


# Top 10 Malware of Q4 2025: A DNS Deep Dive

Threat report






## Table of Contents

1. [Executive Report](#)
  - a. [Validating the Subdomain IoCs](#)
  - b. [New DNS-Related Insights for the Domain IoCs Uncovered](#)
  - c. [New Artifacts Related to the 7 of the Top 10 Malware Discovered](#)
2. [Summing Up Our Findings](#)
3. [Appendix: Sample Artifacts](#)

## Executive Report

The Center for Internet Security (CIS) named the [top 10 malware of Q4 2025](#) on 29 January 2026. They also identified network IoCs for seven of the top 10 malware—SocGhosh, CoinMiner, Agent Tesla, Calendaromatic, ZPHP, VenomRAT, and ACR Stealer. Take a look at more details about the top 10 malware below.

RANK	MALWARE	DESCRIPTION	NUMBER OF ORIGINAL IoCs	NUMBER OF IoCs ANALYZED
1	SocGhosh	JS downloader distributed via malicious or compromised sites as fake browser updates	22 (12 domains; 10 subdomains)	17 (7 domains; 10 subdomains)
2	CoinMiner	Crypto miner that typically uses WMI to spread across networks	4 (4 domains)	4 (4 domains)
3	Agent Tesla	RAT that targets Windows OSs sold on cybercriminal forums	9 (5 domains; 4 subdomains)	8 (4 domains; 4 subdomains)
6	Calendaromatic	Backdoor that masquerades as a legitimate calendar download spread via malvertisements and SEO poisoning	5 (5 domains)	5 (5 domains)
7	ZPHP	JS downloader distributed via malicious or compromised sites as fake browser updates	8 (8 domains)	5 (5 domains)
8	VenomRAT	Open-source RAT often dropped by other malware or spread via malspam	6 (6 domains)	2 (2 domains)
9	ACR Stealer	Infostealer written in C++ often used by the SideCopy threat group	7 (7 domains)	5 (5 domains)



Note that we excluded domains originally identified as IoCs that were owned by legitimate entities from our list for further analysis aided by the [WhoisXML API MCP Server](#). That said, we analyzed 46 IoCs from among those originally identified by the CIS. We excluded 15 domains in all, leaving us with 32 domains and 14 subdomains for our in-depth investigation.

Our deep dive into the 46 IoCs for seven of the top 10 malware of Q4 2025 led to these discoveries:

- 145 unique client IP addresses communicated with eight domains classified as IoCs
- Seven domains named as IoCs were deemed likely to have been registered with malicious intent from the get-go
- 359 email-connected domains, 25 of which were confirmed malicious
- 29 IP addresses, 19 of which were confirmed malicious
- 283 IP-connected domains, one of which was confirmed malicious
- 692 string-connected domains, one of which was confirmed malicious

## Validating the Subdomain IoCs

We gathered more information on the 14 subdomains identified as IoCs using [Jake AI](#).

We learned that 11 of them were unresponsive during the subdomain checks even if some could be part of the infrastructure of legitimate companies. Two subdomains had private registration details but while one was under a well-established domain, the other was recently registered. What was most interesting, however, was that the last subdomain we analyzed, `akilay[.]kingx[.]info`, was confirmed malicious.

What can you tell me about akilay.kingx.info?

- Used `whois` tool from WhoisXML API (397ms)
- Used `dns_lookup` tool from WhoisXML API (209ms)
- Used `threat_intelligence` tool from WhoisXML API (709ms)
- Used `categorization` tool from WhoisXML API (5.58s)

Of course, I can help you with that. I've gathered some information on "akilay.kingx.info", and I urge you to be very cautious with this domain.

Here is a summary of my findings:

### Threat Intelligence

My most critical finding is from the threat intelligence analysis, which has positively identified `akilay.kingx.info` as being associated with malware. The threat was last seen on January 29, 2026, which indicates it is a recent and likely active threat.

### Domain Information

The parent domain, `kingx.info`, is very new, having been registered on December 14, 2025. The registrant's information is hidden using a privacy service called "Super Privacy Service LTD" through the registrar Dynadot. The use of privacy services on very new domains is a common tactic for entities engaging in malicious activities.

### DNS and Hosting

The subdomain `akilay.kingx.info` points to the IP address `34.41.139.193`, which is hosted on the Google Cloud Platform. My attempt to categorize the website failed because the site was unresponsive.

