WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

The DNS Anatomy of the Axios Supply Chain Attack

Threat Report

Table of Contents

Executive Report

GTIG uncovered a UN1069 attack targeting the popular NPM package axios on 31 March 2026. They published their in-depth analysis of the threat on 1 April 2026 and in it named three IoCs.

Two other reports on the attack identified IoCs as well. Elastic Security Labs disclosed two on 1 April 2026 and GitHub listed 16 on 31 March 2026.

After removing duplicates, extracting domains from the subdomains, and filtering out legitimate domains aided by the WhoisXML API MCP Server, we ended up with 22 IoCs for our analysis comprising five subdomains, seven domains, and 10 IP addresses.

Our DNS deep dive into the Axios supply chain attack IoCs led to these discoveries:

- 16 unique client IP addresses that communicated with two of the domain IoCs
- Two domain IoCs appeared in two typosquatting groups with 5–12 members each
- One domain IoC likely registered with malicious intent 651 days before being confirmed as malicious
- 32 distinct IP addresses potentially owned by victims that communicated with seven of the IP IoCs
- 676 email-connected domains
- Two additional IP addresses, both confirmed as malicious
- 58 IP-connected domains, four of which were confirmed as malicious
- 1,034 string-connected domains, one of which was confirmed as malicious

A sample of the additional artifacts obtained from our analysis is available for download from our website.

Studying the Subdomains Singled Out as Axios Supply Chain Attack IoCs

We kicked our investigation off by looking more closely at five subdomain IoCs and documented our findings below.

SUBDOMAIN IoC	WXA MCP SERVER FINDING
cloud[.]dnx[.]capital	Lacks DNS records, WHOIS data, or web presence, which are red flags especially if used in the financial context in emails, messages, or ads
crypto[.]hondchain[.]com	Has all the hallmarks of a fraudulent or inactive phishing

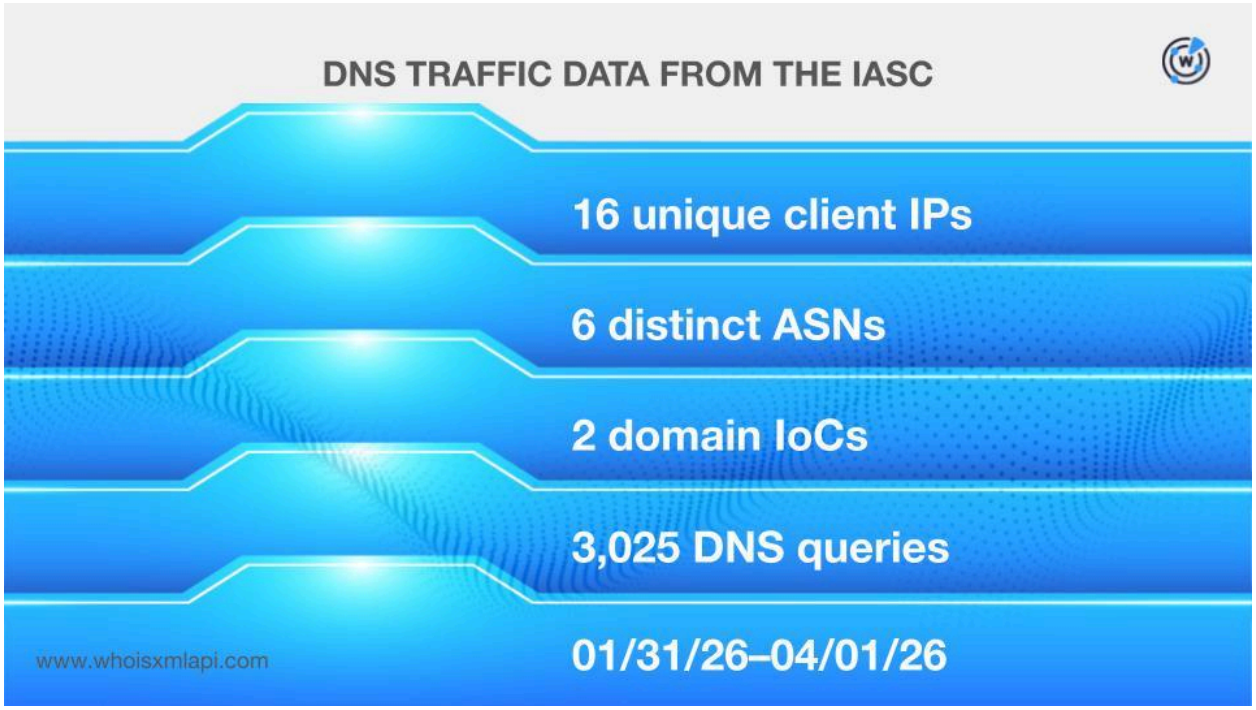
	or scam site
deck[.]31ventures[.]info	Almost certainly impersonating the legitimate 31VENTURES venture capital firm and combined with being newly registered and full WHOIS privacy, is a textbook setup for either phishing or an investment fraud scheme
docsend[.]linkpc[.]net	Follows a textbook phishing domain construction — a fake docsend subdomain on a free, anonymous dynamic DNS service known for abuse
webhostwatto[.]work[.]gd	Not connected to a legitimate business operation, currently inactive, and structured using a fabricated name on a free, anonymous subdomain service

