WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Shining the DNS Spotlight on Lumma Stealer

Table of Contents

Executive Report

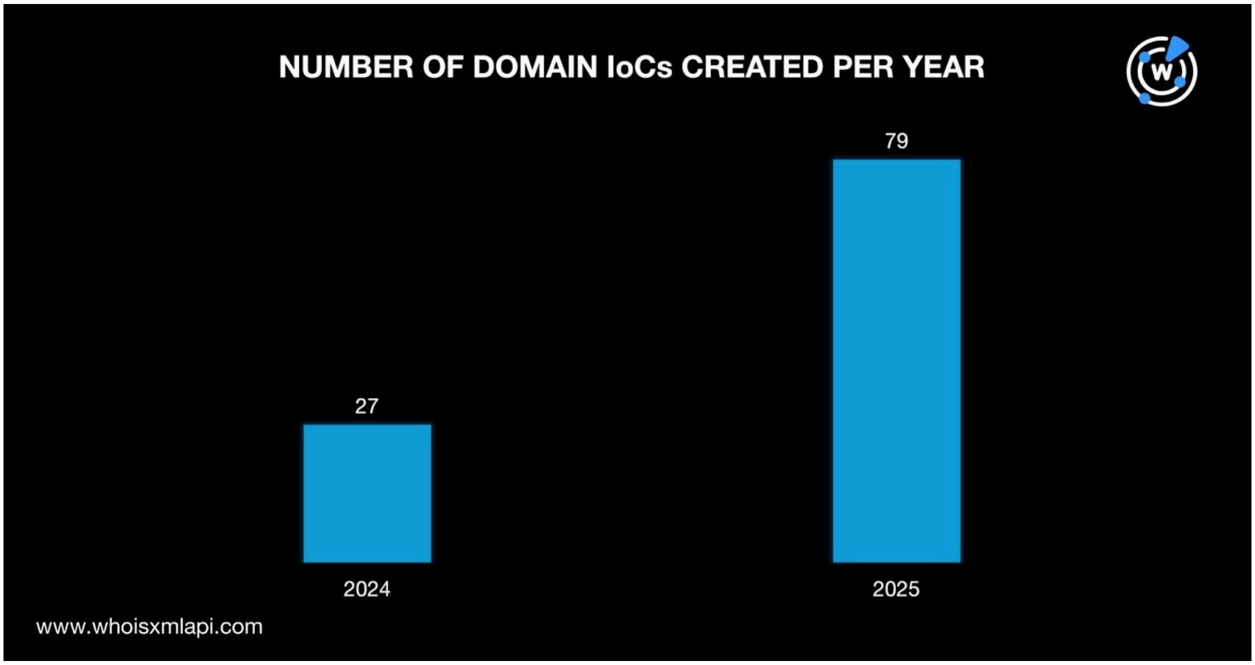
The U.S. Department of Justice seized 114 domains connected to a major information-stealing campaign utilizing Lumma Stealer on 21 May 2025. The Cybersecurity and Infrastructure Security Agency (CISA) released the list of indicators of compromise (IoCs) on the same date.

In a bid to uncover more connected artifacts and other information, WhoisXML API analyzed the IoCs in great depth. Here is a summary of our findings.

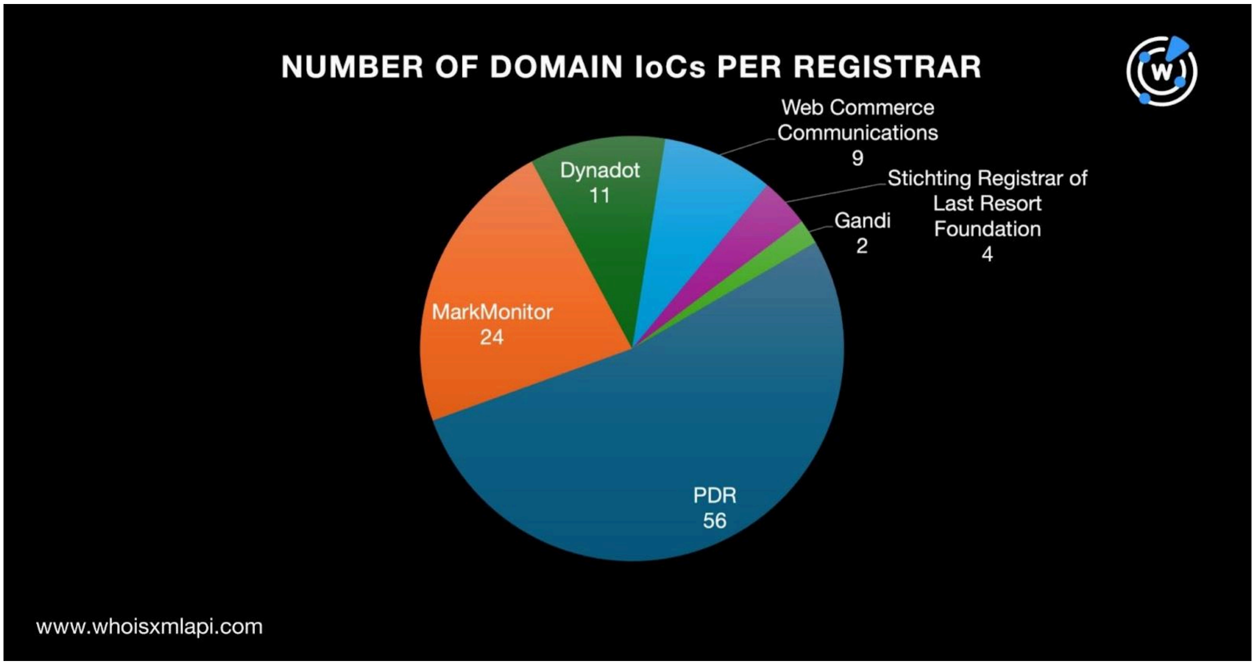
- 28 domain IoCs found on First Watch on an average of 97 days prior to the disclosure date—19 May 2025
- 1–16 VirusTotal engines that classified the eight additional .digital look-alike domains found on First Watch as malicious
- 265 unique domain-to-IP resolutions
- 68 unique IP addresses resolving the domain IoCs before 19 May 2025, 62 were malicious
- Five unique IP addresses actively resolving the domain IoCs, four were malicious
- 187 IP-connected domains
- 346 string-connected domains, one was malicious

