WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Inside a TDS-Powered ClickFix Malware Ecosystem: A DNS Deep Dive

Threat Report

Table of Contents

Executive Report

Check Point Research investigated an ongoing large-scale operation impersonating open-source and freeware projects to capture search traffic. Their well-designed sites often looked like legitimate project portals at a glance. Their deception, however, did not lie in their page content, they were spurred by user interactions.

The attacks loaded a CloudFront-hosted JavaScript staging layer that redirected user clicks to a traffic distribution system (TDS) with strict gating features. Their upstream ecosystem may have been built primarily to acquire and monetize traffic while their downstream redirect chains led selected users to malware delivery infrastructure for RemusStealer, AnimateClipper, and the SessionGate framework.

The researchers identified 27 network IoCs made up of subdomains, domains, and IP addresses. After extracting unique domains from the subdomains and domain legitimacy and activity checks aided by the WhoisXML API MCP Server, we compiled 30 IoCs comprising eight subdomains, 19 domains, and three IP addresses for further investigation.

Our DNS deep dive into the threat led to these discoveries:

- One client IP address that communicated with one of the domain IoCs
- One domain IoC that appeared in one typosquatting group with five members
- Three domain IoCs that were likely registered with malicious intent
- 22 unique IP addresses potentially owned by victims that communicated with two of the IP IoCs
- 2,892 email-connected domains, 11 of which were confirmed malicious
- 26 additional IP addresses, all of which were confirmed malicious
- 23 IP-connected domains, 10 of which were confirmed malicious
- 157 string-connected domains

Studying the RemusStealer, AnimateClipper, and SessionGate Subdomain IoCs

We began our in-depth IoC investigation by looking more closely at the eight subdomain IoCs.

We used the WhoisXML API MCP Server to analyze the subdomain IoCs and uncovered interesting findings. Take a look at more information for three examples shown below.

SUBDOMAIN IoC	WXA MCP SERVER FINDING
cdn-1415[.]brightcanvas[.]digital	An active subdomain pointing to Cloudflare CDN IP addresses whose apex domain was registered in January 2026 via PDR; has a GDPR-masked registrant who is U.K.-based; the only subdomain with live DNS A records
cw[.]hugo-lapp[.]lat	Has a suspended apex domain, no active DNS records, and a registrant email address with a random string, suggesting a fake or disposable identity
ed[.]hugo-lapp[.]lat	Has the same apex domain as cw[.]hugo-lapp[.]lat and no active DNS resolutions due to domain suspension

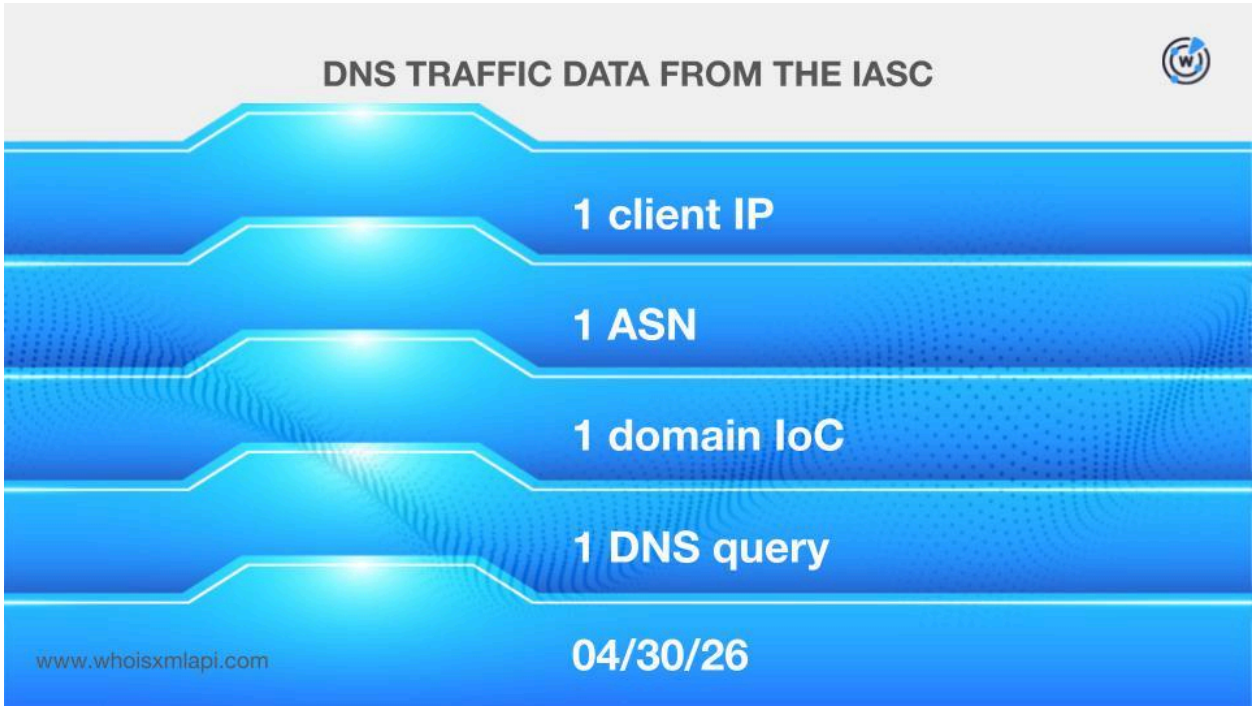
In sum, the hugo-lapp subdomain family is clearly part of a suspended or abusive infrastructure cluster. The apex domains—brightcanvas[.]digital and hugo-lapp[.]lat share the same registrar. The differences? While hugo-lapp[.]lat has been suspended, brightcanvas[.]digital remains live behind a Cloudflare IP address, which could mean it is still operational or has not been subjected to action yet. And while brightcanvas[.]digital had a redacted registrant email address, hugo-lapp[.]lat had a public but suspicious email address.

