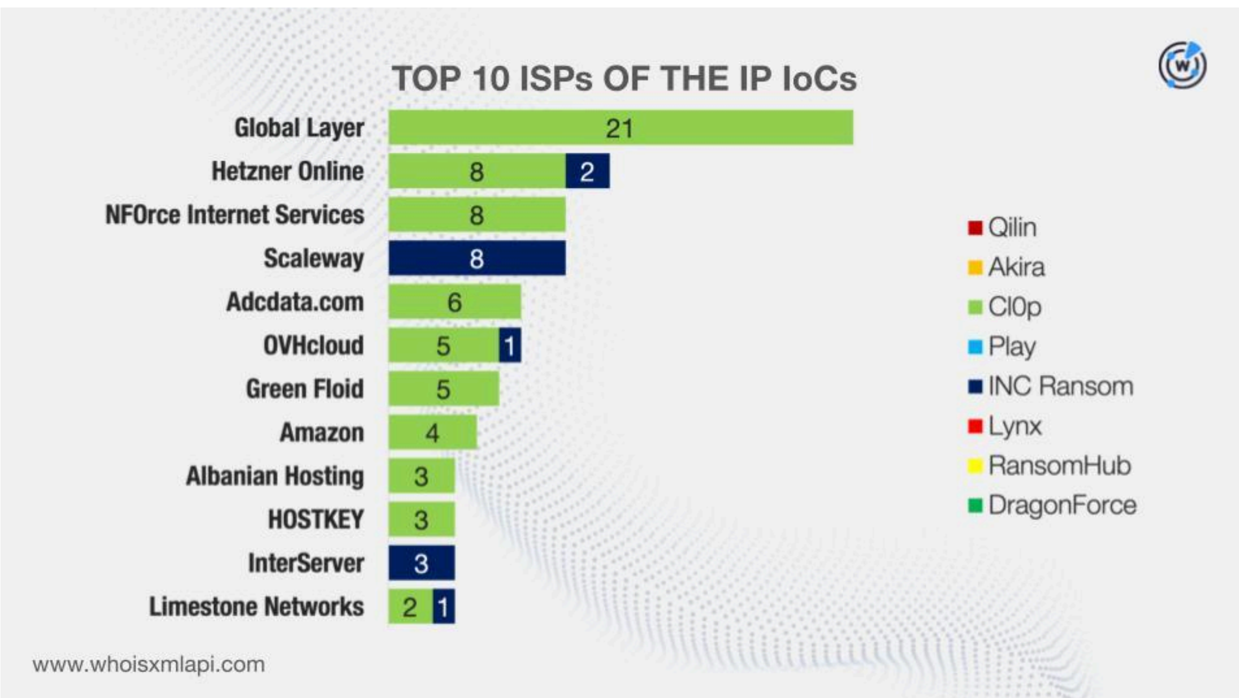


We then queried the IP addresses on Bulk IP Geolocation Lookup and found out that:

- They were geolocated in 33 countries. And it is worth noting that four of the geolocation countries were also named as registrant countries of some of the domains tagged as IoCs.



- While 122 IP addresses did not have ISPs on record, the remaining 114 were administered by 39 ISPs.



DNS Chronicle API queries for the IP addresses showed that 160 recorded 25,643 IP-to-domain resolutions over time. Here are more details for five examples.

RANSOMWARE	IP IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	DATES SEEN
Cl0p	46[.]161[.]27[.]113	27	02/05/17–10/29/22
INC Ransom	212[.]83[.]137[.]94	650	02/05/17–10/21/25
RansomHub	164[.]138[.]90[.]2	258	02/05/17–08/25/24
Qilin	176[.]113[.]115[.]209	223	11/01/20–01/17/26
Akira	109[.]205[.]195[.]21	172	07/02/25–08/04/25

Interestingly, all of the IP addresses with the oldest resolution dates were connected to the oldest ransomware in the top 10 list—Cl0p.

Evaluating the Email IoCs Associated with 3 Ransomware

We also collated three email addresses affiliated with three ransomware for this study.

Our checks via the WhoisXML API MCP Server revealed that two were worth avoiding all forms of communication with specifically because they contained the names of two notorious ransomware—Qilin and Babuk. They also showed that none of them were used to register any domain, hence they will no longer appear in the next steps of our analysis.

According to our prompt results, for instance, while the email address named as an IoC qilin@exxxxxx[.]im was correctly formatted and not a catch-all, disposable, or free email address, the SMTP check showed it could not currently receive mail, meaning the mailbox may not be active or blocks SMTP verification. Also, while it was not necessarily tagged as malicious, users should note that Qilin is a well-known RaaS group. As such, the username "qilin' could indicate it belongs to an actor operating in cybercriminal circles likely on or affiliated with the group.