Domain Intel Revelations

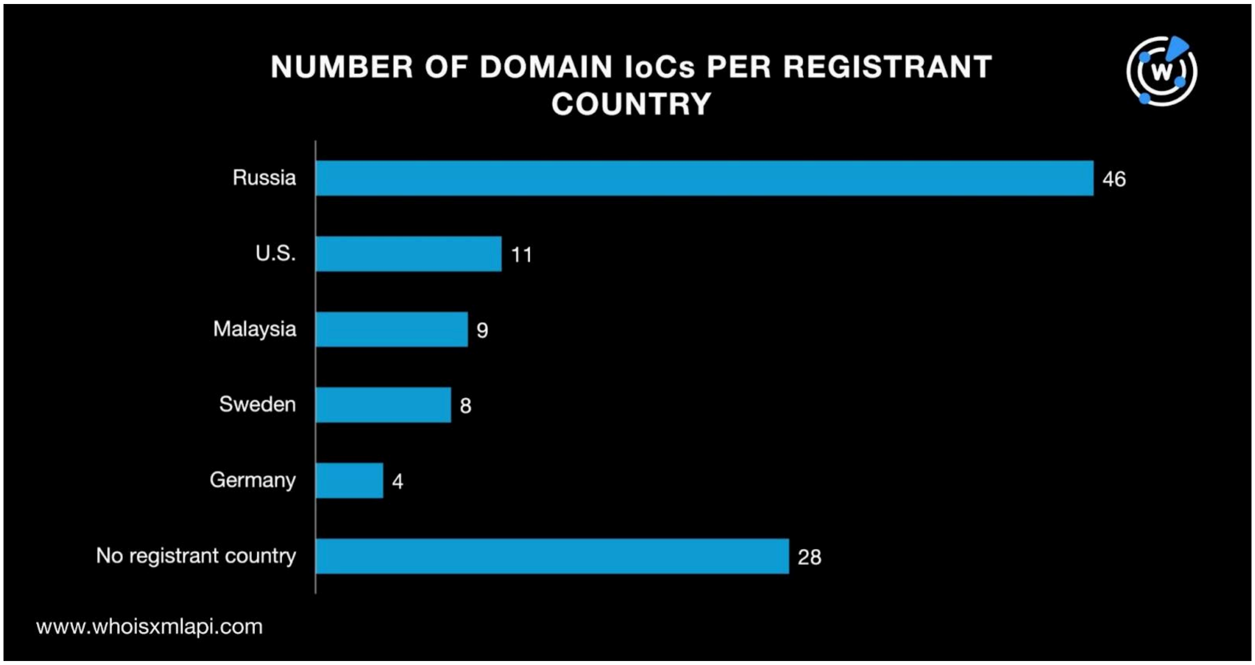
We kicked off our investigation by looking more closely into the WHOIS records of the 114 domains identified as IoCs. A Bulk WHOIS API query for the 114 domains showed that only 106 had current WHOIS records. They were created between 2024 and 2025, making them relatively new when they were weaponized for attacks.