Our verdict? All subdomains under the two apex domains may be worth avoiding.

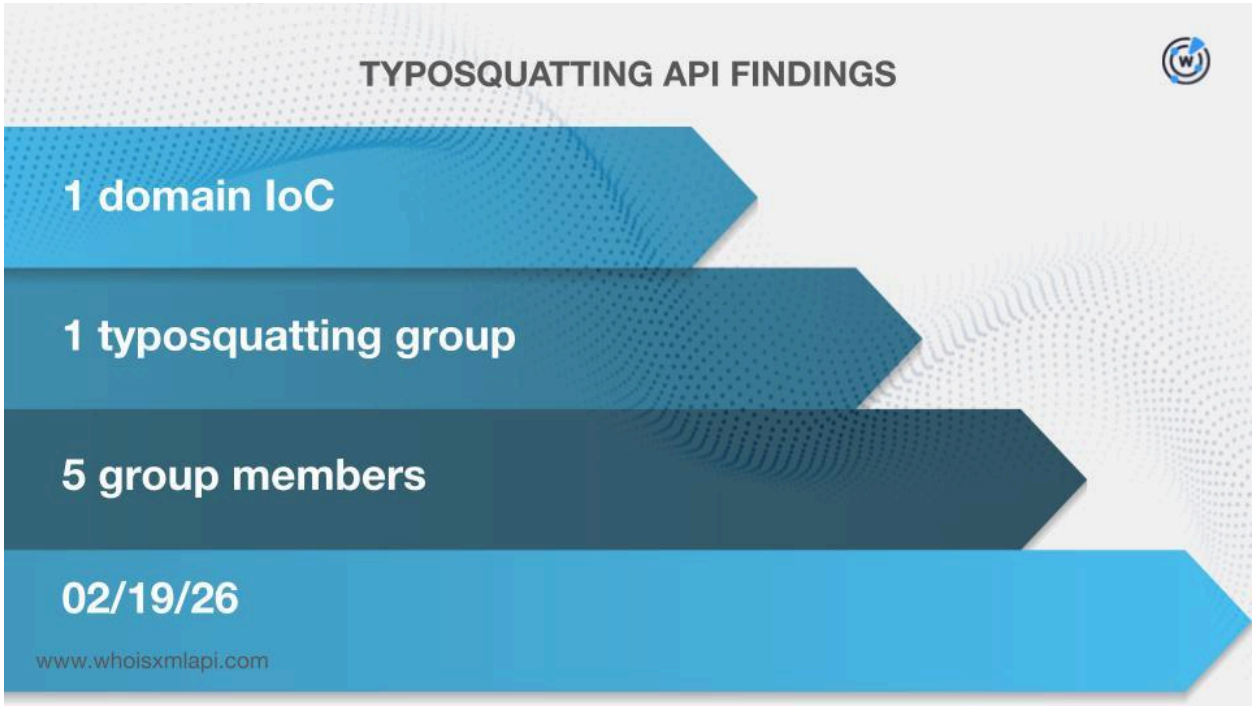
Dissecting the RemusStealer, AnimateClipper, and SessionGate Domain IoCs

Next, we zoomed in on the 19 domain IoCs.

First, sample network traffic data from the IASC revealed that one client IP address communicated with one of the domain IoCs via a single DNS query made on 30 April 2026.



The findings of our Typosquatting API queries for the domain IoCs, meanwhile, showed that the domain IoC ropea[.]top appeared in a typosquatting group along with four look-alikes—rosca[.]cn, rozea[.]co, rosea[.]lat, and rosca[.]health. The five group members were all registered on 19 February 2026.