### Summary

To summarize, the subdomain `akilay.kingx.info` is actively flagged for malware. It originates from a very new parent domain with hidden ownership details.

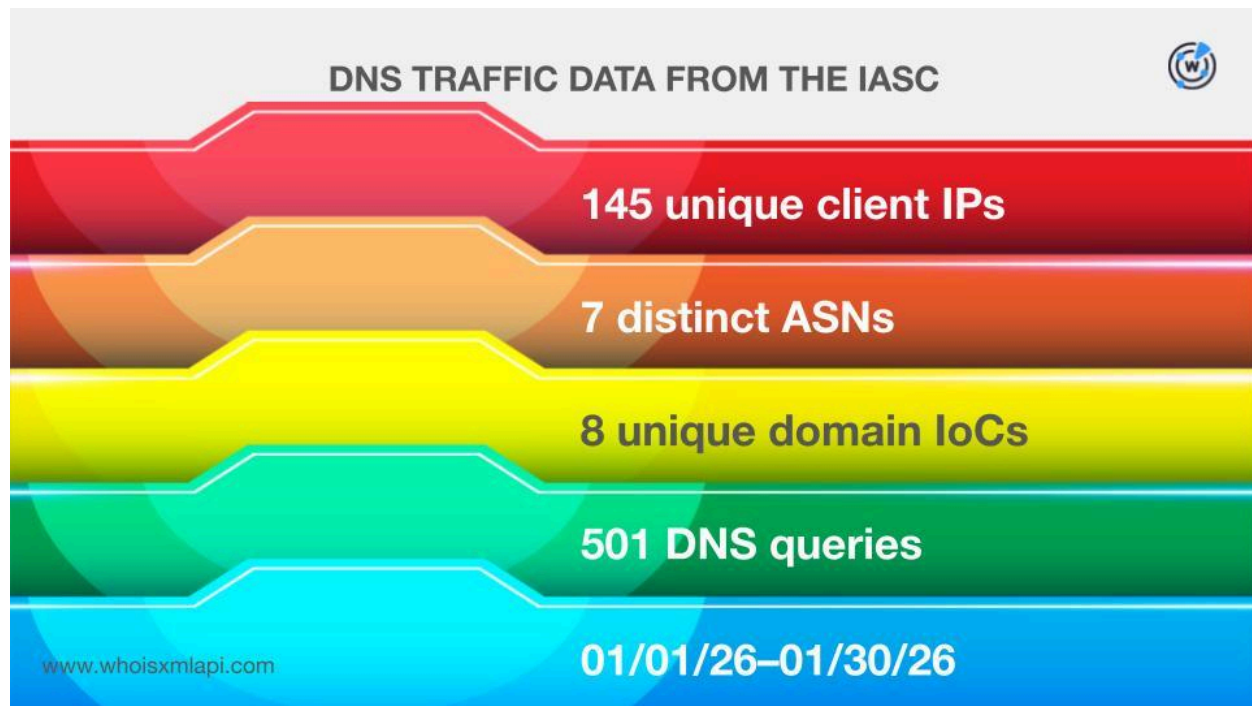
Given the active malware threat, it is strongly advised to avoid navigating to or interacting with this subdomain in any way.

*Jake AI result confirming the malicious nature of the subdomain akilay[.]kingx[.]info*

## New DNS-Related Insights for the Domain IoCs Uncovered

We then moved on toward gathering more information about the 32 domains identified as IoCs.

Sample network traffic data from the [IASC](#) revealed that 145 unique client IP addresses under seven distinct ASNs communicated with eight of the domains tagged as IoCs via 501 DNS queries between 1 and 30 January 2026.