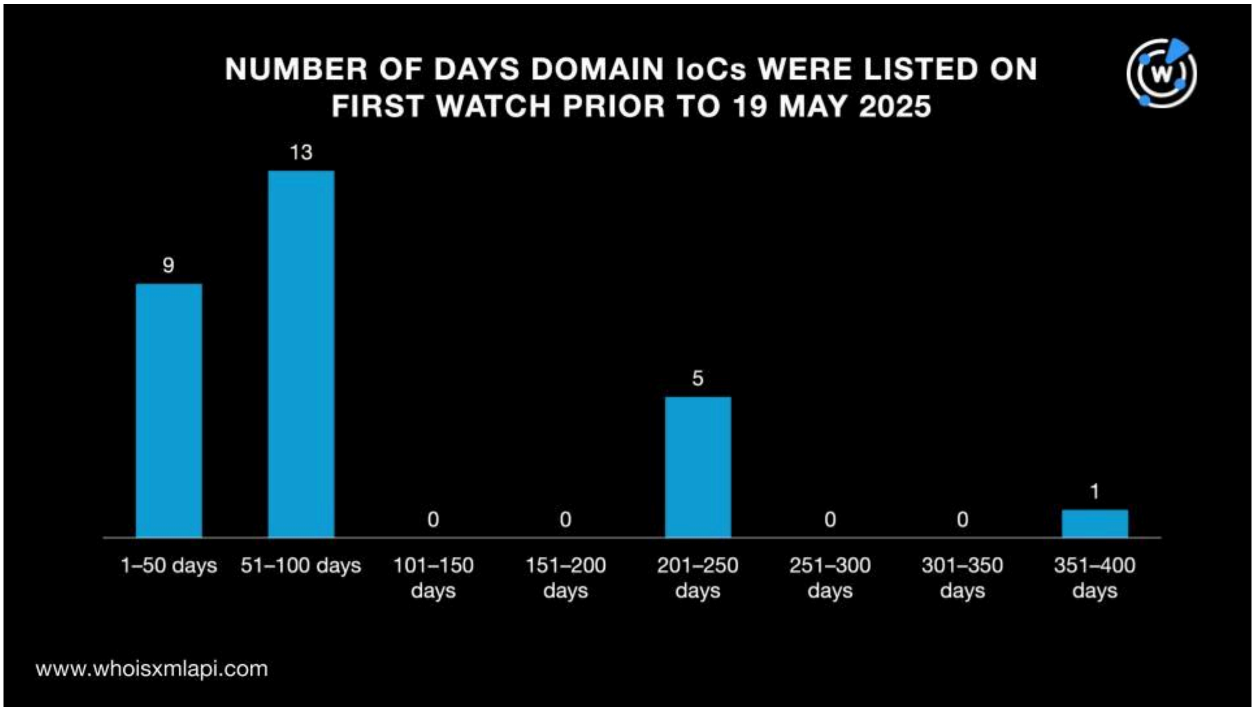
The 106 domains with current WHOIS records were split among six registrars led by PDR, which accounted for 56 domains. The five remaining registrars were MarkMonitor, Dynadot, Web Commerce Communications, Stichting Registrar of Last Resort Foundation, and Gandi.



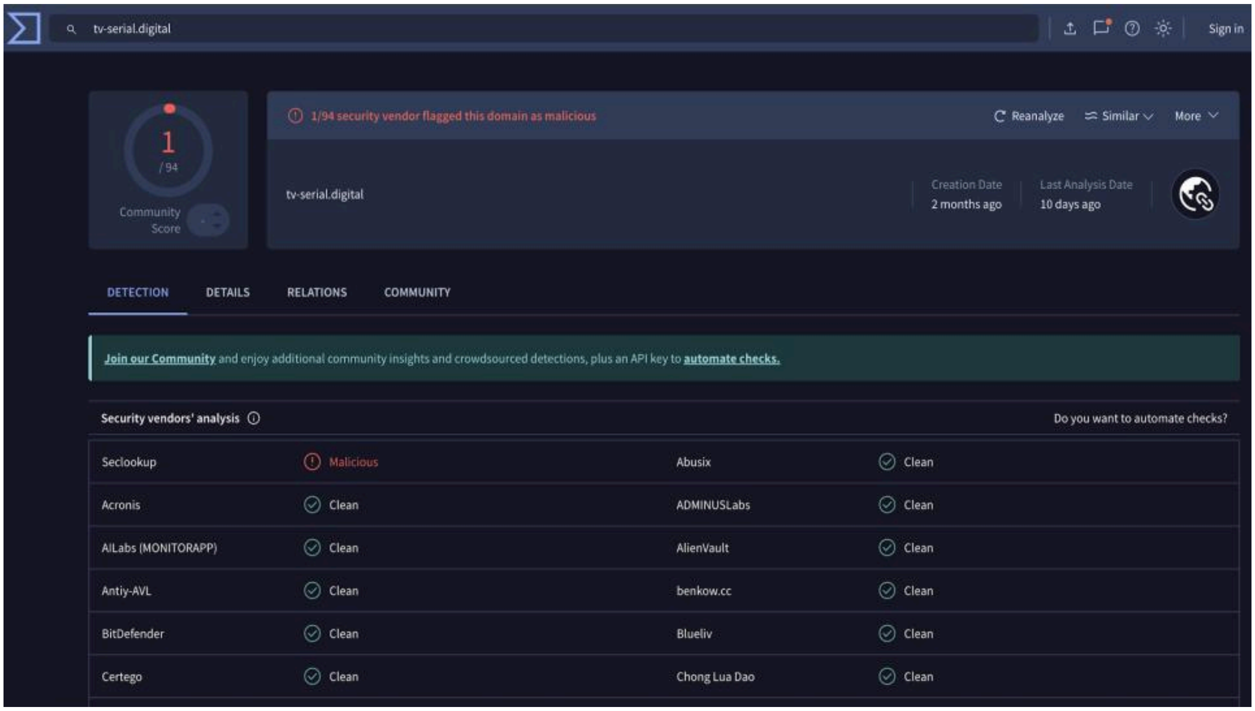
While 28 of the 106 domains with current WHOIS records did not have registrant countries on record, the remaining 78 were registered in five countries topped by Russia, which accounted for 46 domains. The remaining registrant countries were the U.S., Malaysia, Sweden, and Germany.