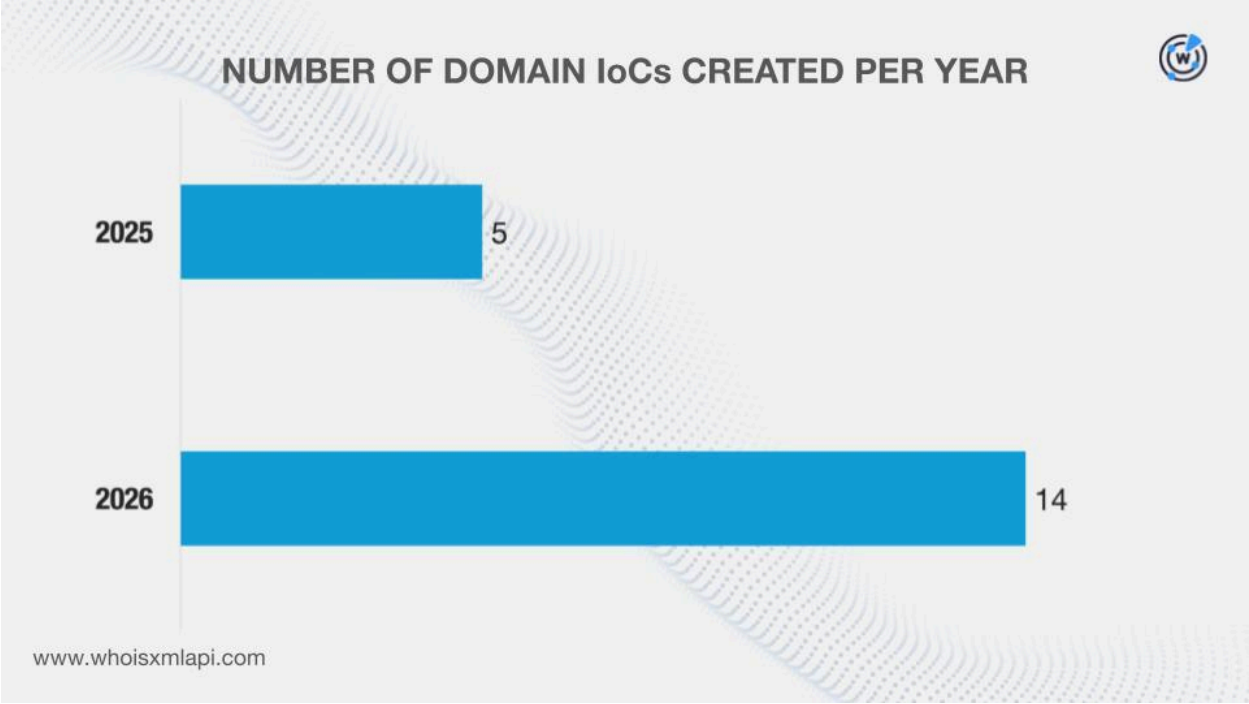


We also learned from the results of our First Watch Malicious Domains Data Feed queries that three of the domain IoCs were likely registered with malicious intent 104–161 days before Check Point Research dubbed them as IoCs in their report published on 3 June 2026.

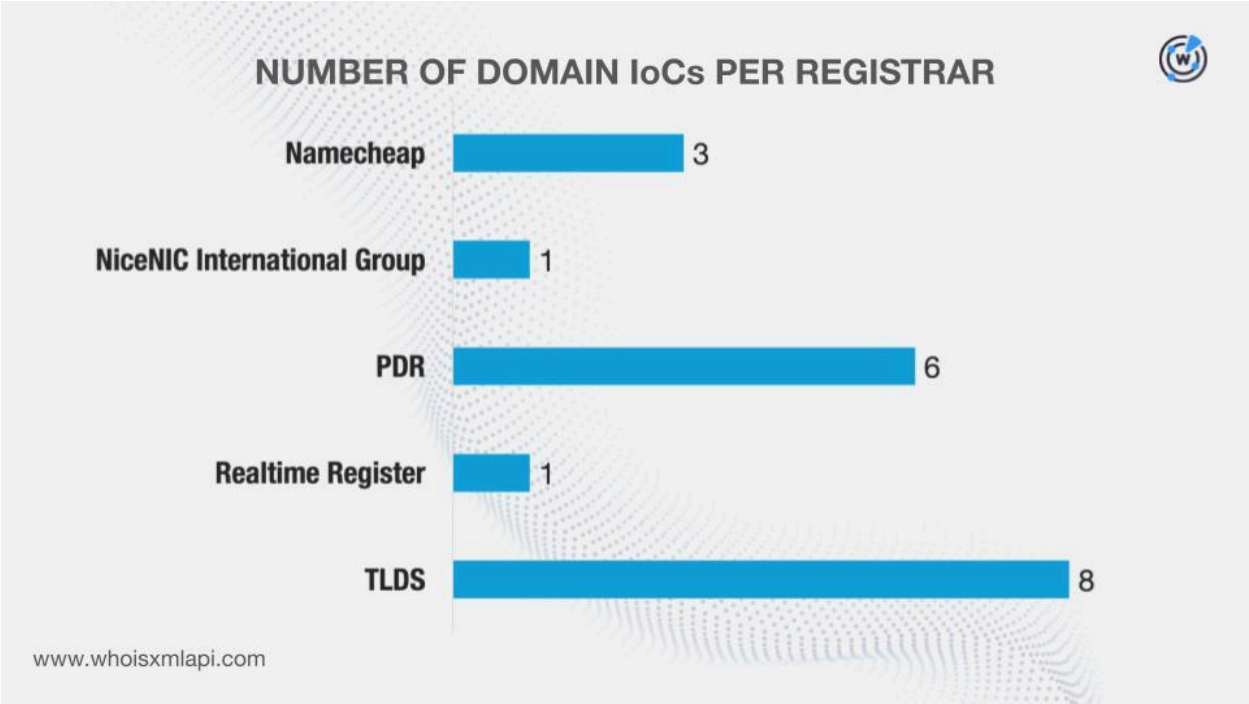
The domain IoC carlessclapped[.]com, for instance, was registered as far back as 24 December 2025, 161 days before the report publishing date.