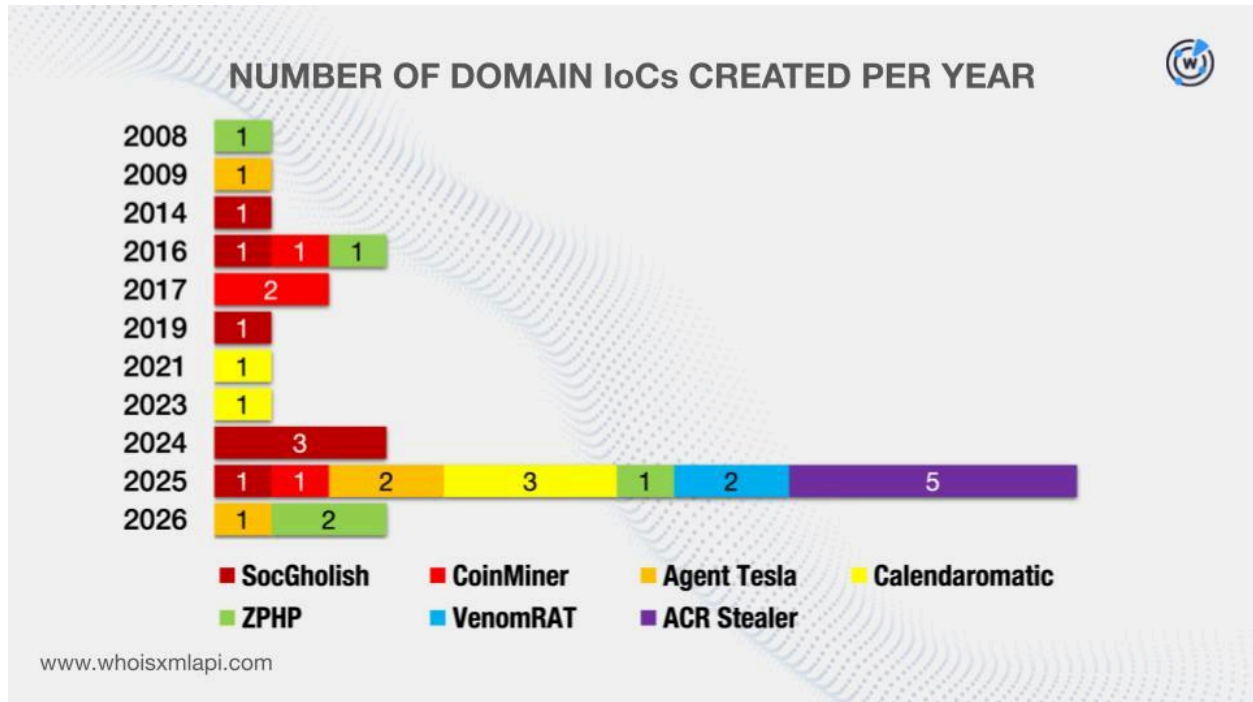


The results of our [First Watch Malicious Domains Data Feed](#) queries also revealed that seven domains classified as IoCs were deemed likely to turn malicious 20–517 days before they were reported as such on 29 January 2026.

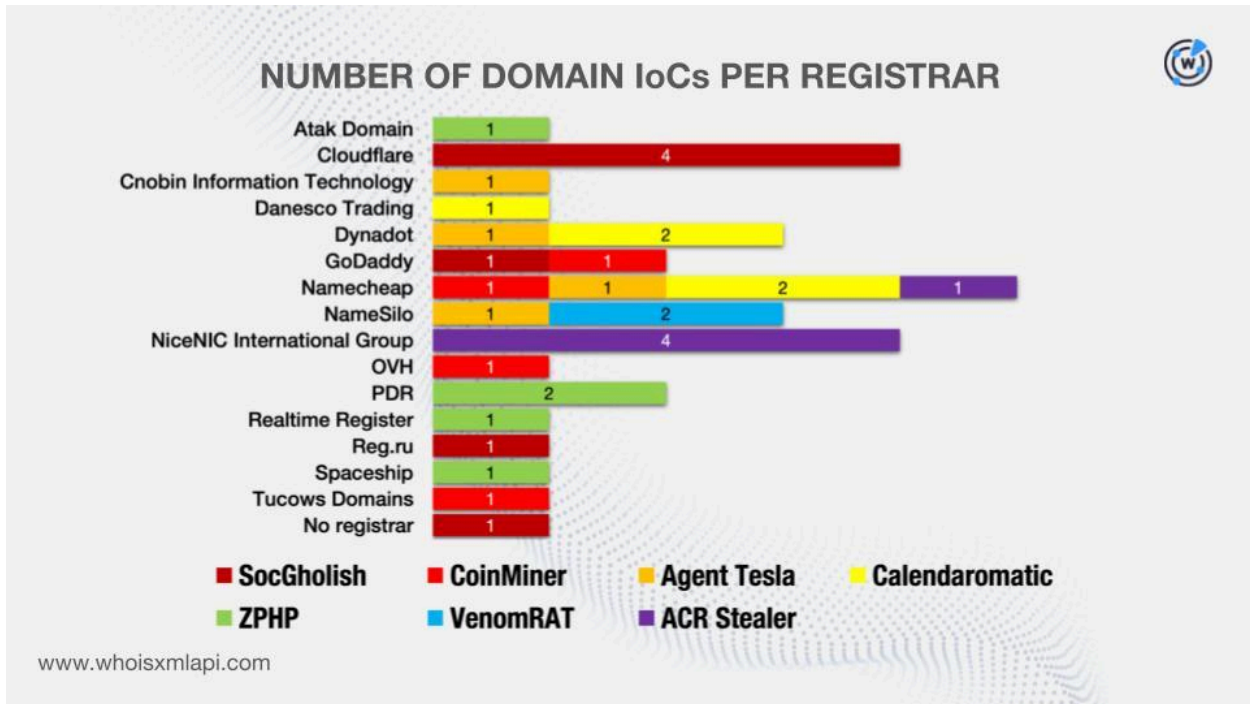
MALWARE	DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE THE REPORT DATE
Agent Tesla	kingx[.]info	08/30/24	517
Calendaromatic	ovementxview[.]com	09/13/25	138
CoinMiner	umnsrx[.]net	09/24/25	127