Next, we searched for the 114 domains identified as IoCs on First Watch Malicious Domains Data Feed files and found 28 matches with corresponding discovery dates. A comparison with the date when the IoC list was released—19 May 2025—revealed that all 28 domains were listed on First Watch first. Specifically, they were listed on First Watch between 39 and 360 days prior to 19 May 2025, translating to an average of 97 days.



Next, we zoomed in on the IoC ferromny[.]digital. Its current WHOIS record showed that it was created on 24 March 2025, used the .digital TLD extension, and was administered by PDR. We downloaded the First Watch file for 24 March 2025 and uncovered eight additional domains likely to turn malicious but were not on the IoC list that shared all the aforementioned WHOIS details. The similarities potentially suggest they could be part of the same attack infrastructure but have not been identified during the Lumma Stealer analysis or fully weaponized. An example would be tv-serial[.]digital, which only one out of 94 VirusTotal engines currently detects as malicious.



1/94 security vendor flagged this domain as malicious

tv-serial.digital

Creation Date
2 months ago

Last Analysis Date
10 days ago

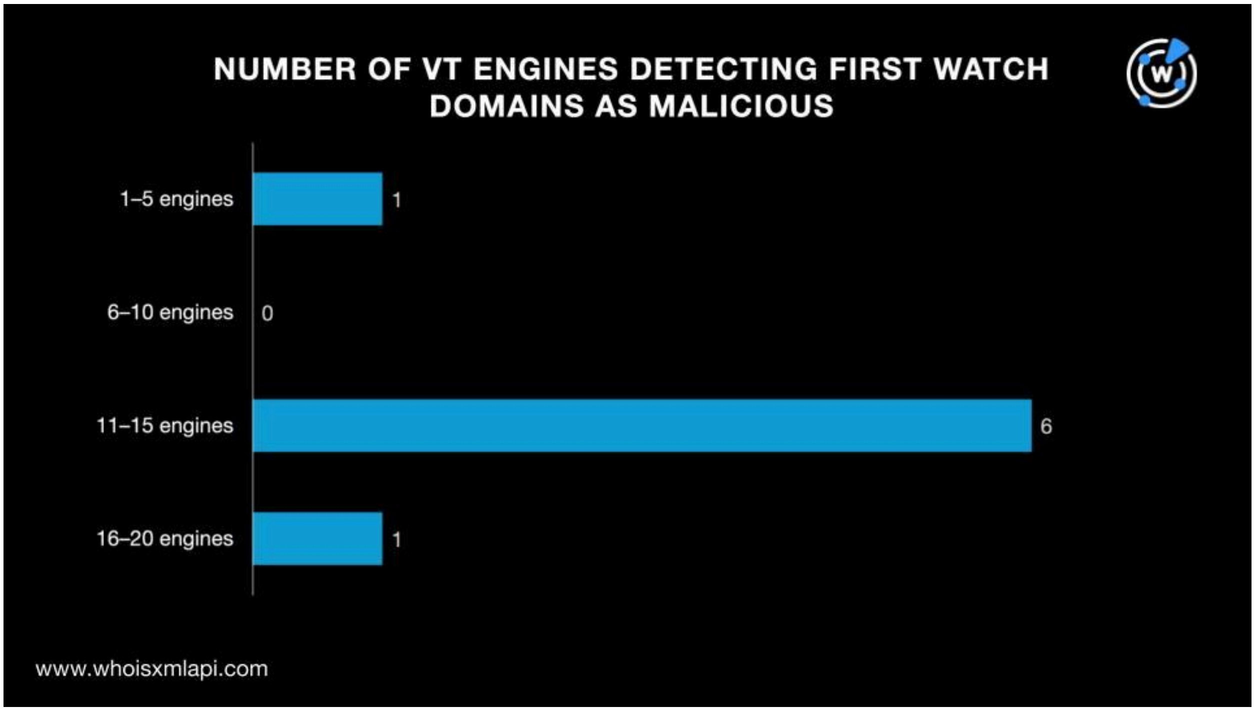
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Seclookup	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean

It is also worth noting that all of the eight domains First Watch found that were not part of the IoC list were already being detected as malicious by an average of 12 engines on VirusTotal.