Overall, it is advisable not to click any links containing the five subdomains above as they could be tied to financially motivated or other scams.

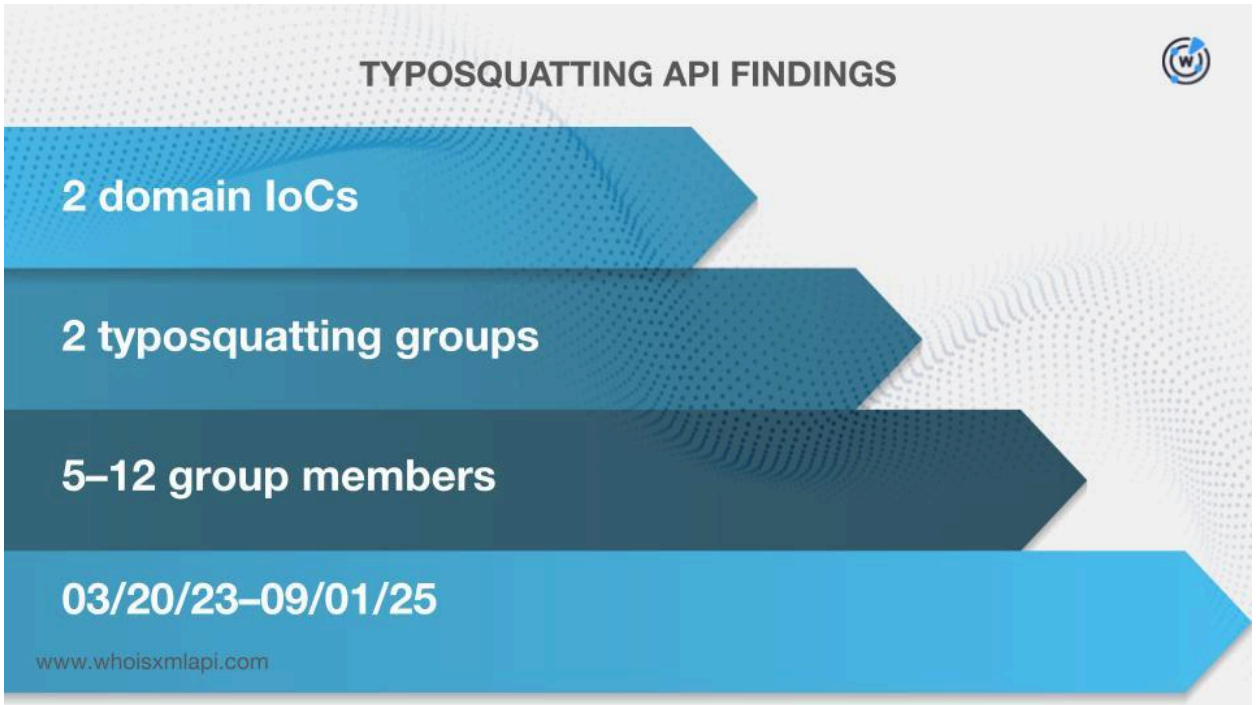
Deep Diving into the Domains Disclosed as Axios Supply Chain Attack IoCs

Next, we looked further into the seven domain IoCs.