Amassing New Artifacts Affiliated with the Top 10 Ransomware of 2025

For this step, we only focused on the 28 domains and 236 IP addresses identified as IoCs.

First, we queried the domains on WHOIS History API and discovered that 16 had 49 email addresses in their historical WHOIS records. Further scrutiny showed that 12 were public email addresses.

Our Reverse WHOIS API queries for the public email addresses led to the discovery of 8,491 unique email-connected domains after those already tagged as IoCs were filtered out.

Threat Intelligence API queries for the email-connected domains then revealed that 36 have already been weaponized for various attacks. Take a look at five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
acrislegt[.]su	Malware distribution	09/09/25–03/16/26
angryipscanner[.]net	Malware distribution	09/14/23–03/16/26
averiryvx[.]su	Malware distribution	09/09/25–03/16/26
basilicros[.]su	Malware distribution	01/02/26–03/16/26
bendavo[.]su	Malware distribution	09/26/25–03/16/26

We also queried the domains on DNS Lookup API and found out that 11 actively resolved nine IP addresses that were not part of our IoC list.

Threat Intelligence API queries for the additional IP addresses showed that eight have already figured in malicious campaigns. Here are more details on five examples.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
103[.]224[.]182[.]253	Phishing Malware distribution Generic threat Spam campaign C&C	03/28/23–03/31/26 03/29/23–03/30/26 03/28/23–03/08/26 04/14/23–02/10/26 04/05/23–01/03/26
34[.]209[.]195[.]255	C&C Malware distribution Generic threat	06/11/25–03/30/26 06/11/25–03/30/26 06/13/25–03/26/26

104[.]21[.]30[.]173	Malware distribution Phishing	08/29/24–03/30/26 07/18/23–03/30/26
172[.]67[.]173[.]121	Phishing Malware distribution	07/18/23–03/31/26 08/29/24–03/30/26
34[.]229[.]166[.]50	Malware distribution C&C	03/15/25–03/30/26 03/15/25–03/29/26

At this point, we had 245 IP addresses for further investigation. We queried them on Reverse IP API and learned that 47 were currently in use. Of these, 40 could be dedicated IP addresses, and together they hosted 713 IP-connected domains after filtering out those already named as IoCs and the email-connected domains.

Threat Intelligence API queries for the IP-connected domains revealed that 75 have already been classified as malicious. Take a look at more information on five examples below.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
archlnr[.]qpon	Malware distribution	09/13/25–03/30/26
atalozv[.]qpon	Malware distribution	09/13/25–03/30/26
banabmw[.]qpon	Malware distribution	09/13/25–03/30/26
basehce[.]qpon	Malware distribution	09/13/25–03/30/26
batonra[.]qpon	Malware distribution	09/09/25–03/30/26

As our final step, we looked more closely at the domains dubbed as IoCs and extracted 27 unique text strings. We then searched for other domains that started with these strings using Domains & Subdomains Discovery and found out that 21 had connections. Here are some sample strings.

- 2rxyt9urhq0bgj.
- angryipscanner.
- axiscamerastation.
- ip-scanner.
- opmanager.
- cl-leaks.
- he1p-me.
- in2pay.
- pubstorm.
- americajobmail.
- blast-hubs.

Our hunt led to the discovery of 324 string-connected domains after those already categorized as IoCs and the email- and IP-connected domains were filtered out. Note, however, that these 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.

Threat Intelligence API queries for the string-connected domains showed that two have already figured in malicious campaigns. An example would be nestlecompany[.]world that was associated with malware distribution between 18 February 2025 and 30 March 2026.

Wrapping Up Our Findings for the Top 10 Ransomware of 2025

Our DNS deep dive into the 267 network IoCs connected to the top 10 ransomware of 2025 revealed that one domain identified as an IoC was bulk-registered with eight look-alikes. In addition, three domains tagged as IoCs were likely registered with malicious intent from the get-go. On top of that, 2,626 potential victim IP addresses communicated with 40 of the IP addresses dubbed as IoCs.