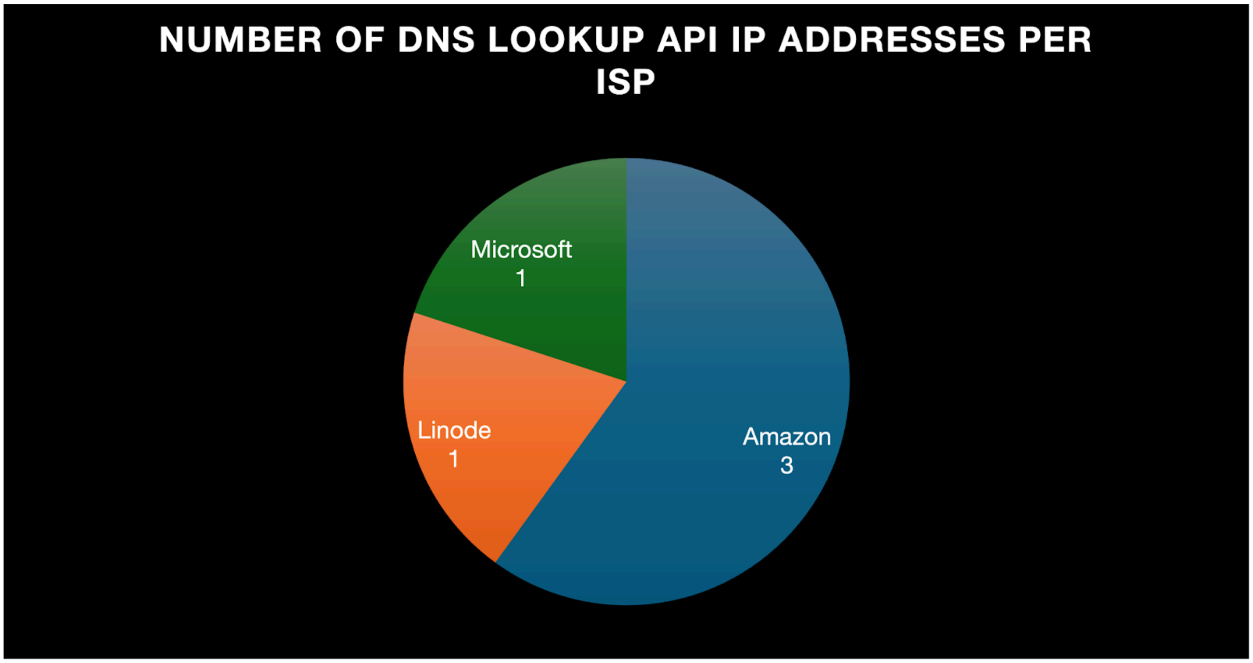


DNS Data-Related Findings

After gathering as much domain-connected intelligence as we could, we then went onto uncovering the DNS traces the 114 domains identified as IoCs left behind.

First off, we queried the 114 domain IoCs on DNS Lookup API and found that 33 of them had active domain-to-IP resolutions. We obtained five unique IP addresses, four of which have already been tagged as malicious based on Threat Intelligence API query results. An example would be 52[.]26[.]80[.]133, which was associated with malware distribution, generic threats, command and control (C&C), and attacks.

A Bulk IP Geolocation Lookup query for the five IP addresses showed that they were all geolocated in the U.S. and split among three ISPs—Amazon, Linode, and Microsoft.



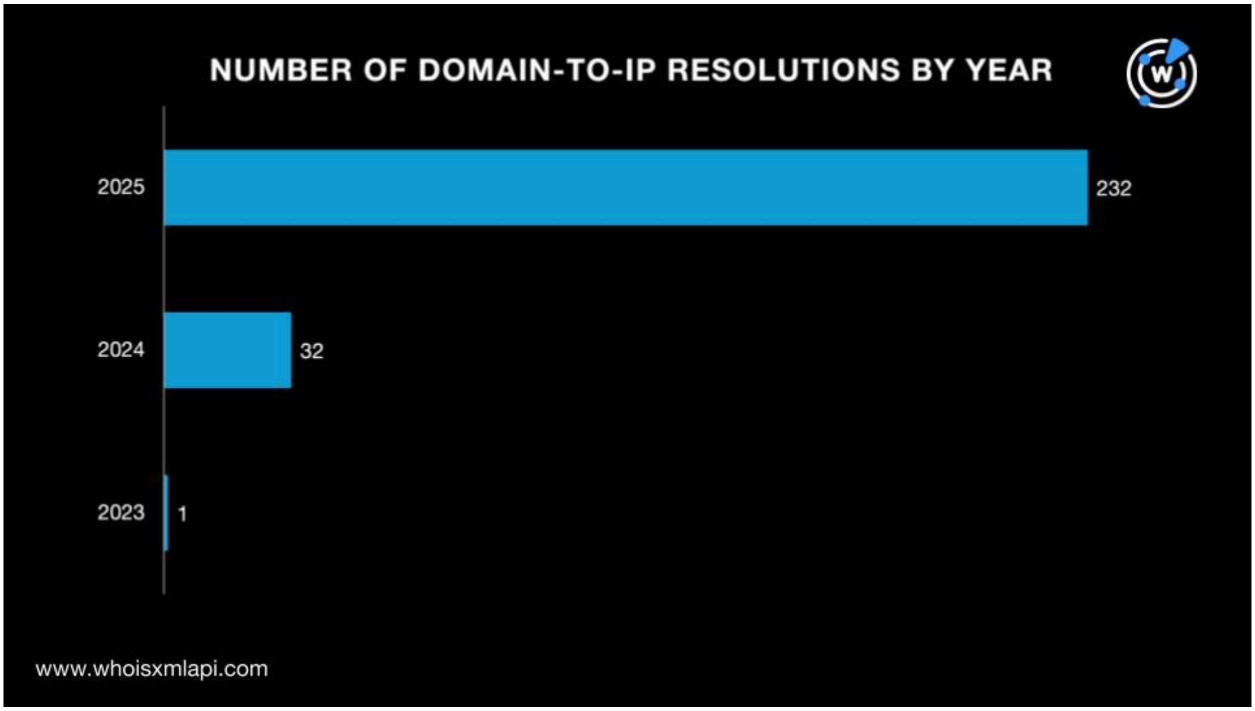
Since none of the five IP addresses from DNS Lookup API were dedicated hosts, we could not use them to find IP-connected domains. We thus had to turn to DNS Chronicle API instead.