Sample network traffic data from the IASC revealed that 16 unique client IP addresses under six distinct ASNs communicated with two domain IoCs via 3,025 DNS queries between 31 January and 1 April 2026.



According to our Typosquatting API findings, meanwhile, two domain IoCs appeared in two groups with 5–12 members each between 20 March 2023 and 1 September 2025.



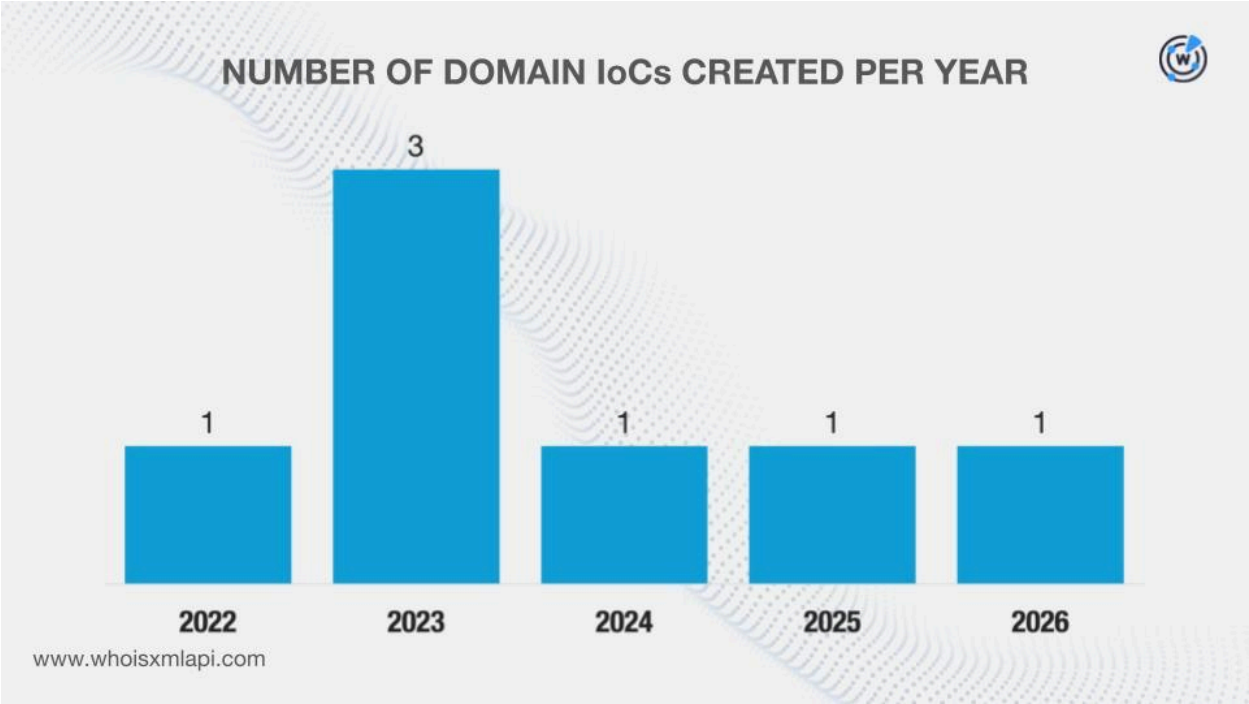
Take a look at more details about the typosquatting domains below.

DOMAIN IoC	GROUP NUMBER	GROUP MEMBER NUMBER	GROUP MEMBERS	CREATION DATE
31ventures[.]info	1	5	adventures[.]capetown h4ventures[.]dev ad-venture1[.]pl adventure[.]capetown 31ventures[.]info	08/29/25–09/01/25
starbucls[.]xyz	1	12	starbucls[.]makeup starbucls[.]autos starbucls[.]ink starbucls[.]guru starbucls[.]quest starbucls[.]today starbucls[.]cyou starbucls[.]xyz starbucls[.]life starbucls[.]top starbucls[.]icu starbucls[.]homes	03/20/23