We also uncovered 9,537 new artifacts comprising 8,491 email-connected domains, nine additional IP addresses, 713 IP-connected domains, and 324 string-connected domains. It is worth noting that 121 of these newly unearthed artifacts have already been weaponized for various 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

- acrislegt[.]su
- angryipscanner[.]net
- averiryvx[.]su
- basilicros[.]su
- bendavo[.]su
- boustrn[.]su
- broguenko[.]su
- cerasatvf[.]su
- consnbx[.]su
- conxmsw[.]su
- coverxyzer[.]su
- descroej[.]su
- diadtuky[.]su
- exposqw[.]su
- familyriwo[.]su
- hammernew[.]su
- heavylussy[.]su
- homuncloud[.]su
- iosif-brodskiy[.]su
- iranbar[.]org
- izzardtow[.]su
- korney-chukovsky[.]su
- lumma-market[.]su
- narroxp[.]su
- ozonelf[.]su
- phrupmv[.]su
- prebwle[.]su
- sirhirssg[.]su
- spoar[.]org[.]in
- squatje[.]su
- squeaue[.]su
- telephoned[.]su
- todoexy[.]su
- vicareu[.]su
- whitepepper[.]su
- yuriy-gagarin[.]com
- 000111[.]com[.]tw
- 0034expat[.]com
- 003xxw[.]cn
- 004xxw[.]cn
- 005xxw[.]cn
- 006xxw[.]cn
- 007carteblanchebentley[.]com
- 007xxw[.]cn
- 008xxw[.]cn
- 009xxw[.]cn
- 011xxw[.]cn
- 012xxw[.]cn
- 013xxw[.]cn
- 014xxw[.]cn
- 015xxw[.]cn
- 01shops[.]com
- 02138mag[.]com
- 021espai[.]com
- 0317gz[.]cn
- 0335zx[.]cn
- 0597666[.]com
- 070829[.]com
- 080xxw[.]cn
- 081xxw[.]cn
- 082xxw[.]cn
- 083xxw[.]cn
- 084xxw[.]cn
- 085xxw[.]cn
- 086xxw[.]cn
- 087xxw[.]cn
- 088xxw[.]cn
- 089xxw[.]cn
- 090xxw[.]cn
- 091xxw[.]cn
- 092xxw[.]cn
- 093xxw[.]cn
- 094xxw[.]cn
- 095xxw[.]cn

- 09soutai[.]com
- 0bugatti[.]com
- 0career[.]com
- 0rbitalis[.]com
- 0scat[.]com
- 0tutor[.]com
- 0webroot[.]com
- 0xx[.]info
- 10-bit[.]com
- 1000sofrugs[.]com
- 1008611[.]info
- 100jpegs[.]com
- 100ncy[.]cn
- 101[.]bg
- 101selfhelpsuccessmotivation[.]com
- 1029thegame[.]com
- 1057crushfm[.]com
- 108chaju[.]com
- 10jq[.]info
- 111ccc[.]cn
- 11qz[.]cn
- 12-ladouce[.]com
- 121marketing[.]at
- 127xxw[.]cn
- 128xxw[.]cn
- 129xxw[.]cn

Sample Additional IP Addresses

- 103[.]224[.]182[.]253
- 34[.]209[.]195[.]255
- 104[.]21[.]30[.]173
- 172[.]67[.]173[.]121
- 34[.]229[.]166[.]50

Sample IP-Connected Domains

- archlnr[.]qpon
- atalozv[.]qpon
- banabmw[.]qpon
- basehce[.]qpon
- batonra[.]qpon
- bondixa[.]qpon
- brainnrk[.]com
- cadqdwk[.]qpon
- caressv[.]qpon
- convysj[.]qpon
- corrierede[.]com
- corrieredella-serada[.]com
- curdlep[.]qpon
- detachs[.]qpon
- dishine[.]qpon
- dmybfje[.]qpon
- finikoa[.]qpon
- fiobmzv[.]qpon
- flnsyfb[.]qpon
- franceinffo[.]com
- grewbix[.]qpon
- heothjg[.]qpon
- herwdwy[.]qpon
- infonrk[.]com
- lamboey[.]qpon
- leafleg[.]qpon
- leffdigaro[.]com
- lefighahro[.]info
- lefihagrro[.]top
- lefiharo[.]info
- lefphigaro[.]info
- legisld[.]qpon
- lephfigron[.]pro
- lifsnbu[.]qpon
- minrkhub[.]com
- neextgaz1a[.]info
- nexxtgaz1a[.]info
- nexxtgaz1a[.]top