Next, we queried the domain IoCs on WHOIS API and discovered that:

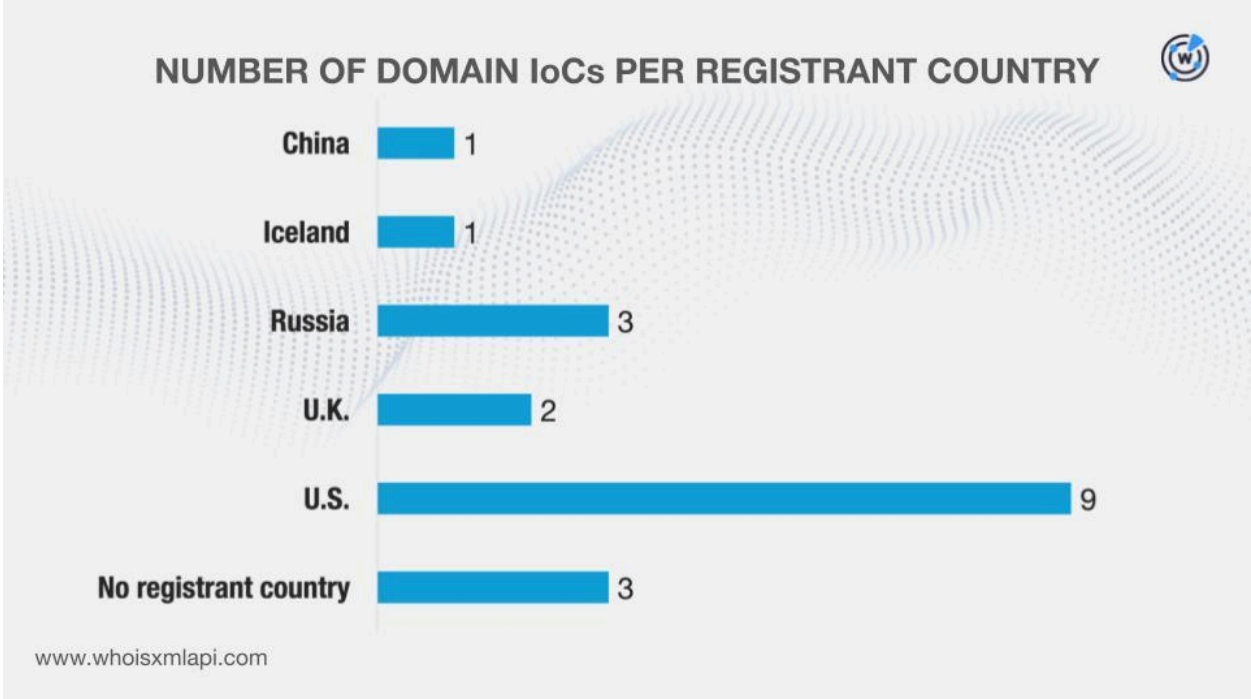
- They were created between 23 September 2025 and 4 March 2026, hinting that the threat actors could prefer using NRDs for their attacks.



- They were administered by five different registrars.



- While three did not have registrant countries on record, the remaining 16 were registered in five different countries.



The results of our DNS Chronicle API queries for the domain IoCs revealed that 16 recorded 181 historical domain-to-IP resolutions over time. Here are more details for five examples.

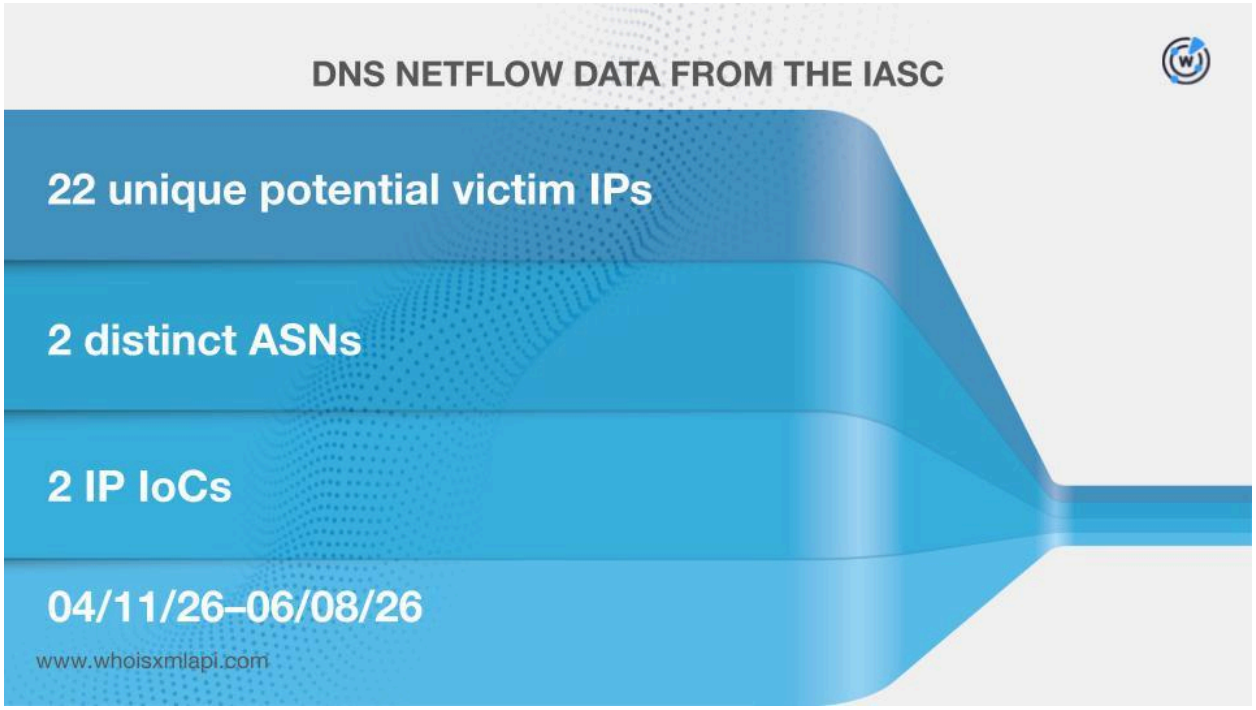
DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
ropea[.]top	24	10/15/21–02/19/26
webcrcprove[.]com	24	01/03/26–05/27/26
webinnosetup[.]com	24	09/23/25–05/13/26
appgetonline[.]com	21	12/07/25–04/30/26
appfreshstart[.]com	15	12/04/25–05/13/26

