WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A DNS Study of the Macsync, Shub Stealer, and AMOS-Distributing macOS ClickFix Campaign

Threat Report

Table of Contents

Executive Report

Microsoft recently published their in-depth analysis of a ClickFix campaign targeting macOS users with three infostealers—Macsync, Shub Stealer, and AMOS. The threat actors attempted to take advantage of users looking for helpful advice on macOS-related issues in blog sites and other user-driven content platforms by hosting their malicious commands in these sites. The researchers identified 140 network IoCs connected to the threat.

We extracted unique domains from the subdomain IoCs and weeded out those that belonged to legitimate entities and were currently inactive aided by the WhoisXML API MCP Server. That left us with 138 IoCs for our investigation comprising nine subdomains, 121 domains, and eight IP addresses.

Our DNS deep dive into the macOS ClickFix campaign led to these discoveries:

- 11 unique client IP addresses that communicated with 14 of the domain IoCs
- Eight domain IoCs that appeared in seven typosquatting groups with 3–33 members each
- Eight domain IoCs that were likely registered with malicious intent
- 119 unique IP addresses potentially owned by victims that communicated with five of the IP IoCs
- 691 email-connected domains, 14 of which were confirmed malicious
- 141 additional IP addresses, all of which were confirmed malicious
- Seven IP-connected domains, four of which were confirmed malicious
- 322 string-connected domains, 29 of which were confirmed malicious

Subdomain IoCs in the DNS Spotlight

We kicked off our analysis by subjecting the nine subdomain IoCs to further scrutiny.

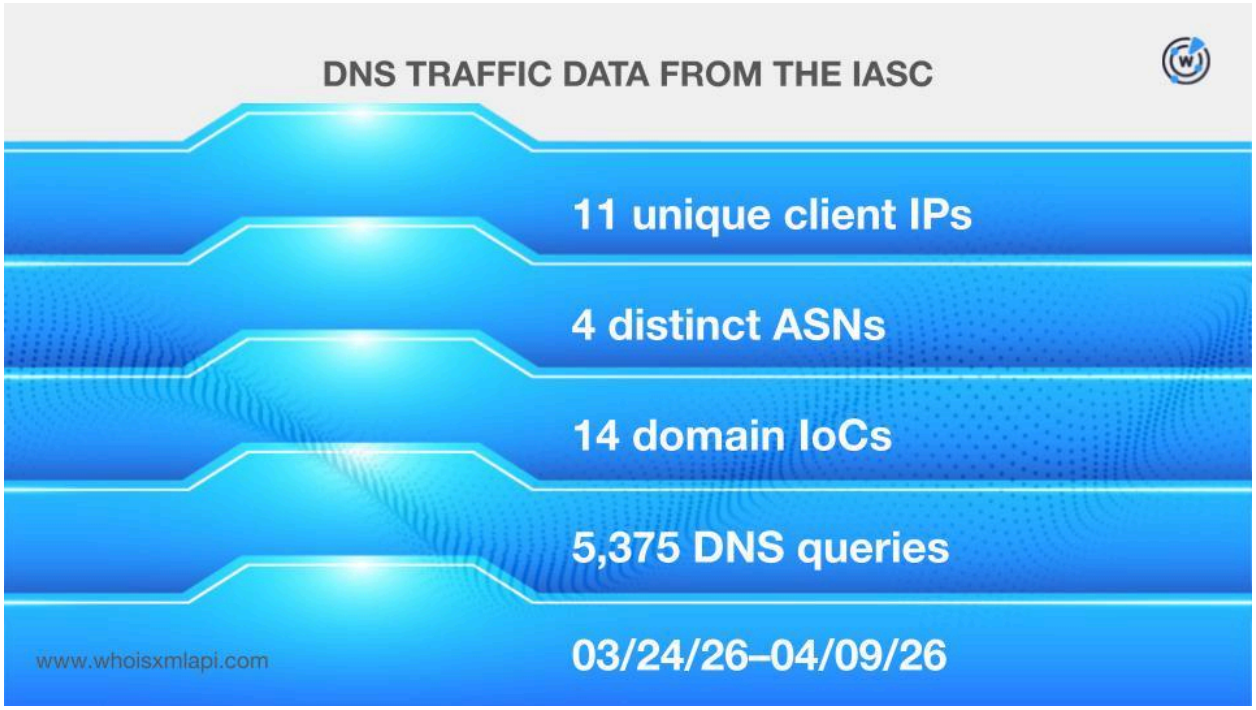
Our WhoisXML API MCP Server queries for the subdomain IoCs revealed that while a majority were under legitimate apex domains, all of them still warrant suspicion from users. Take a look at possible reasons for five examples below.

SUBDOMAIN IoC	WXA MCP SERVER FINDING
apple-mac-fix-hidden[.]medium[.]com	While hosted on a legitimate publishing platform, the keyword-stuffed Apple or Mac fix or hidden name is typical of tech-support scams or SEO lures.
claudecodedoc[.]squarespace[.]com	While also hosted on a legitimate publishing platform, it possibly impersonates official Claude Code docs that reside in docs[.]claude[.]com, never a Squarespace subdomain.
kvrnjr30[.]apexharvestor[.]digital	It contains random strings on an unrecognized apex domain, which is a pattern associated with disposable or automated infrastructure.