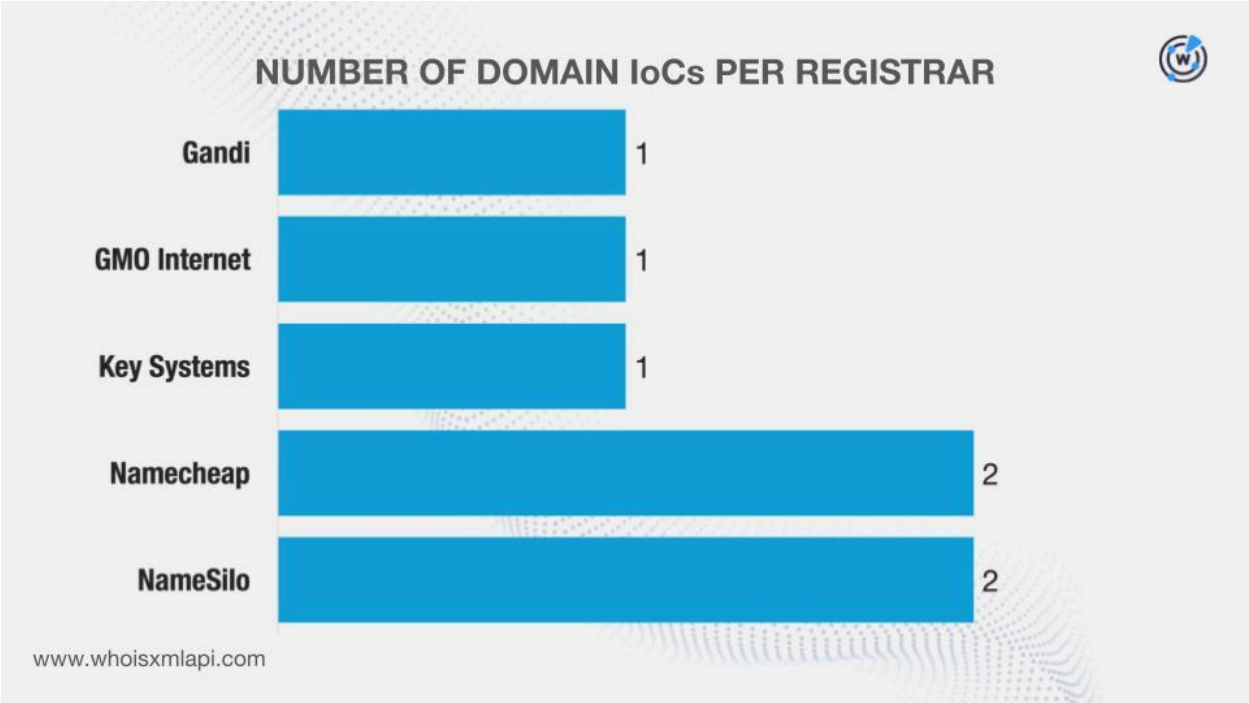
Based on the results of our First Watch Malicious Domains Data Feed queries, on the other hand, the domain IoC dnx[.]capital was likely registered with malicious intent 651 days before it was dubbed as an IoC on 31 March 2026 by GitHub.

Next, we queried the domain IoCs on WHOIS API and filled in missing details using Domain Info API. We discovered that:

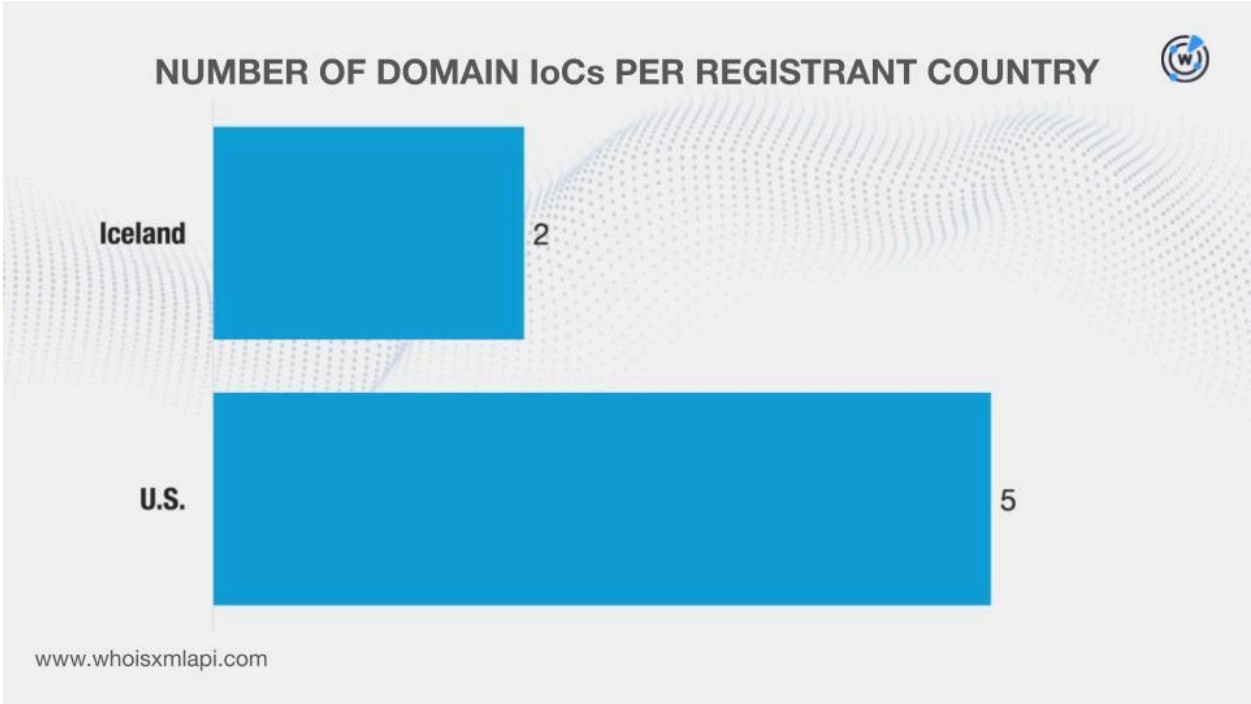
- They were created between 18 June 2022 and 30 March 2026.



- They were administered by five registrars.



- They were registered in two countries.



Finally, we queried the domain IoCs on DNS Chronicle API and learned that they recorded 913 historical domain-to-IP resolutions over time. Here are more details for three examples.

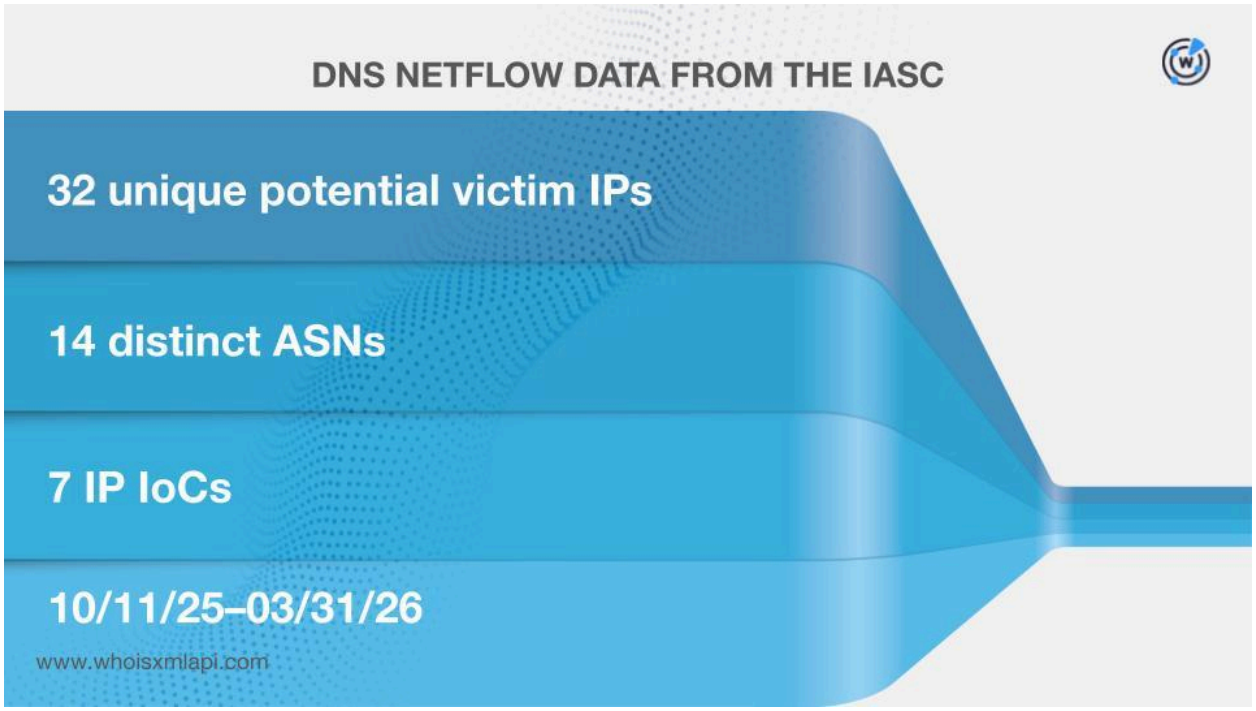
DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
work[.]gd	803	08/26/17–03/23/26
31ventures[.]info	51	06/06/22–03/16/26
dnx[.]capital	42	11/07/22–05/28/25