To date, all 16 domain IoCs with historical resolutions continue to resolve IP addresses.

Investigating the RemusStealer, AnimateClipper, and SessionGate IP IoCs

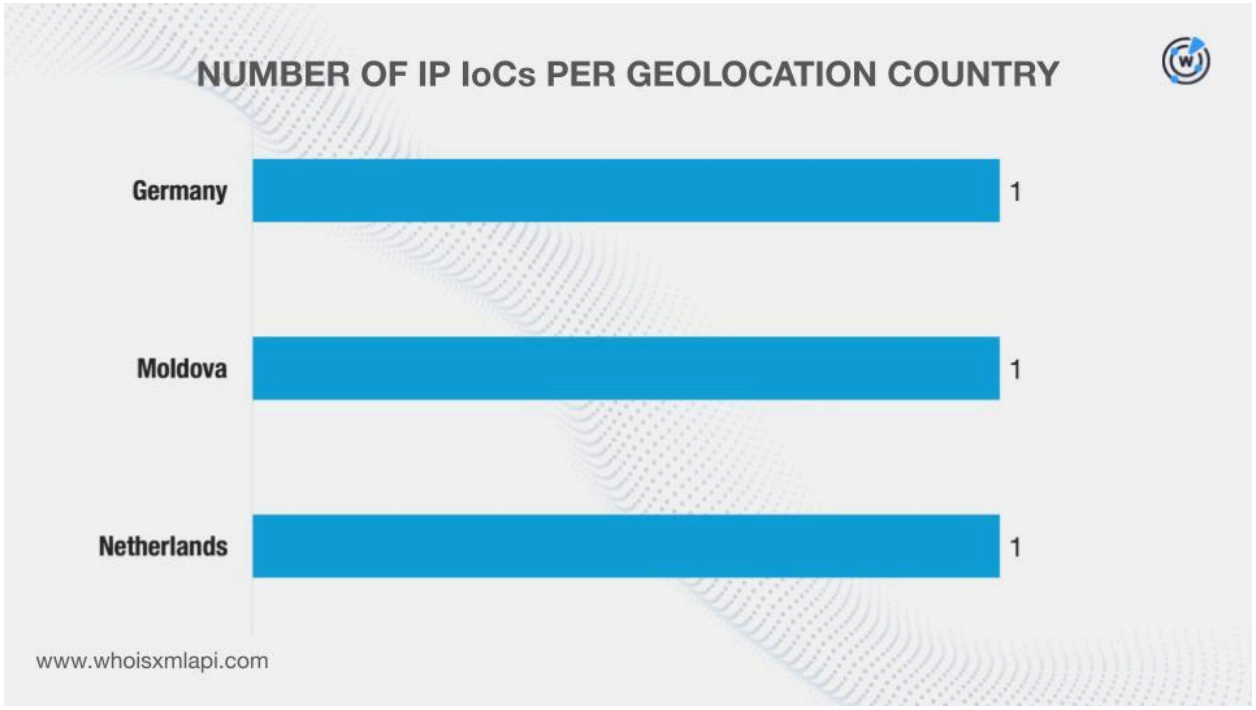
Next, we scrutinized the three IP IoCs.

First, sample network traffic data from the IASC revealed that 22 unique IP addresses that could belong to victims under two distinct ASNs communicated with two of the IP IoCs between 11 April and 8 June 2026.