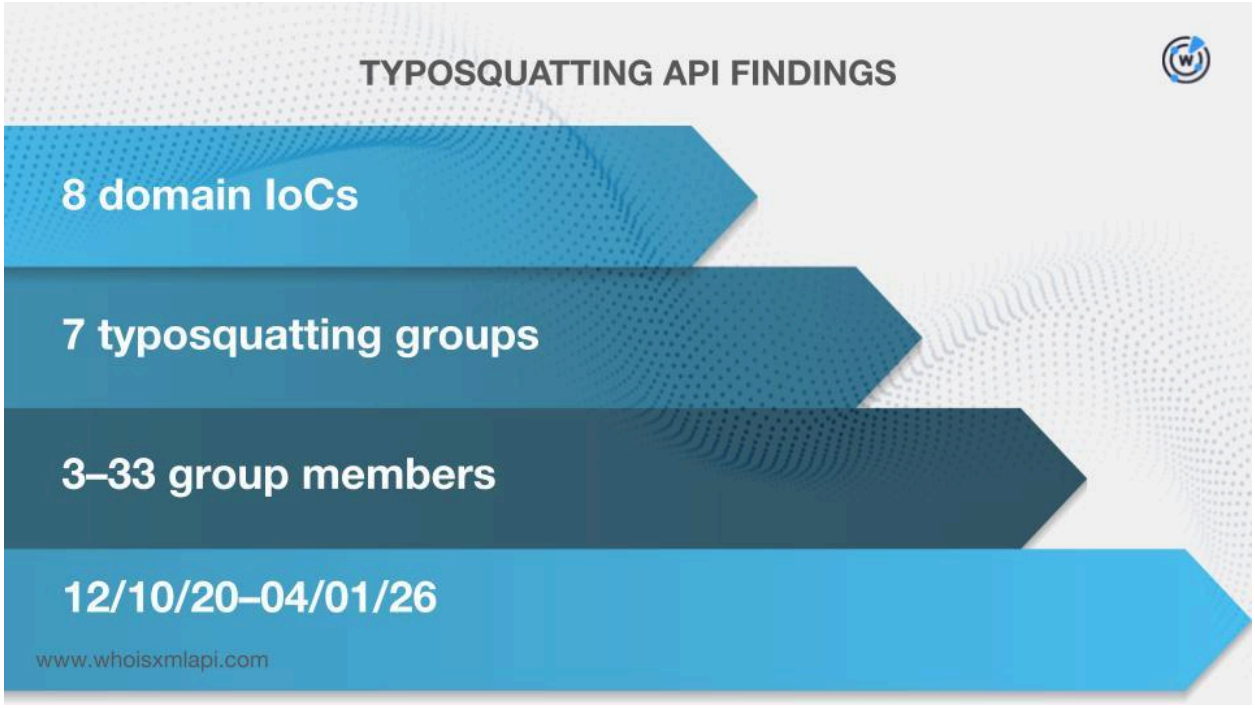
Domain IoCs Demystified

Next, we looked more closely into the 121 domain IoCs.

First, sample network traffic data from the IASC revealed that 11 unique client IP addresses under four distinct ASNs communicated with 14 of the domain IoCs via 5,375 DNS queries made between 24 March and 9 April 2026.



The results of our Typosquatting API queries, meanwhile, showed that eight of the domain IoCs appeared in seven groups with 3–33 members each between 10 December 2020 and 1 April 2026.