In addition, we discovered that all three domains above could have been reregistered, as they posted older domain-to-IP resolutions than the creation dates in their current WHOIS records.

Investigating the IP Addresses Identified as Axios Supply Chain Attack IoCs

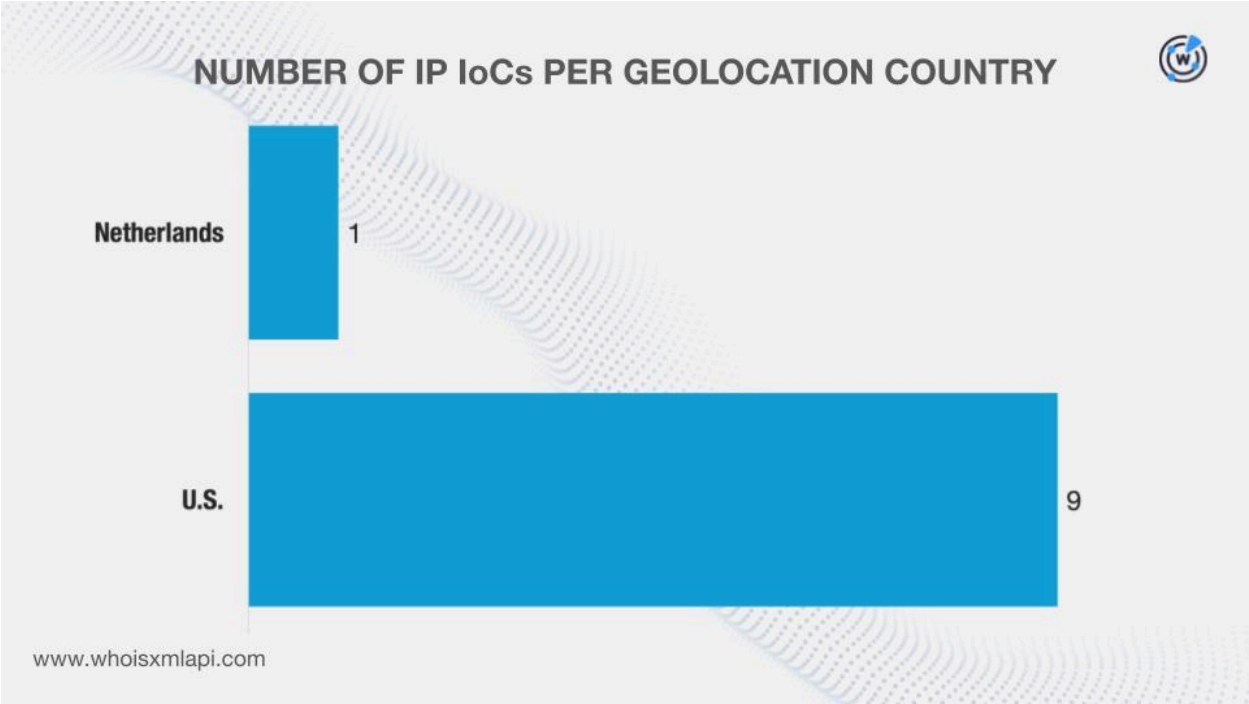
We then further investigated the 10 IP IoCs.

Sample network traffic data from the IASC revealed that 32 unique IP addresses that could belong to victims under 14 distinct ASNs communicated with seven of the IP IoCs between 11 October 2025 and 31 March 2026.