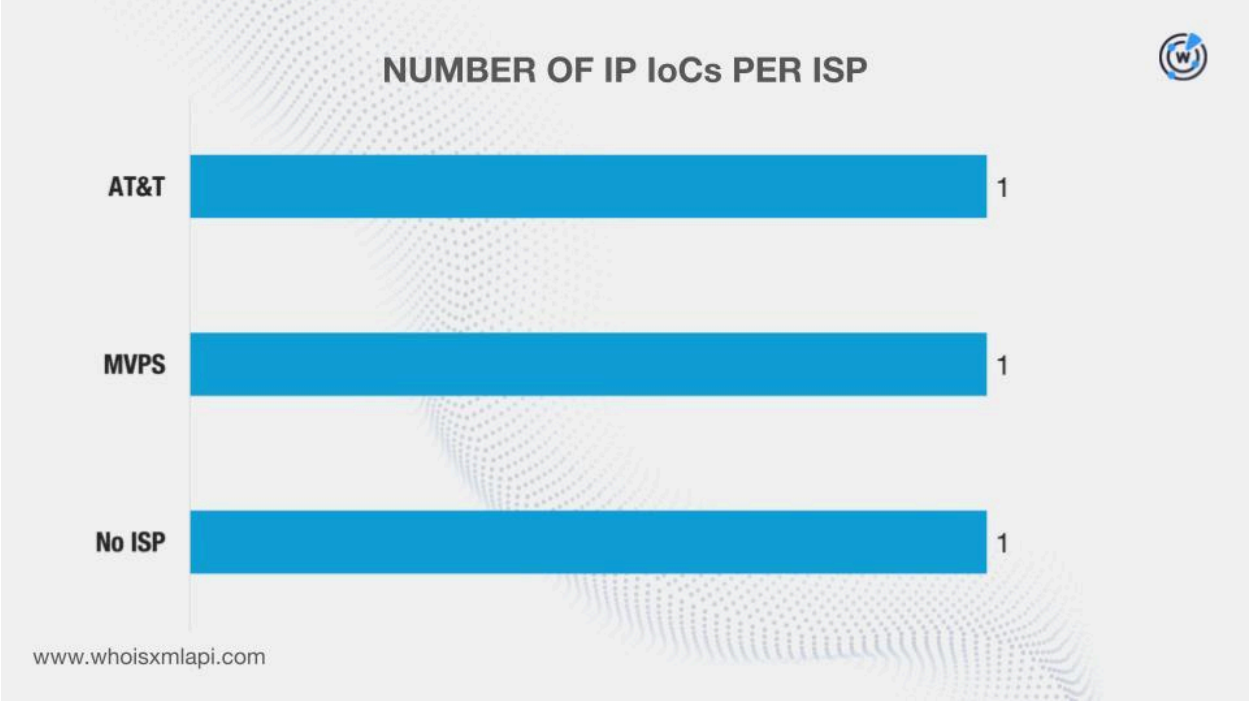


We then queried the IP IoCs on Bulk IP Geolocation Lookup and discovered that:

- Each of them was geolocated in a different country, none of which matched any of the registrant countries of the domain IoCs identified earlier.



- While one did not have an ISP on record, the remaining two fell under the purview of two distinct administrators.



The results of our DNS Chronicle API queries for the IP IoCs showed that all three posted 333 historical IP-to-domain resolutions over time. The IP address 217[.]156[.]122[.]75, for instance, recorded 265 resolutions between 7 February 2017 and 21 April 2025.

As of this writing, only one of the IP IoCs continued to post domain resolutions in 2026.

Ammassing New RemusStealer, AnimateClipper, and SessionGate Artifacts

Next up, we expanded the current list of network IoCs beginning with WHOIS History API queries for the domain IoCs. We learned that 15 had 22 unique email addresses in their historical records. Further scrutiny showed that three were public email addresses.

We queried the public email addresses on Reverse WHOIS API and uncovered 2,892 unique email-connected domains after those tagged as IoCs were filtered out.

Threat Intelligence API queries for the email-connected domains showed that 11 have already been weaponized for various cyber attacks. Take a look more information for five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
bokukagaku[.]net	Malware distribution	05/27/26–06/09/26
chalx[.]live	Malware distribution	03/29/26–06/09/26
mezi[.]bet	Malware distribution	08/26/25–06/09/26
norti[.]top	Malware distribution	03/11/26–06/09/26
tds-packages-update[.]com	Malware distribution	07/08/23–06/09/26

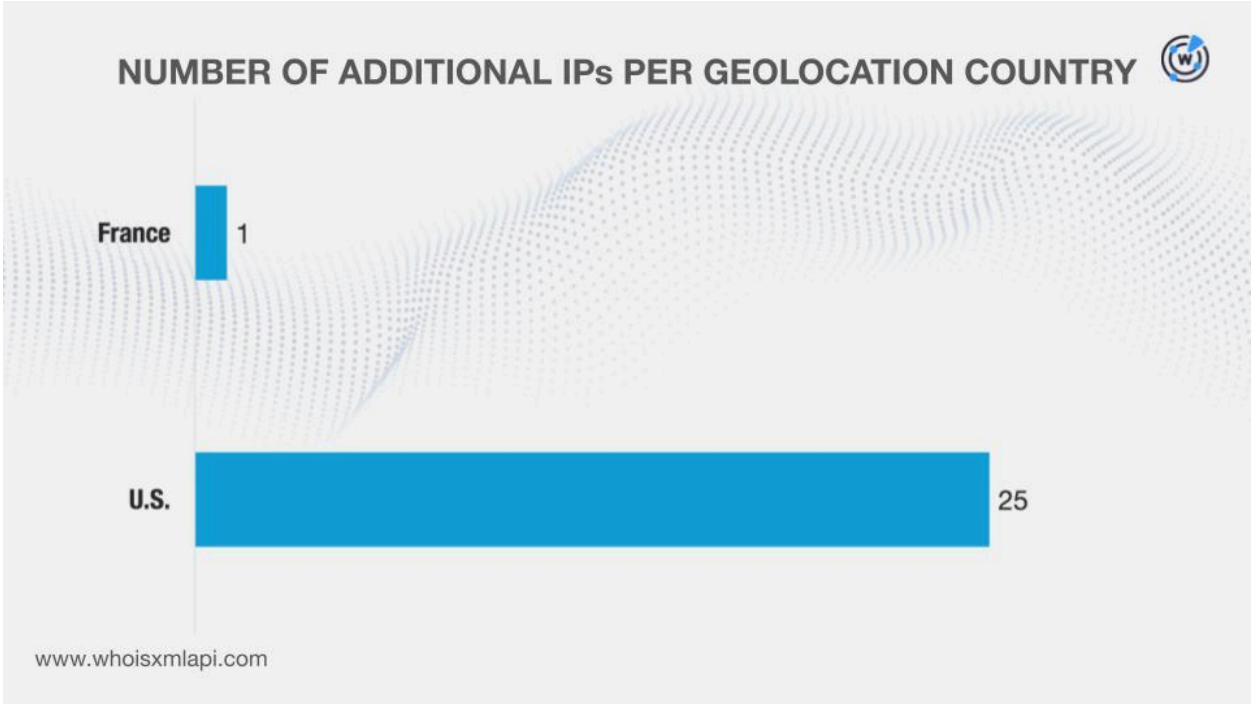
We then queried the domain IoCs on DNS Lookup API and unearthed 26 unique additional IP addresses.