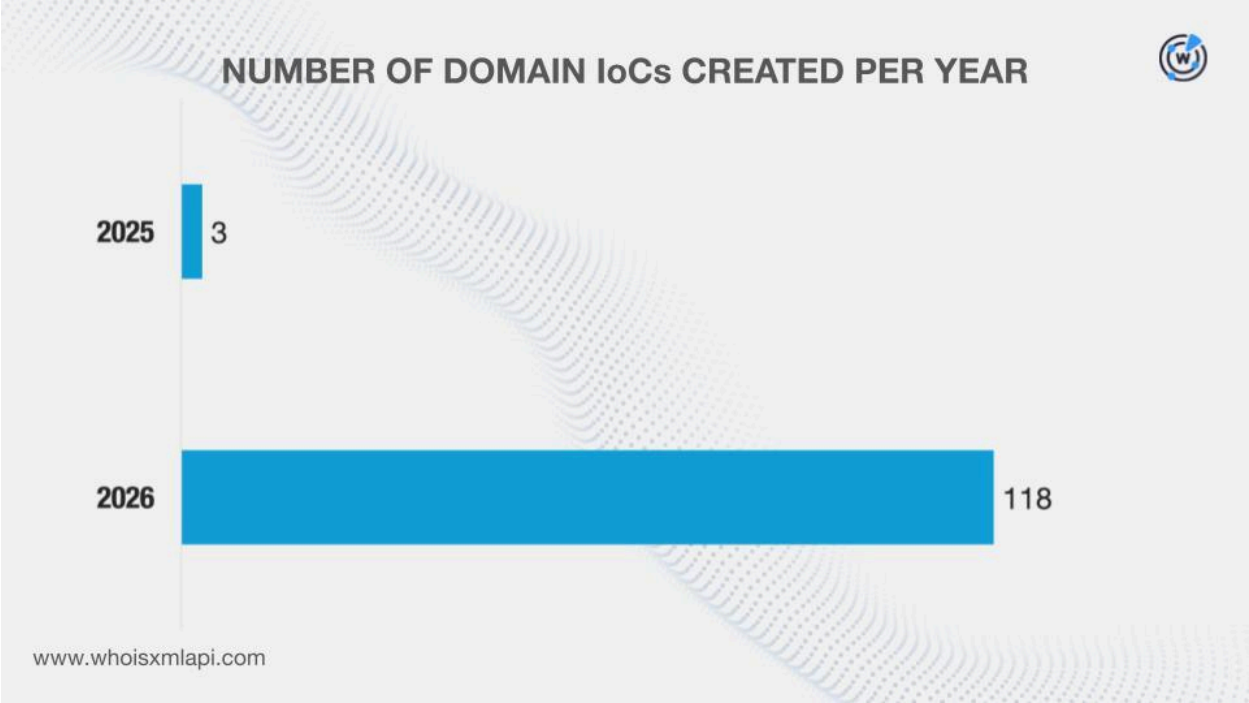
It is worth noting that two domain IoCs—rapidfilevault4[.]cyou and rapidfilevault5[.]sbs—appeared in the same typosquatting group with 11 members, all created on 18 February 2026. Their look-alike domains were rapidfilevault1[.]cfd, rapidfilevault1[.]cyou, rapidfilevault1[.]lat, rapidfilevault1[.]mom, rapidfilevault2[.]mom, rapidfilevault3[.]cyou, rapidfilevault4[.]xyz, rapidfilevault5[.]baby, and rapidfilevault5[.]xyz.

Eight of the domain IoCs also appeared in the First Watch Malicious Domains Data Feed 57–476 days before Microsoft dubbed them as IoCs on 6 May 2026. Take a look at more information for five examples below.

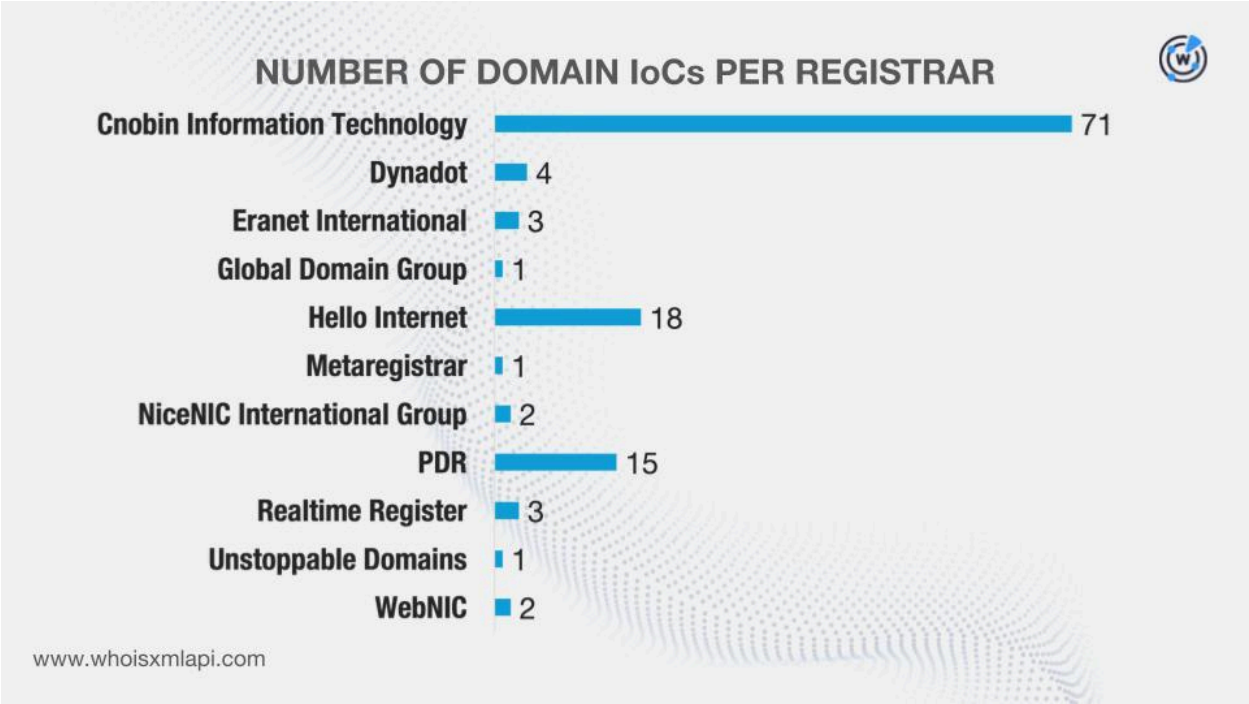
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE THE REPORT DATE
tmcnex[.]com	01/15/25	476
quantumdataserver5[.]homes	02/18/26	77
rapidfilevault4[.]cyou	02/18/26	77
coco2-hram[.]com	02/27/26	68
res2erch-sl0ut[.]com	03/02/26	65