Next, we queried the IP IoCs on Bulk IP Geolocation Lookup and learned that:

- They were geolocated in two countries, one of which—the U.S.—was also named as a registrant country of five of the domain IoCs.



- They were all administered by a single ISP—Hotswinds.

After that, we queried the IP IoCs on DNS Chronicle API and discovered that they recorded 3,155 historical IP-to-domain resolutions over time. Take a look at more information on five examples below.

IP IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	DATES SEEN
23[.]254[.]128[.]114	769	02/05/17–02/06/26
23[.]254[.]253[.]75	736	03/11/18–03/26/26
104[.]168[.]167[.]88	383	03/22/19–11/04/25
142[.]11[.]212[.]104	61	08/16/19–02/27/26
104[.]168[.]214[.]151	305	10/04/19–08/08/24

Hunting for New Axios Supply Chain Attack Artifacts

After knowing more about the 22 IoCs, we searched for more connected artifacts.

First, we queried the domain IoCs on WHOIS History API and discovered that four had six unique email addresses in their historical WHOIS records. Of these, one was a public email address.

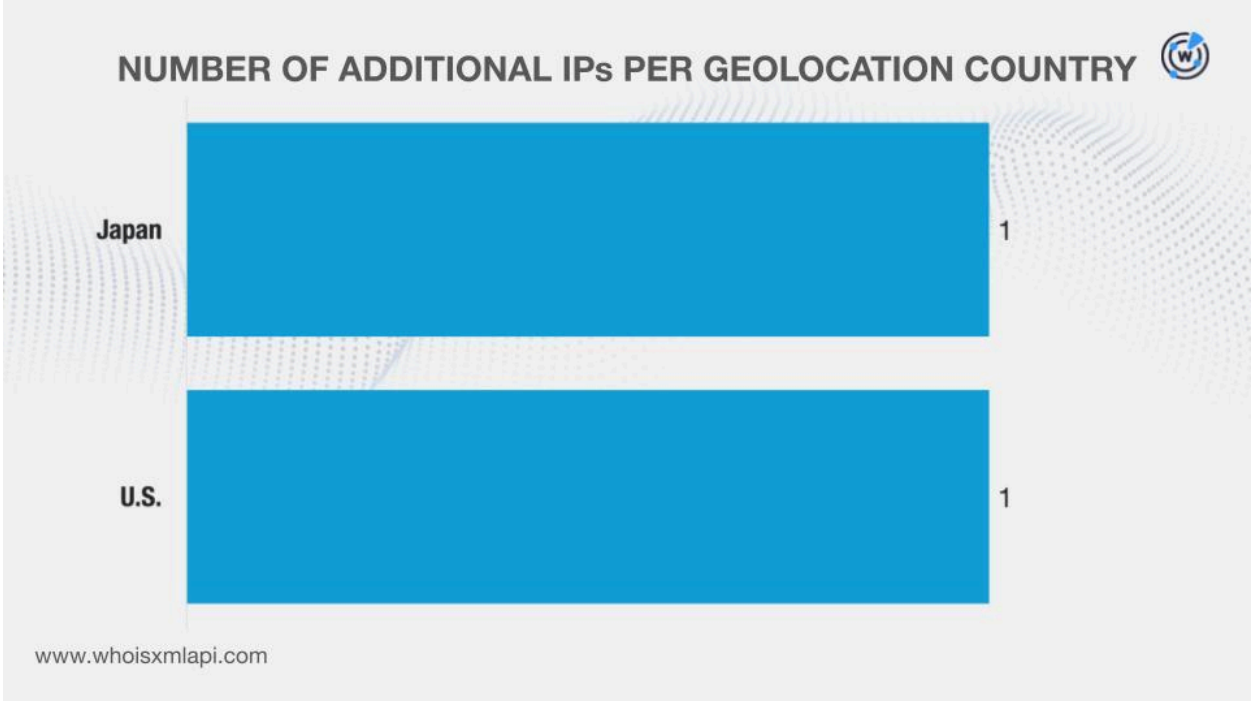
We queried the sole public email address on Reverse WHOIS API and uncovered 676 unique email-connected domains after the domain IoCs were filtered out.

Next, we queried the domain IoCs on DNS Lookup API, which led to the discovery of two unique additional IP addresses.