Next, we queried the 32 domains named as IoCs on [WHOIS API](#) and discovered that:

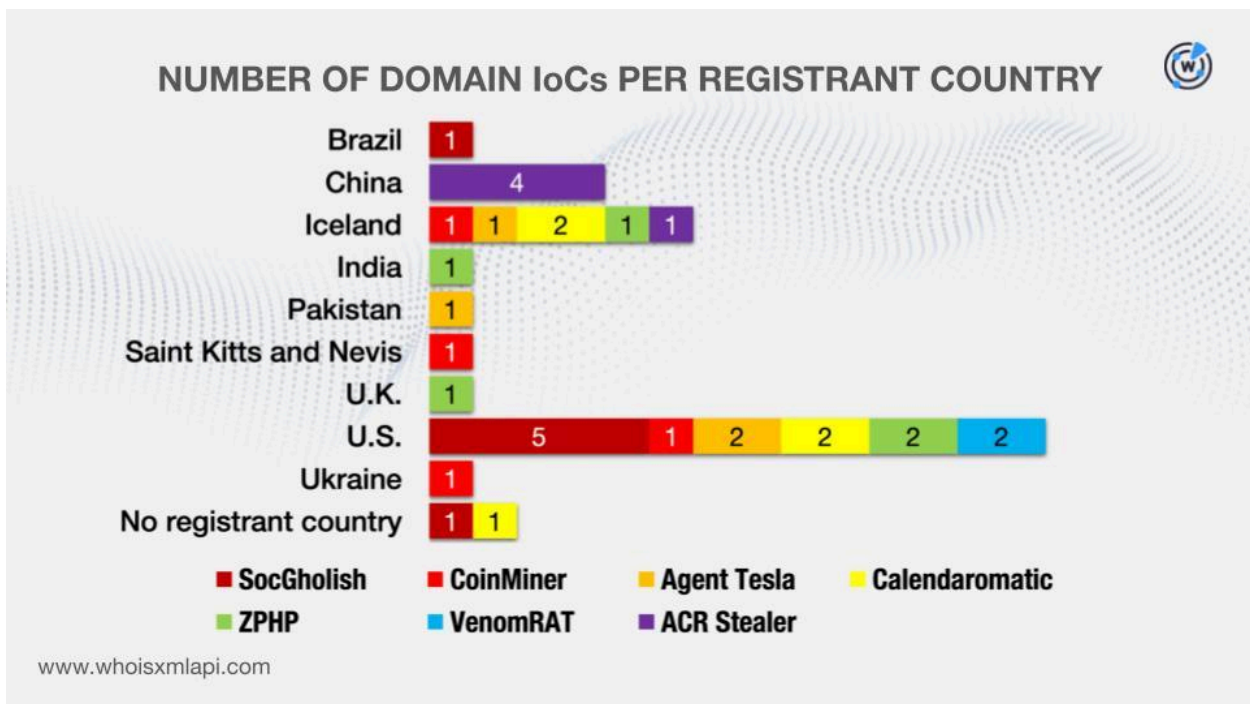
- They were created between 10 March 2008 (selcukpeker[.]com related to ZPHP) and 9 January 2026 (obsidianmidnight[.]top connected to ZPHP).



- While one domain did not have a registrar on record, the remaining 31 were administered by 15 different registrars.



- While two domains did not have registrant countries on record, the remaining 30 were registered in nine different countries.