We then queried the domain IoCs on WHOIS API and discovered that:

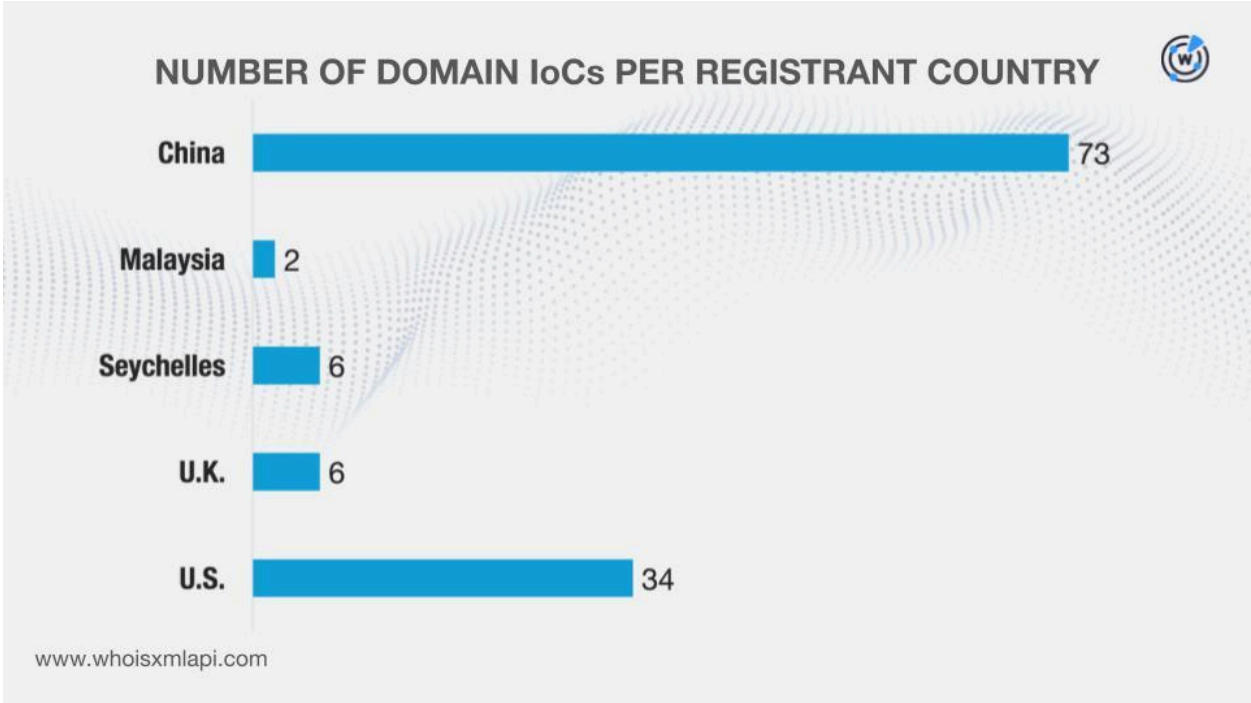
- They were created between 18 July 2025 and 24 April 2026, seemingly indicating the threat actors' penchant for using NRDs in their campaigns.



- They were administered by 11 different registrars.



- They were registered in five different countries.



Finally, we queried the domain IoCs on DNS Chronicle API and learned that together they recorded 12,131 historical domain-to-IP resolutions over time. Here are more details for five examples.

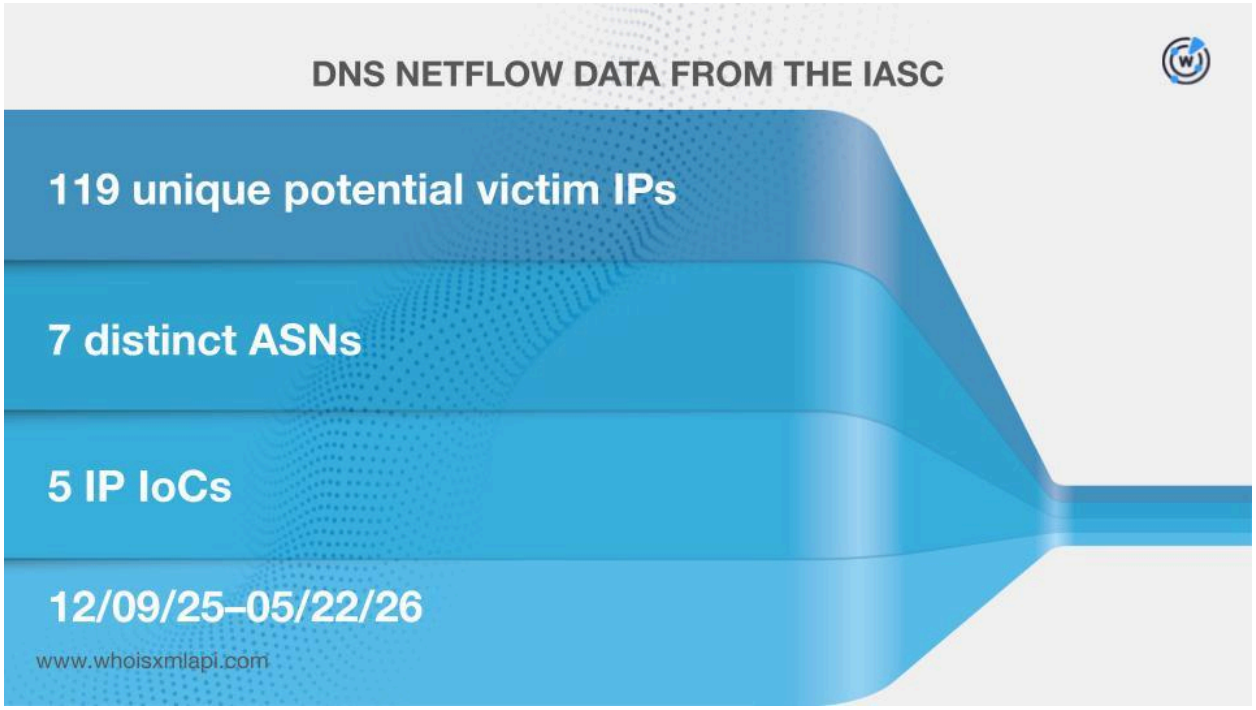
DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
ptrei[.]com	918	02/06/17–03/11/26
aforvm[.]com	608	02/05/17–05/20/26
lakhov[.]com	560	02/06/17–05/17/26
jpbassin[.]com	515	02/06/17–05/20/26
biopranica[.]com	431	06/17/18–05/09/26