The results of our Threat Intelligence API queries for the additional IP addresses revealed that all of them have already figured in various malicious campaigns. Here are more details for five examples.

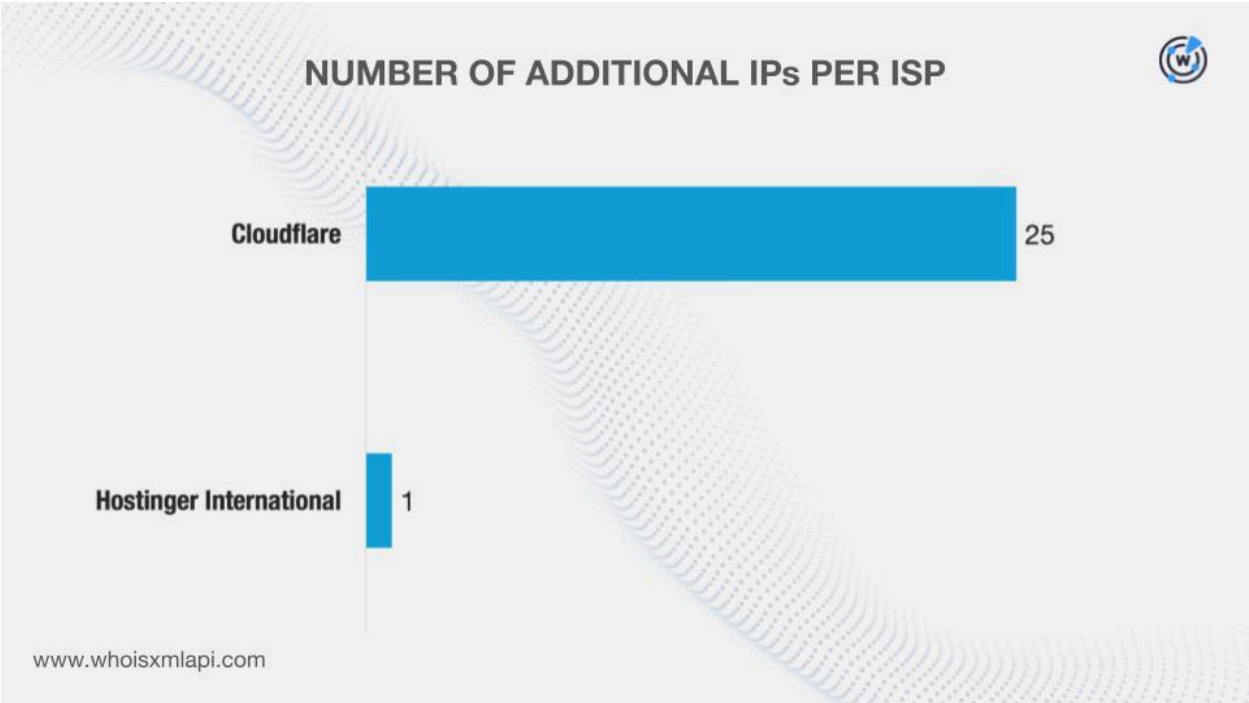
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
104[.]21[.]81[.]50	Phishing Malware distribution Generic threat	05/14/24–06/10/26 03/21/24–06/09/26 08/09/24–04/27/26
104[.]26[.]12[.]30	Malware distribution Phishing	06/04/26–06/09/26 04/09/25–03/29/26
104[.]21[.]24[.]60	Malware distribution	08/23/23–06/09/26
104[.]26[.]0[.]192	Malware distribution	06/04/26–06/09/26
104[.]26[.]0[.]201	Malware distribution	01/26/25–06/09/26

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

- They were geolocated in two countries, one of which—the U.S.—was among the registrant countries of the domain IoCs. None of the two, however, were listed as IP IoC geolocation countries.



- They were administered by two ISPs, none of which were identified as IP IoC administrators.