- nexxtgaze1a[.]info
- nexxtgaze1ta[.]top
- nexxtgaze1ta[.]xyz
- nexxtgazea[.]info
- nexxtgazea[.]top
- nexxtgazea[.]xyz
- nexxtgazetta[.]xyz
- notbibaboaofllflaoti[.]com
- notbubabolklkfofof[.]com
- notcardskoflfkfkfkfk[.]com
- notdominolofpakf[.]com
- notyouwithwihtepowe[.]com
- nuvixohub[.]com
- nyttignrk[.]com
- openrk[.]com
- ourwithwihtepowe[.]com
- outfiqh[.]qpon
- pancred[.]qpon
- provaiy[.]qpon
- repubblicska[.]info
- rtsm[.]xyz
- sculcib[.]qpon
- smashaj[.]qpon
- smeartj[.]bet
- srf-ch-dails[.]com
- srfchance[.]com
- srfgoals[.]com
- stepvss[.]qpon
- stupide[.]qpon
- suctso[.]asia
- support-serv[.]xyz
- syapboc[.]qpon
- telegram[.]services
- unitkgt[.]qpon
- unregun[.]qpon
- veicqxq[.]qpon
- whwwthi[.]qpon
- 038d159d-b3bc-44dd-a0c4-bec68c0c4123[.]random[.]7563489583[.]duckdns[.]org
- 097[.]kh[.]ua
- 1[.]tor-exit[.]nothingtohide[.]nl
- 1539b74c-7254-49c6-a544-1a4421fd7ee2[.]random[.]7563489583[.]duckdns[.]org
- 176-113-115-209[.]plesk[.]page
- 1ecf3864-418d-4c0c-82ed-cfa865e5657f[.]random[.]dere[.]win
- 1fef3895-f2e4-4d89-ad5b-d3c9c347092f[.]random[.]7563489583[.]duckdns[.]org
- 30a93cdb-762a-4bab-88bb-2d03a5fc5a46[.]random[.]7563489583[.]duckdns[.]org
- 391bd779-5fc3-4323-8380-9749d2c78944[.]random[.]tube-plant[.]com
- 3acf7e2c-4e51-4088-883e-6b948c7daa9f[.]random[.]7563489583[.]duckdns[.]org
- 406c81fc-a9dc-42cd-b3a6-0701479fd018[.]random[.]hostednetworks[.]in
- 457f411c-3e51-4f1e-ae47-2395fb9002e1[.]random[.]hostednetworks[.]in
- 4841a27a-aeca-4563-9acf-b84bd2e4a572[.]random[.]tube-plant[.]com
- 4aadf1ce-b64e-45a1-a934-6fd670a849f8[.]random[.]temple[.]is
- 4im5pv76[.]ibxos[.]it
- 51909de5-4091-48af-9f31-74075d71ecbe[.]random[.]temple[.]is
- 53e2e72e-92ec-45bd-b5bf-5230e35c1564[.]random[.]54-39-133-41[.]plesk[.]page
- 5dcee785-e6e0-48e7-915c-74e6e3093a88[.]random[.]7563489583[.]duckdns[.]org
- 5dcee785-e6e0-48e7-915c-74e6e3093a88[.]random[.]temple[.]is

- 64d6e6ec-1ae7-4ff0-bd55-ba2ca39bb55c[.]random[.]temple[.]is
- 68db8bac-b722-4166-acf7-39ec612fe20a[.]random[.]7563489583[.]duckdns[.]org
- 68db8bac-b722-4166-acf7-39ec612fe20a[.]random[.]temple[.]is
- 68db8bac-b722-4166-acf7-39ec612fe20a[.]random[.]tube-plant[.]com
- 8a466c81-277d-4947-8e1e-bca99b62ed88[.]random[.]dere[.]win
- 8f1df85e-ad29-44f1-baec-d0e39c3860ee[.]random[.]temple[.]is

Sample String-Connected Domains

- nestlecompany[.]world
- simplerwebs[.]online
- 2rxyt9urhq0bgj[.]ws
- americajobmail[.]ws
- angryipscanner[.]com
- angryipscanner[.]fr
- angryipscanner[.]tk
- axiscamerastation[.]com
- axiscamerastation[.]xn--55qx5d[.]cn
- blast-hubs[.]ph
- blast-hubs[.]pro
- blast-hubs[.]ws
- blastikcn[.]ph
- blastikcn[.]ws
- cl-leaks[.]cloud
- generalmills[.]ai
- generalmills[.]app
- generalmills[.]asia
- he1p-me[.]bio
- in2pay[.]ru
- in2pay[.]shop
- ip-scanner[.]co
- ip-scanner[.]co[.]bb
- ip-scanner[.]com
- mercharena[.]ai
- mercharena[.]com
- mercharena[.]cz
- nestlecompany[.]com
- nestlecompany[.]info
- nestlecompany[.]online
- nikolay-romanov[.]ru
- nikolay-romanov[.]site
- opmanager[.]aquila[.]it
- opmanager[.]ch
- opmanager[.]cn
- pubstorm[.]site
- rhussois[.]ph
- rhussois[.]ws
- simplerwebs[.]click
- simplerwebs[.]com
- simplerwebs[.]ph
- stormlegue[.]ph
- stormlegue[.]ws
- telete[.]am
- telete[.]bar
- telete[.]cc
- tttttt[.]app
- tttttt[.]asia
- tttttt[.]bid