While many of the domain IoCs seemed to have been reregistered recently given their first resolution dates, 73 were actually NRDs since they posted their first resolutions just this year.

IP IoCs Investigated Further

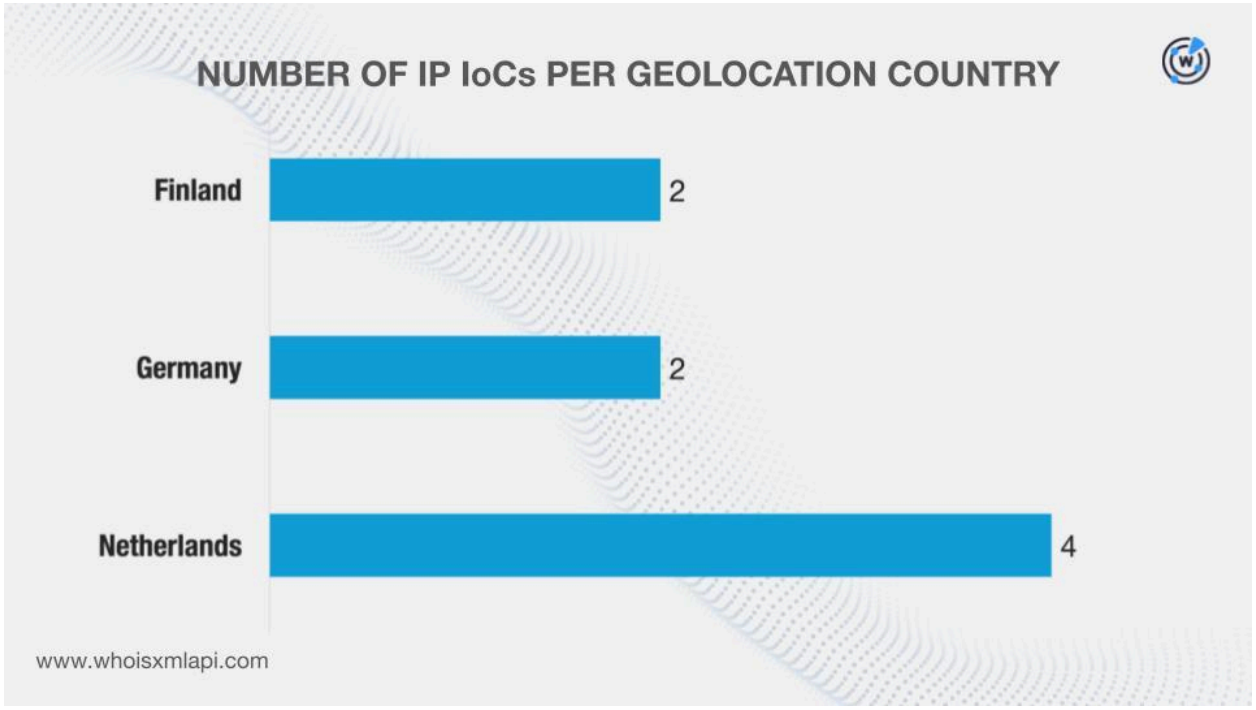
After that, we dug deeper into the DNS footprint of the eight IP IoCs.

First, sample network traffic data from the IASC revealed that 119 unique IP addresses potentially owned by victims under seven distinct ASNs communicated with five of the IP IoCs between 9 December 2025 and 22 May 2026.