Our DNS Chronicle API query for the 114 domains identified as IoCs showed that 55 recorded 265 domain-to-IP resolutions starting on 22 February 2023. Take a look at five examples below.

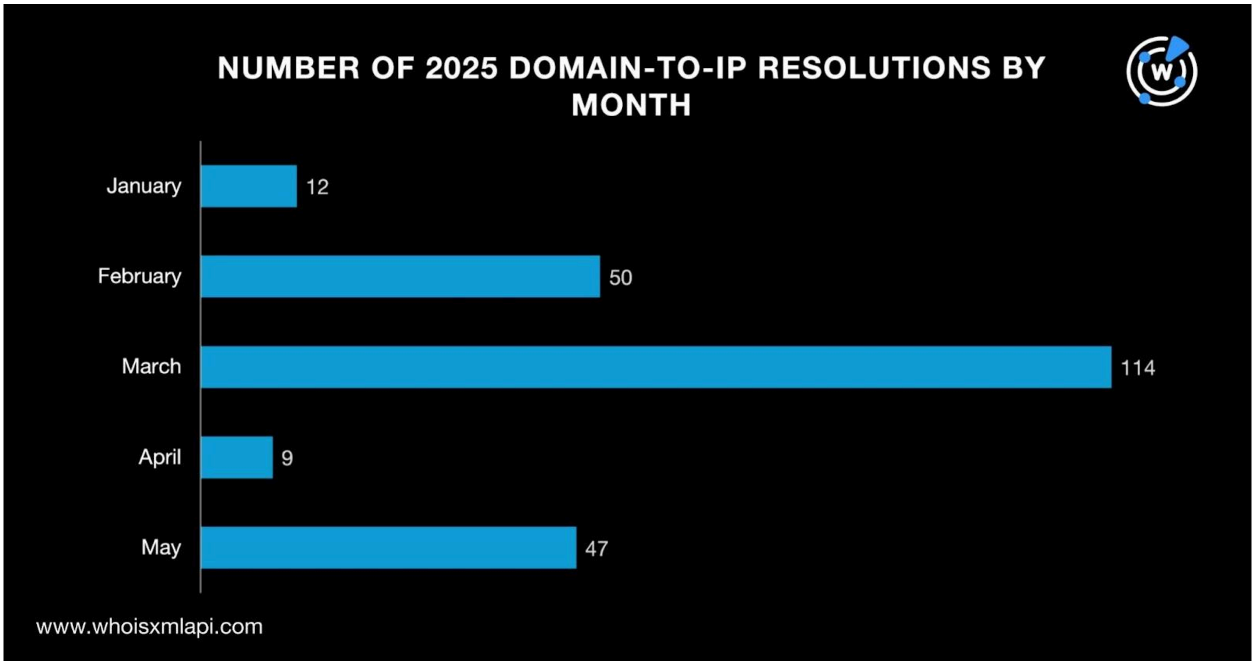
DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE

blast-hubs[.]com	10	11 June 2024
castmaxw[.]run	10	29 March 2025
decreaserid[.]world	7	19 February 2025
earthsymphzony[.]today	2	18 May 2025
featureccus[.]shop	2	11 March 2025

A closer look at the 265 domain-to-IP resolutions revealed that a majority (88%) were recorded in 2025. The rest were recorded in 2023 and 2024.



Zooming in further on the domain-to-IP resolutions recorded in 2025, we discovered that the largest number (49%) were recorded in March.