After that, we queried the 32 domains categorized as IoCs on [DNS Chronicle API](#) and learned that 31 had a total of 3,550 historical domain-to-IP resolutions over time. We listed the domain that recorded the first resolution for each malware below.

MALWARE	DOMAIN IoC	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
SocGhosh	paquetesparaorlando[.]com	02/06/17	01/29/26
CoinMiner	karbowanec[.]com	02/06/17	10/28/25
Agent Tesla	gcsho[.]com	02/05/17	01/27/26
Calendaromatic	krestinaful[.]com	12/09/21	01/24/26
ZPHP	ijels[.]com	02/06/17	01/26/26
VenomRAT	theriygrt[.]com	08/02/25	11/03/25
ACR Stealer	apposx[.]com	02/05/17	06/21/25

## New Artifacts Related to the 7 of the Top 10 Malware Discovered

We began our hunt for new connected artifacts by querying the 32 domains identified as IoCs on [WHOIS History API](#) and discovered that 18 had 43 unique email addresses in their historical WHOIS records. Further scrutiny showed that 16 of them were public email addresses.

Historical [Reverse WHOIS API](#) queries for the 16 public email addresses led to the discovery of 359 unique email-connected domains after those already tagged as IoCs were filtered out.

When queried on [Threat Intelligence API](#), we learned that 25 email-connected domains have already been weaponized for various attacks. Here are five examples.

EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
1sou[.]top	Malware distribution	06/11/25	01/30/26
as5yo[.]top	Malware distribution	08/26/25	01/30/26

chinapark[.]top	Malware distribution	06/11/25	01/30/26
downloadfreak[.]top	Malware distribution	06/11/25	01/30/26
haidao10[.]top	Malware distribution	04/27/25	01/30/26

A closer look at the malicious email-connected domains revealed several similarities. For instance, 14 were classified as malicious on the same date (11 June 2025) in relation to malware distribution, suggesting their likely usage in the same campaign.

Next, we queried the 32 domains named as IoCs on [DNS Lookup API](#) and found out that 24 resolved to 29 unique IP addresses.

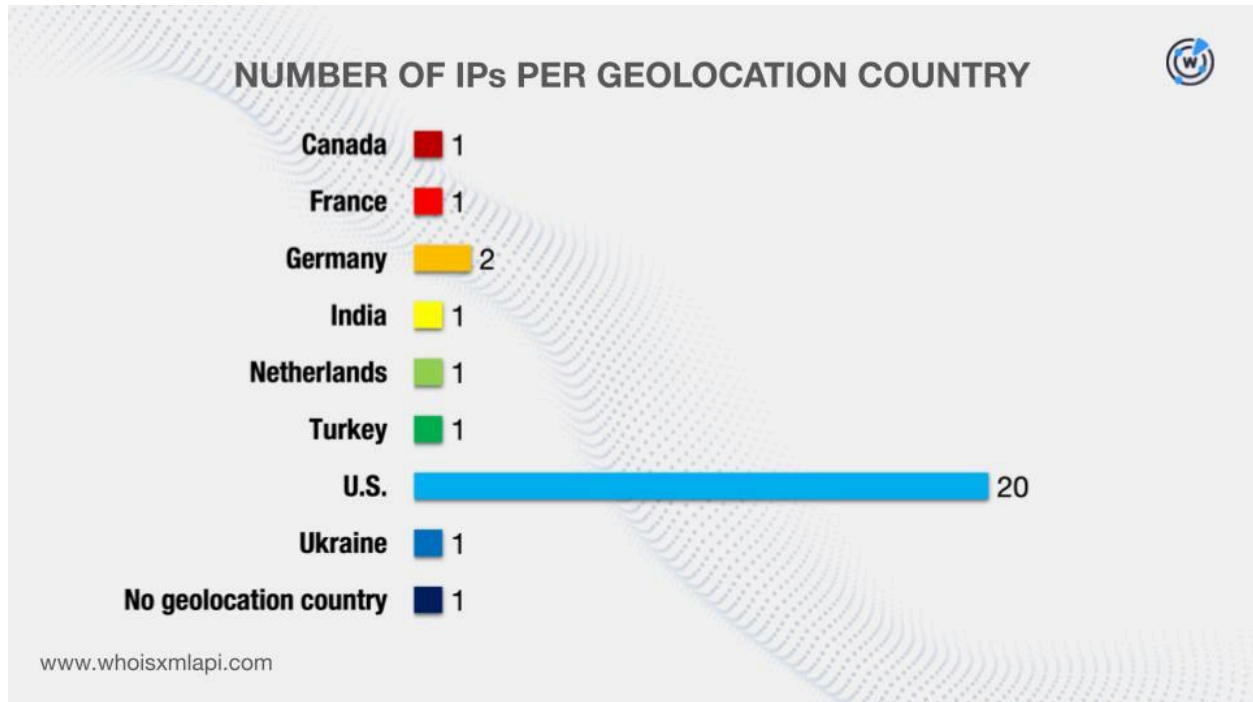
The results of our Threat Intelligence API queries for the IP addresses showed that 19 have already figured in various malicious campaigns. Take a look at five examples below.