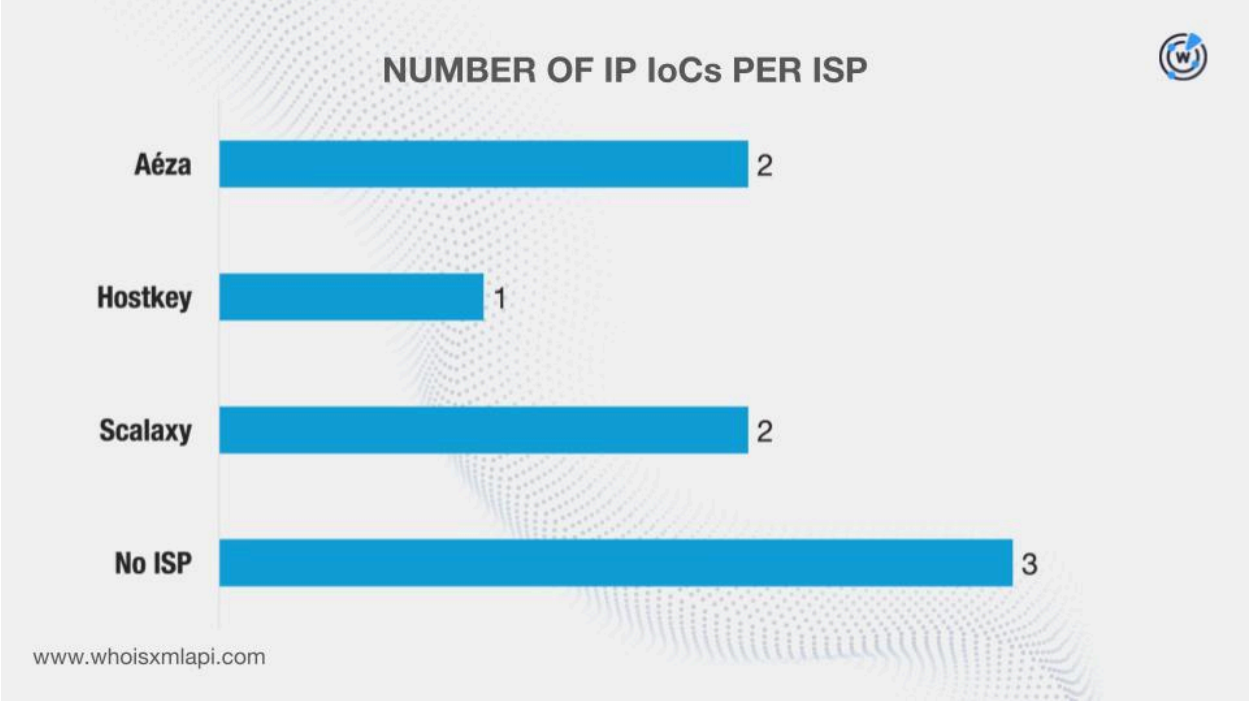


We then queried the IP IoCs on [Bulk IP Geolocation Lookup] and found out that:

- They were geolocated in three different countries, none of which were consistent with any of the registrant countries identified earlier.



- While three did not have ISPs on record, the remaining five were administered by three different entities.



Finally, DNS Chronicle API queries for the IP IoCs revealed that four recorded 208 historical IP-to-domain resolutions over time. The IP IoC 199[.]217[.]98[.]33, for instance, posted 173 resolutions spanning 25 January and 22 May 2026.

Hunting for New Artifacts

After learning more about the network IoCs, we then searched for new artifacts.

First, we queried the domain IoCs on WHOIS History API. We discovered that 61 had 375 unique email addresses in their historical records. Further scrutiny revealed that 50 were public email addresses.

Reverse WHOIS API queries for the public email addresses allowed us to name 691 unique email-connected domains after the domain IoCs were filtered out.

The results of our Threat Intelligence API queries for the email-connected domains showed that 14 have already been weaponized for various cyber attacks. Take a look at more information for five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
woupp[.]com	Malware distribution Generic threat	03/14/26–05/22/26 03/15/26
atcoconst[.]com	Malware distribution	04/30/26–05/22/26
cvols[.]com	Malware distribution	05/08/26–05/22/26
ejecen[.]com	Malware distribution	03/26/26–05/22/26
rvdownloads[.]com	Malware distribution	03/24/26–05/22/26