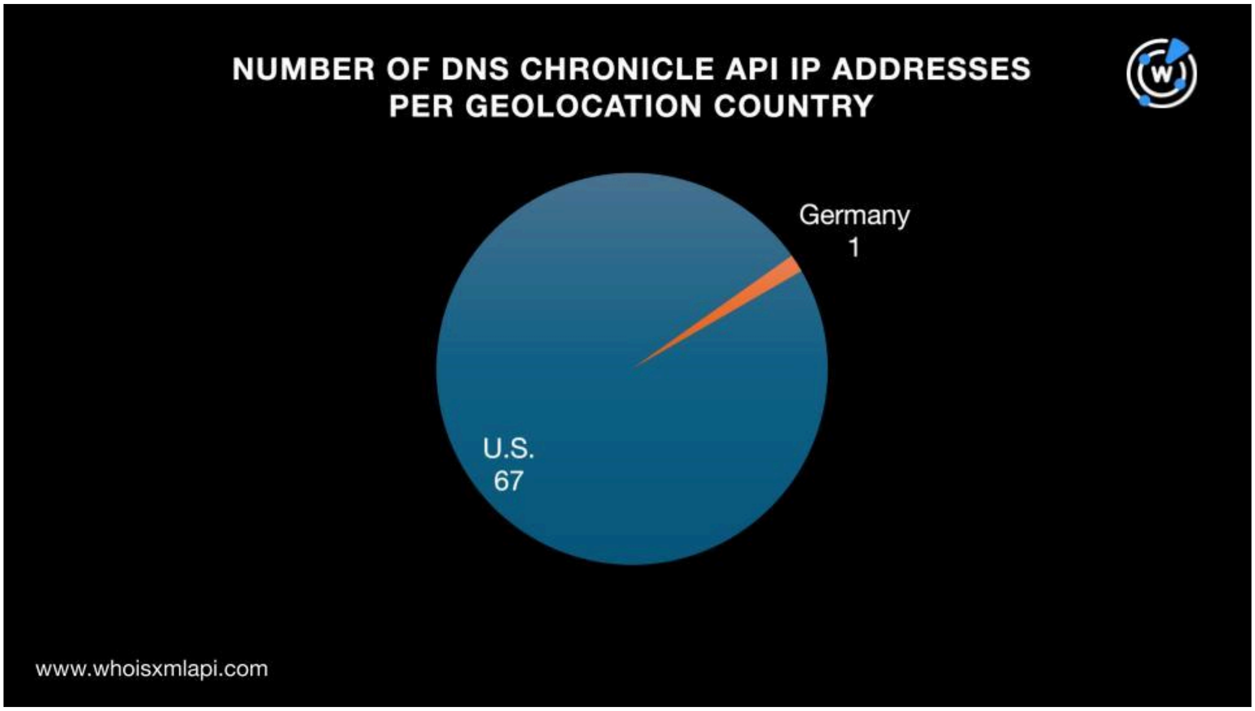
To obtain a list of IP-connected domains, we focused on the 49 domain IoCs with domain-to-IP resolutions made before 19 May 2025. That gave us 68 unique IP addresses, which we queried on Threat Intelligence API. We found that 62 IP addresses have already been weaponized for various attacks. See five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]112[.]1	Phishing Malware distribution C&C Suspicious activity Generic threat Attack
15[.]197[.]240[.]20	Malware distribution Generic threat Suspicious activity Phishing C&C Attack
173[.]255[.]204[.]62	Malware distribution C&C
40[.]91[.]108[.]115	Malware distribution Phishing

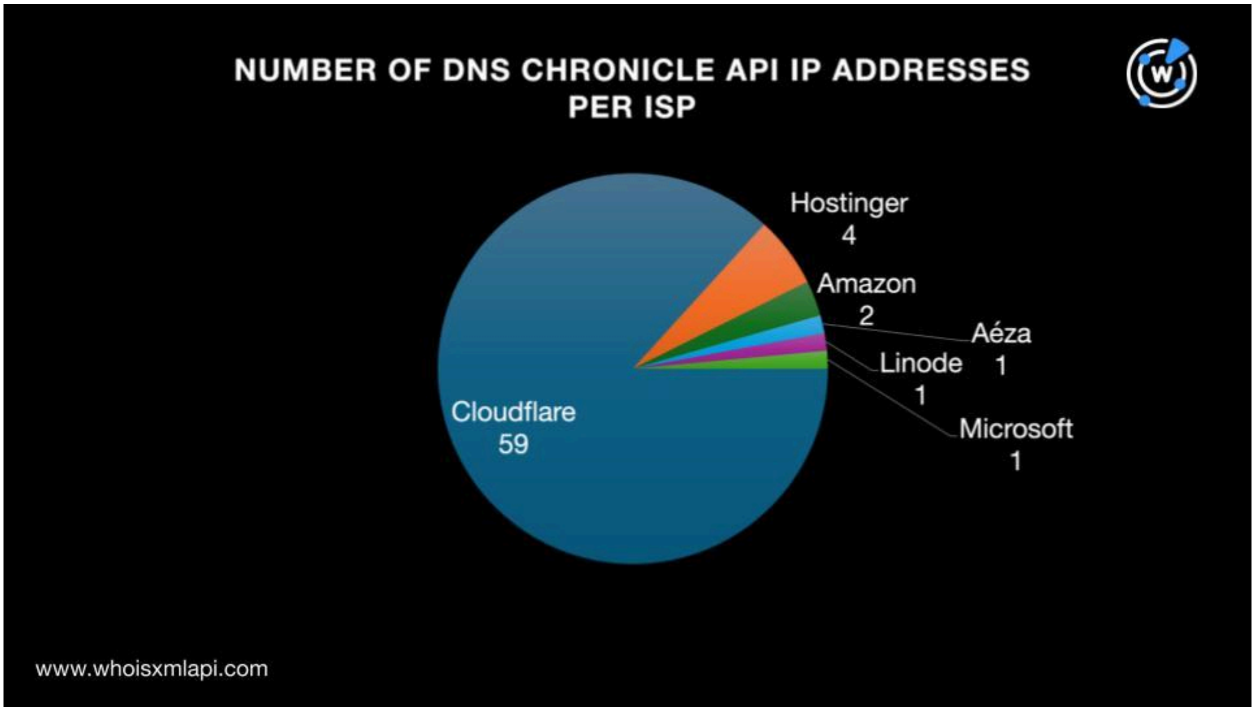
75[.]2[.]115[.]196	Malware distribution Generic threat Phishing Suspicious activity Attack

Note that three IP addresses—15[.]197[.]240[.]20, 173[.]255[.]204[.]62, and 40[.]91[.]108[.]115—were present in both the DNS Lookup API and DNS Chronicle API results.