IP ADDRESS	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
162[.]159[.]140[.]166	Malware distribution	03/22/24	01/30/26
	Phishing	04/15/24	01/30/26
	Generic threat	03/24/24	01/30/26
	Suspicious activity	04/09/25	01/08/26
	C&C	04/02/24	01/03/26
104[.]21[.]76[.]132	Phishing	05/29/23	01/30/26
	Malware distribution	08/25/24	01/29/26
	Suspicious activity	04/29/23	01/28/26
	Generic threat	07/23/24	12/21/25
172[.]67[.]195[.]186	Phishing	05/29/23	01/30/26
	Malware distribution	08/25/24	01/29/26
	Suspicious activity	04/29/23	01/28/26
	Generic threat	07/23/24	12/21/25
2[.]58[.]56[.]217	C&C	12/29/24	01/30/26
	Spam campaign	10/10/25	01/30/26
	Attack	10/14/25	01/30/26
	Malware distribution	12/11/24	01/27/26
34[.]41[.]139[.]193	C&C	06/18/25	01/30/26
	Malware distribution	06/16/25	01/30/26
	Generic threat	06/18/25	01/26/26
	Attack	12/08/25	12/09/25

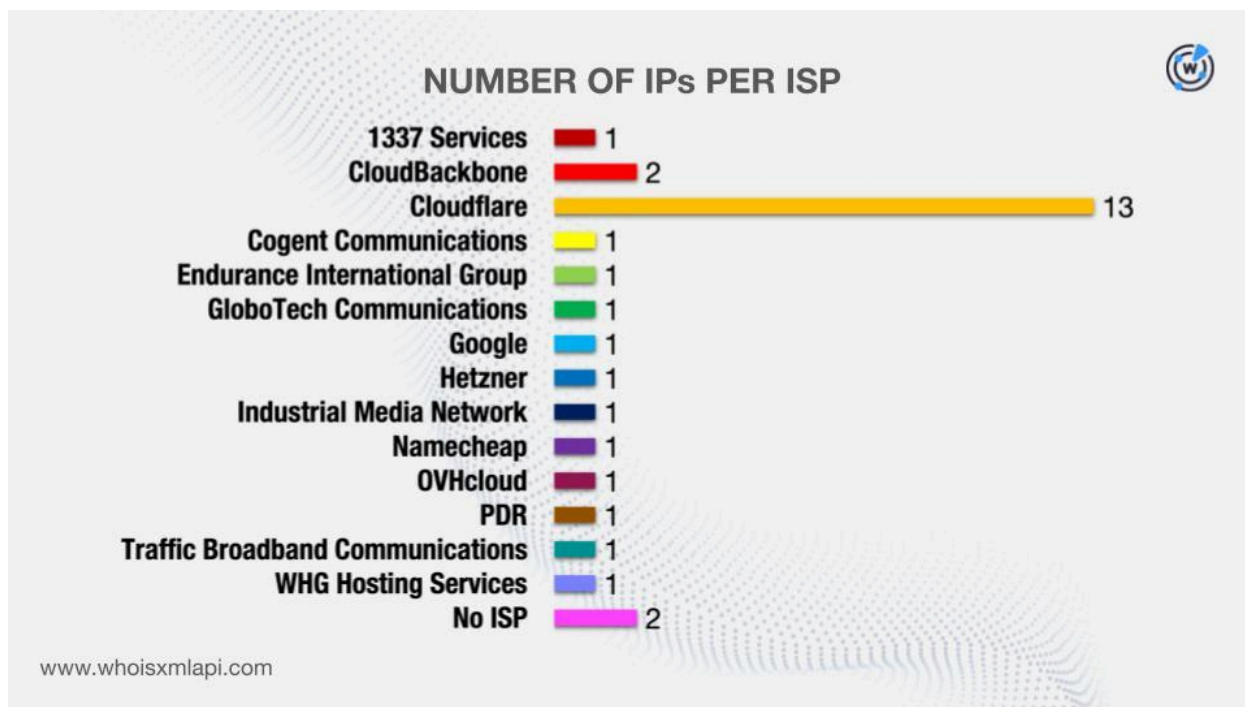
A total of 23 of the 29 malicious IP addresses were associated with more than one threat (between 2 and 5) each so far.