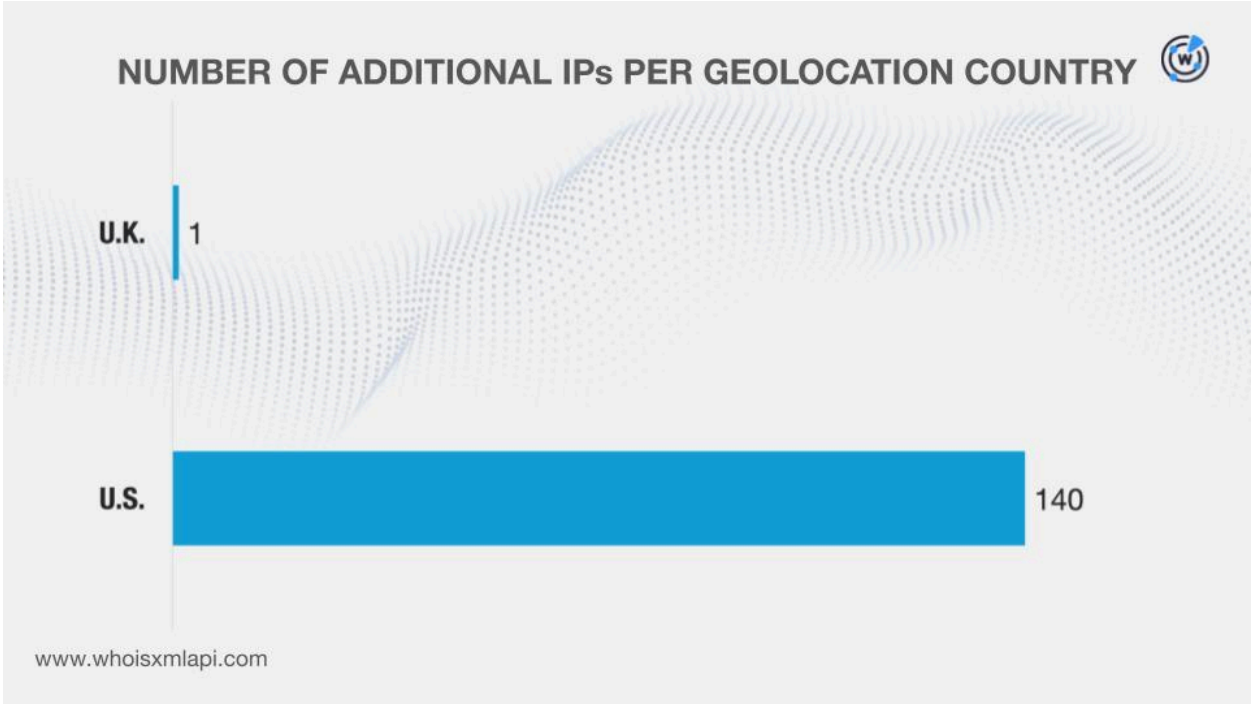
We then queried the domain IoCs on DNS Lookup API and found out that 71 actively resolved to various IP addresses. This led to the discovery of 141 unique additional IP addresses after the IP IoCs were filtered out.

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.

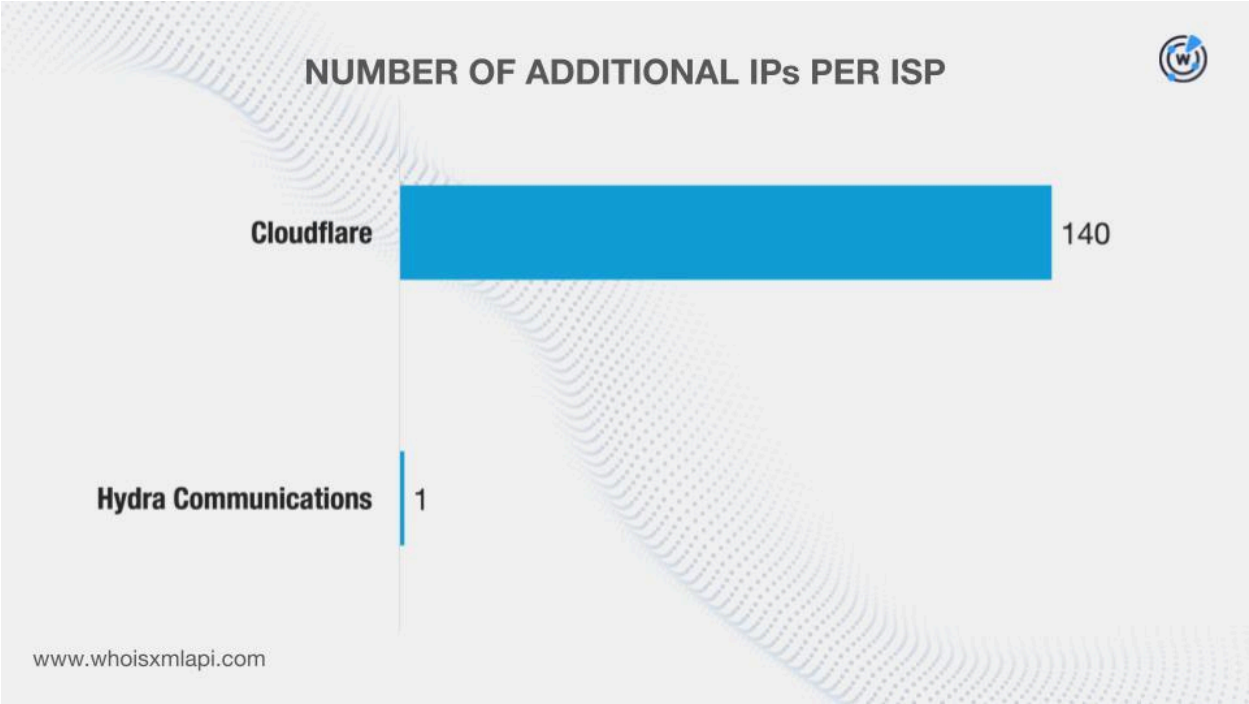
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
104[.]21[.]92[.]235	Malware distribution Phishing Generic threat Suspicious activity Spam campaign	01/02/25–05/21/26 07/19/23–05/04/26 10/09/23–05/03/26 05/15/25–08/25/25 02/17/24–06/21/24
172[.]67[.]145[.]188	Malware distribution Phishing Generic threat Suspicious activity	04/03/24–05/21/26 02/23/24–05/21/26 02/23/24–05/18/26 05/19/25–09/09/25
104[.]21[.]10[.]79	Malware distribution Phishing Generic threat	12/04/23–03/28/26 03/28/23–05/18/26 03/30/23–05/07/26
104[.]21[.]12[.]180	Phishing Malware distribution	04/01/23–05/22/26 01/11/24–05/21/26
104[.]21[.]12[.]186	Malware distribution	06/10/24–05/22/26

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

- They were geolocated in two countries—the U.K. and the U.S. Both were named registrant countries earlier.