A Bulk IP Geolocation Lookup query for the 68 IP addresses showed that a huge chunk were geolocated in the U.S. (99%) while one IP originated from Germany.



The 68 IP addresses were also split among six ISPs led by Cloudflare, which accounted for 87%. The other ISPs were Hostinger, Amazon, Aéza, Linode, and Microsoft.



Next, we queried the 68 IP addresses on Reverse IP API and discovered that two could be dedicated hosts. Together, they played host to 187 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

After that, we looked closer at the 114 domains identified as IoCs and determined they contained 114 unique text strings. Domains & Subdomains Discovery searches for the 114 strings turned up 346 string-connected domains for the 21 strings below after duplicates, those already identified as IoCs, and the IP-connected domains were filtered out:

- advennture.
- blast-hubs.
- citydisco.
- citywand.
- climatologfy.
- dsfljsdfjewf.
- furthert.
- generalmills.
- hoyoverse.
- jrxsafer.
- liftally.
- longitudde.
- mercharena.
- nestlecompany.
- salaccgfa.
- starcloc.
- steelixr.
- stormlegue.
- targett.
- tracnquilforest.
- ywmedici.

A Threat Intelligence API query for the 346 string-connected domains revealed that one—nestlecompany[.]world—has already figured in malware distribution.

—

Our in-depth investigation of this Lumma Stealer campaign yielded interesting findings like 28 of the 114 domains identified as IoCs were recorded on First Watch even earlier than when they were publicized. We also uncovered 601 connected artifacts comprising 68 IP addresses, 187 IP-connected domains, and 346 string-connected domains. In addition, 67 of the web properties we identified have already been tagged as malicious.

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 Domain IoCs Found on First Watch

- clarmodq[.]top
- dsfljsdfjewf[.]info
- earthsymphzony[.]today
- faulteyotk[.]site
- galxnetb[.]today
- hemispherexz[.]top
- jrxsafer[.]top
- longitudde[.]digital
- metalsyo[.]digital
- opposezmny[.]site
- pepperiop[.]digital
- quietswtreams[.]life
- rambutanvcx[.]run
- seizedsentec[.]online
- weldorae[.]digital
- ywmedici[.]top

Sample IP Addresses

- 104[.]16[.]198[.]133
- 104[.]21[.]112[.]1
- 104[.]21[.]16[.]1
- 15[.]197[.]240[.]20
- 156[.]67[.]74[.]145
- 172[.]67[.]144[.]247
- 172[.]67[.]150[.]100
- 172[.]67[.]155[.]64
- 173[.]255[.]204[.]62
- 2a02[:]4780[:]b[:]662[:]0[:]2465[:]85b8[:]9
- 2a02[:]4780[:]b[:]662[:]0[:]2465[:]85b8[:]c
- 2a02[:]4780[:]b[:]662[:]0[:]2465[:]85b8[:]d
- 40[.]91[.]108[.]115
- 75[.]2[.]115[.]196
- 89[.]208[.]106[.]21

Sample IP-Connected Domains

- 0-o[.]website
- 1-800support[.]com
- academia-essentia[.]com
- agentedora[.]com
- chainlogistics[.]mx
- co-coffee[.]shop
- datachronicle[.]org
- datadrunklabs[.]com
- ecocarga-soluciones[.]com
- emmaenyo[.]com
- frankietseventoselegantes[.]com
- ftp[.]0-o[.]website
- ghloanapp[.]xyz
- happylifesociety[.]com
- hospitalitygh[.]com
- idekhea[.]com
- integralmarketinghub[.]com
- jamberagency[.]com
- jiakautomotriz[.]com
- kadiehargis[.]com
- kalfas[.]net
- lacasadelabalsa[.]com
- luzdeluna[.]ec
- mbitec[.]site
- melhorperfumemasculino[.]com
- oftamologiamexicali[.]com
- ohmesgroup[.]com
- pdfconvertorlixi[.]com

- plasma-corte[.]site
- safehomerepairs[.]com
- seminuevosautoplus[.]com
- templadosandadre[.]site
- thelifestylegrimoire[.]com
- visualcaptain[.]com
- www[.]0-o[.]website
- www[.]1-800support[.]com

Sample String-Connected Domains

- advennture[.]co[.]za
- blast-hubs[.]pro
- citydisco[.]co[.]uk
- dsfljsdfjewf[.]ph
- furthert[.]cn
- generalmills[.]ai
- hoyoverse[.]ai
- jrxsafer[.]ws
- liftally[.]com
- mercharena[.]com
- nestlecompany[.]com
- salaccgfa[.]ph
- targett[.]ae
- ywmedici[.]ph