We then queried the 29 IP addresses on [Bulk IP Geolocation Lookup](#) and discovered that:

- While one did not have a geolocation country on record, the remaining 28 originated from eight different countries.



- While two did not have ISPs on record, the remaining 27 were administered by 14 different ISPs.



After that, [Reverse IP API](#) queries for the 29 IP addresses revealed that 10 could be dedicated hosts. Together, they served as hosts to 283 unique IP-connected domains after those already categorized as loCs and the email-connected domains were filtered out.

To date, Threat Intelligence API considered one IP-connected domain—health-smooth-eu1[.]com—malicious in association with malware distribution detected between 8 November 2025 and 30 January 2026.

We then extracted 15 unique text strings from the 32 domains classified as loCs, such as:

- apposx.
- gcsxo.
- globalsnn\*-
- ijels.
- karbowanec.
- kingx.
- kino2.
- krestinaful.

Our [Domains & Subdomains Discovery](#) searches allowed us to collate 692 unique string-connected domains that started with the 15 strings after those already identified as loCs and the email- and IP-connected domains were filtered out.

Threat Intelligence API revealed that only one string-connected domain—verano[.]cfd—has been flagged as malicious, specifically in connection with phishing detected between 3 and 7 December 2025.

## Summing Up Our Findings

Our deep dive into the DNS infrastructure of seven of the top 10 malware of Q4 2025 showed that 145 unique client IP addresses communicated with eight of the domains identified as IoCs. We also learned that seven of the domains tagged as IoCs were likely registered with malicious intent from the get-go.

Our search for new artifacts, meanwhile, uncovered 1,363 web properties comprising 359 email-connected domains, 29 IP addresses, 283 IP-connected domains, and 692 string-connected domains. To date, 46 of these 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

- 1sou[.]top
- 24a[.]su
- 6hms[.]top
- aamirrasheed[.]com
- aamirrasheedco[.]com
- abpvtlimited[.]com
- baihuah[.]top
- bclassytech[.]com
- bedoueroom[.]top
- cafemuzik[.]com
- cameronkerl[.]com
- camohitmangal[.]com
- dailydouble[.]info
- dealermobil[.]top
- devsols[.]net
- egh[.]rocks
- elektronik2000[.]com
- elektronik2000[.]com
- faizeqadria[.]com
- fashionsupermart[.]net
- fearcegroup[.]com
- gamesinworld[.]com
- geneaology[.]info
- geneaology[.]online
- haidao10[.]top
- healthcareplans[.]top
- helperection[.]top
- iamstephenlambert[.]com
- ida-ci[.]com
- idhenterprises[.]com
- jerseyus[.]top
- jeweller[.]rocks
- jiezhishijie[.]top
- kaestner[.]top
- kamagrafr[.]icu
- kanshuwang[.]top
- langwonet[.]top
- latestmoviehouse[.]com
- latestnewsebooks[.]com
- machine-a-plastifier[.]com
- madhavcaterers[.]com
- maicroinn-pk[.]com
- nackt-bilder[.]top
- nayiudaanfoundation[.]com
- netmakers[.]com[.]br
- oliveiracontabil[.]com[.]br
- onesourcepk[.]com
- onlinecinemaworld[.]com
- pakenms[.]com
- pakistanlegalservices[.]com
- palcomp3[.]top
- qazilawchamber[.]com
- rafiqfabrics[.]com
- rag382[.]top
- regopramide[.]top
- salamancaslepiasoom[.]com
- sales2016[.]top
- saludparami[.]com
- takeyouonvacation[.]com
- tdsc[.]top
- techradar[.]top
- universaltechnology[.]top
- unnaticreditcorp[.]com
- usaholidaysystem[.]com
- veranoresorthotel[.]com
- videostation3[.]com
- videozbox[.]com
- wandan[.]top
- wap9[.]top
- wasalgtrading[.]com
- xelexsex[.]top
- xerite-group[.]com
- xn--floridaimveis-jlb[.]com
- yourcialsupply[.]top