- They were administered by two ISPs, none of which were named as administrators of the IP IoCs.



After that, we now had 149 IP addresses for our study—eight identified as IoCs and 141 additional ones. Reverse IP API queries for them showed that four could be dedicated hosts. Together, our search led to the discovery of seven unique IP-connected domains after the domain IoCs and the email-connected domains were filtered out.

According to Threat Intelligence API, the IP-connected domain instantgofast[.]click has already been flagged for malware distribution between 16 and 23 May 2026.

Next, we extracted unique text strings from the domain IoCs. Domains & Subdomains Discovery searches for other domains (i.e., not yet tagged as IoCs) that started with them uncovered connections for 36 strings including but not limited to the following:

- 0x666.
- avafex.
- biopranica.
- cleanmymacos.
- ejecen.
- ftduk.
- hacelu.
- isgilan.
- jihiz.
- kcbps.
- lakhov.
- malext.
- ouilov.
- play67.
- quantumdataserver5.
- rapidfilevault4.
- stclegion.
- vagturk.
- woupp.
- xeebii.

We were able to uncover 322 unique string-connected domains after the domain 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.

The results of our Threat Intelligence API queries for the string-connected domains showed that 29 have already been associated with various threats. Take a look at more information for five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
biopranica[.]com	Malware distribution	02/23/26–05/23/26
cleanmymacos[.]com	Malware distribution	06/19/25–05/23/26
ptrei[.]com	Malware distribution	03/26/26–05/23/26
quantumdataserver5[.]baby	Malware distribution	03/07/26–05/23/26
rapidfilevault4[.]baby	Malware distribution	03/01/26–05/23/26

Conclusion

Our in-depth DNS investigation of the ClickFix campaign targeting macOS users with Macsync, Shub Stealer, and AMOS revealed that 11 unique client IP addresses communicated with 14 of the domain IoCs while 119 IP addresses potentially owned by victims communicated with five of the IP IoCs.

In addition, eight of the domain IoCs appeared in seven typosquatting groups with 3–33 members each. Also, eight of the domain IoCs were likely registered with malicious intent.

Our IoC list expansion analysis, meanwhile, led to the discovery of 1,161 new artifacts comprising 691 email-connected domains, 141 additional IP addresses, seven IP-connected domains, and 322 string-connected domains that could be tied to the threat. To date, 188 of these artifacts have already been weaponized for various cyber 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

- 10gbp[.]com
- 30jourspourboostersaliste[.]com
- 4allpay[.]biz
- 99p-research[.]com
- a4tech[.]webcam
- bankorbis[.]com
- cafespitz[.]com
- d-proof[.]com
- e-osap[.]com
- faciledocs[.]com
- galeranchhoa[.]com
- hangesulka[.]digital
- ibercursos[.]com
- jepeux[.]net
- kalite[.]webcam
- laevitas[.]com
- m-abs[.]com
- negralia[.]com
- occass[.]com
- pactvm[.]com
- quantumharbinger[.]digital
- radiantprospera[.]digital
- saadaprint[.]com
- ta-dent[.]com
- u-ranker[.]com
- valontime[.]com
- waaiex[.]com
- xeebii[.]com
- yaixa[.]com
- zayk[.]net

Sample Additional IP Addresses

- 104[.]21[.]10[.]79
- 172[.]67[.]130[.]102
- 185[.]125[.]207[.]135

Sample IP-Connected Domains

- balifastferries[.]shop
- instantgofast[.]click
- mediaboosting[.]ru

Sample String-Connected Domains

- 0x666[.]art
- avafex[.]co[.]bb
- biopranica[.]cl
- boosterjuices[.]ca
- cleanmymacos[.]app
- contatoplus[.]app[.]br
- ejecen[.]es
- ftduk[.]co[.]uk
- hacelu[.]cn
- honestly[.]ae
- isgilan[.]com[.]tr
- jihiz[.]us
- joytion[.]cn
- kcbps[.]cn
- korovkamu[.]online
- lakhov[.]ru
- lbarticle[.]ru
- malext[.]io

- malkim[.]ca
- miappl[.]edu[.]ee
- ouilov[.]fr
- play67[.]com
- ptrei[.]arab
- quantumdataserver5[.]baby
- rapidfilevault4[.]baby
- rapidfilevault5[.]baby
- raxelpak[.]com
- raytherrien[.]ca
- reachnv[.]org
- stclegion[.]ws
- stinarosen[.]online
- vagturk[.]net
- vcopp[.]co[.]za
- woupp[.]cn
- xeebii[.]in