At this point, we had 29 IP addresses in all—three dubbed as IoCs and 26 additional. We queried them on Reverse IP API and learned that two could be dedicated hosts. This step also led to the discovery of 23 unique IP-connected domains after those already named as IoCs and the email-connected domains were filtered out.

The results of our Threat Intelligence API queries for the IP-connected domains revealed that 10 have already been weaponized for various attacks. Take a look at more information for five examples below.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
6clubgame[.]online	Malware distribution	03/11/26–06/09/26
firewai[.]biz	Malware distribution	05/06/26–06/09/26
hazydvs[.]surf	Malware distribution	05/14/26–06/09/26
jalwa-games[.]shop	Malware distribution	03/11/26–06/09/26
planoch[.]cloud	Malware distribution	04/14/26–06/09/26

After that, we extracted 18 unique text strings from the domain IoCs and used them as Domains & Subdomains Discovery search terms to identify other domains that started with them. We uncovered connections for:

- baxe.
- brightcanvas.
- flame-guard.
- intem.
- ropea.

We unearthed 157 unique string-connected domains after those already named as IoCs and the email- and IP-connected domains were filtered out.

Note that the 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.

Conclusion

Our DNS deep dive into the threat revealed that one client IP address communicated with one of the domain IoCs. We also learned that the domain IoC ropea[.]top was bulk-registered with four look-alikes on 19 February 2026. Three of the domain IoCs, meanwhile, were likely registered with malicious intent 104–161 days before they were identified as IoCs by Check Point Research. In addition, 22 unique IP addresses that could belong to victims communicated with two of the IP IoCs.

We also uncovered 3,098 new artifacts comprising 2,892 email-connected domains, 26 additional IP addresses, 23 IP-connected domains, and 157 string-connected domains. To date, 47 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

- 001441[.]com
- 001550[.]com
- 0018vip[.]com
- a-zonic[.]com
- a7702[.]com
- aa2012qq[.]com
- b4ska[.]com
- badgjgfw[.]com
- bag-new[.]com
- ca-citrus[.]com
- ca88ca88e[.]com
- ca88yazhouca888[.]com
- d9vod[.]net
- dad59[.]com
- dajian88tb[.]com
- e-legions[.]com
- e-mesas[.]com
- e-viethoa[.]com
- farmtwand[.]com
- farmtwios[.]com
- fashionrb-sunglasses[.]us
- g2009[.]com
- gamesholidays[.]com
- gan33[.]com
- h28v[.]com
- h2ql[.]com
- haideaed[.]com
- iambrosi[.]com
- iamgcp[.]com
- iappsnet[.]com
- j13800[.]com
- j138139[.]com
- j168168[.]com
- ka-889[.]com
- kaiweiqipai[.]com
- kaixinporn[.]com
- l8gjptlhji[.]com
- lacostecheaponline[.]org
- lacosteoutletstore[.]com
- machining-cnc[.]net
- mackayecc[.]com
- madbrooks[.]com
- nailsnews[.]com
- nanayy[.]com
- nannilux[.]com
- oakforyou[.]com
- oapbingo[.]com
- ochpub[.]com
- papacao[.]com
- partwall[.]com
- patagoniasaleonline[.]org
- qb999[.]us
- qbet2013[.]com
- qbshua[.]com
- radartrak[.]com
- raigyoroddo[.]com
- ramcondo[.]com
- s13800[.]com
- s138139[.]com
- s188189[.]com
- taderbaby[.]com
- taihesupply[.]com
- talarbyra[.]com
- ubg260[.]com
- ubg263[.]com
- ubg265[.]com
- valcampus[.]com
- vaugency[.]com
- vaughanfs[.]com
- w88-phone[.]com
- w88con[.]com
- w88funs[.]com
- xadkgm[.]com
- xaztyxcm[.]com

- xcguitar[.]com
- yangguangqipai[.]com
- yaonilu[.]co
- yaonilu[.]net
- zaixianzhajinhua[.]net
- zaogroup[.]com
- zapatosdenikefutbol[.]com

Sample Additional IP Addresses

- 104[.]21[.]24[.]60
- 104[.]21[.]81[.]50
- 104[.]26[.]0[.]192
- 172[.]67[.]156[.]249
- 172[.]67[.]217[.]34
- 172[.]67[.]70[.]18
- 194[.]164[.]72[.]136

Sample IP-Connected Domains

- 6clubgame[.]online
- checkx1[.]spidy[.]shop
- checkx3[.]spidy[.]shop
- dtmertsakarya[.]com
- energbn[.]surf
- firewai[.]biz
- hazydvs[.]surf
- jalwa-games[.]shop
- olydent[.]com
- panel1[.]spidy[.]shop
- questerbox[.]top
- remnane[.]biz
- servif[.]shop
- www[.]dtmertsakarya[.]com

Sample String-Connected Domains

- baxe[.]ai
- baxe[.]arab
- baxe[.]belau[.]pw
- brightcanvas[.]ae
- brightcanvas[.]ai
- brightcanvas[.]art
- flame-guard[.]co[.]uk
- flame-guard[.]co[.]za
- flame-guard[.]com
- intem[.]academy
- intem[.]asia
- intem[.]at
- ropea[.]cn
- ropea[.]com
- ropea[.]de