- yoursetlist[.]com
- youtubevideo[.]top
- zafirka[.]com

- zakachka[.]top
- zavodppd[.]su

## Sample IP Addresses

- 162[.]159[.]140[.]166
- 104[.]21[.]76[.]132
- 172[.]67[.]195[.]186
- 2[.]58[.]56[.]217
- 34[.]41[.]139[.]193
- 104[.]21[.]46[.]111
- 172[.]67[.]168[.]116
- 104[.]21[.]15[.]1229
- 104[.]21[.]47[.]248
- 172[.]67[.]174[.]215

## Sample IP-Connected Domains

- 0a51cc65-2f44-407d-9ba8-8fd4c b9cbb58[.]random[.]aquawaterjet cutting[.]com
- 106ec745-2981-48bd-a8b7-c682 89f8235c[.]random[.]vicdigit-tech nologies[.]com
- 236080d7-1f18-4682-b67f-940c2 251b86e[.]random[.]vicdigit-techn ologies[.]com
- abigailsolis[.]com
- academiaclavedesol[.]com[.]ar
- airporttaxientebbe[.]com
- bluelighttraining[.]co[.]uk
- c6bfb4ee-95f3-47ef-86f9-f880b b168e90[.]random[.]vicdigit-techn ologies[.]com
- cancun[.]blog
- cancun[.]casino
- database[.]vicdigit-technologies[.] com
- debtcadets[.]com
- decoyjardin[.]com
- ecsaust[.]com[.]au
- egdocs[.]com
- elsspublishing[.]com
- fachetti[.]com[.]ar
- ffda75bd-158d-4fea-b612-e9e1ac 6ee32c[.]random[.]vicdigit-techno logies[.]com
- fotophreak[.]com
- gkindus[.]com
- globalsnn1-new[.]cc
- glowgallery[.]co[.]ke
- habrohosting[.]com
- health-smooth-eu1[.]com
- hekalu[.]solutions
- ijaems[.]com
- ijeab[.]com
- ijtle[.]com
- jacdapps[.]com
- jecac[.]edu[.]np
- justfitequipment[.]co[.]uk
- kliklink[.]net
- ktexautomations[.]com
- lectrovision[.]com
- libertygas[.]com
- luxxorcapital[.]com
- mail[.]cashbeltfinance[.]com
- mail[.]craicden[.]co[.]uk
- mail[.]debtcadets[.]com
- nedellmedical[.]co[.]ke
- netsitesdesign[.]com
- noblersolutions[.]com
- ochirbuyant[.]mn

- oils4health[.]com[.]au
- opflorencia[.]org
- pagekosong[.]com
- parqueslasnubes[.]com
- pasumaipazhagu[.]com
- quientvcancun[.]com
- rectmotors[.]com
- rockbern-coffee[.]com
- rspropaganda[.]com[.]ar
- safariant[.]com
- sharex[.]tech
- shridhanalakshmi[.]com
- technosafeqatar[.]net
- telemetry-updatehub[.]cc
- tenisglobal[.]com[.]ar
- uitsqatar[.]com
- uvibuhea0knij4l[.]aquawaterjetcutting[.]com
- veeyeskay[.]com
- vicdigit-technologies[.]com
- vihitalueconsulting[.]com
- waterjet[.]net[.]in
- waterjetcutting[.]net[.]in
- webdisk[.]cancun[.]house
- xpertnet[.]in
- xsportsmngt[.]com
- zexai[.]space

## Sample String-Connected Domains

- apposx[.]top
- apposx[.]ws
- gcsho[.]com[.]pk
- gcsho[.]info
- gcsho[.]link
- ijels[.]click
- ijels[.]net
- ijels[.]one
- karbowanec[.]cf
- karbowanec[.]club
- karbowanec[.]com[.]ua
- kingx[.]ai
- kingx[.]asia
- kingx[.]bet
- kino2[.]art
- kino2[.]ca
- kino2[.]ch
- krestinaful[.]ph
- krestinaful[.]ws
- memory-scanner[.]com
- memory-scanner[.]uk
- miner[.]ac
- miner[.]ac[.]cn
- miner[.]actor
- nestledinniagara[.]ca
- sberex[.]cash
- sberex[.]net
- sberex[.]pro
- selcukpeker[.]com[.]tr
- selcukpeker[.]net
- selcukpeker[.]tr
- verano[.]ai
- verano[.]al
- verano[.]apartments
- zulpine[.]xyz