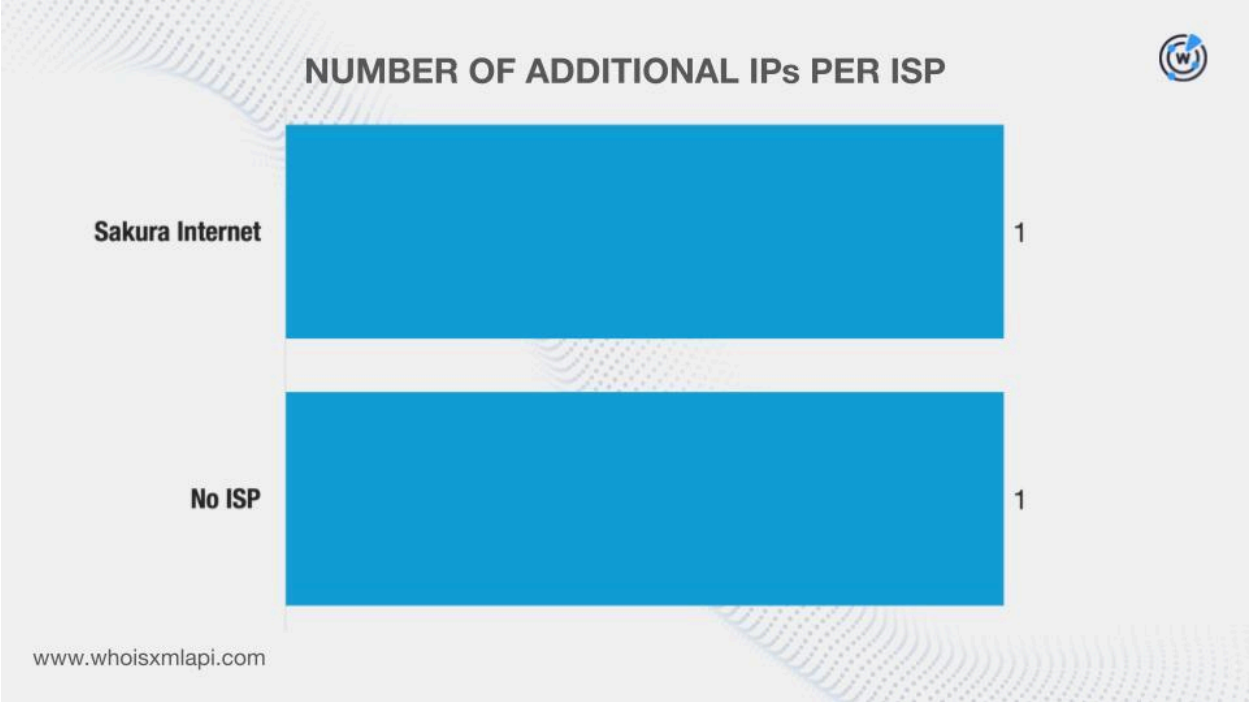
According to our Threat Intelligence API query results, both additional IP addresses have already been weaponized for various attacks. The IP address 160[.]16[.]200[.]77, for instance, has already been associated with phishing (04/01/25–04/01/26) and malware distribution (10/19/24–03/28/26).

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

- Each was registered in a different country and one—the U.S.—was also the geolocation country of nine of the IP IoCs.



- While one did not have an ISP on record, the other was administered by an ISP that was not on the list for the IP IoCs—Sakura Internet.



After that, we now had 12 IP addresses (10 IoCs and two additional) on hand for the next step. We queried them on Reverse IP API and discovered that seven could be dedicated hosts. Together, they hosted 58 unique IP-connected domains after the domain IoCs and the email-connected domains were filtered out.

Threat Intelligence API queries for the IP-connected domains showed that four have already been weaponized for various attacks. The IP-connected domain callnrwise[.]com, for instance, has already been associated with malware distribution between 31 March and 1 April 2026.

Finally, we scoured the DNS for other domains that started with the same text strings as the domain IoCs via Domains & Subdomains Discovery. We collated 1,034 unique string-connected domains after the domain IoCs and the email- and IP-connected domains were filtered out. They started with these strings:

- 31ventures.
- dnx.
- sfrclak.
- starbucls.
- work.

Note 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. Pay special attention to those starting with **31ventures.** as some

may turn out to be legitimate, likely belonging to Japanese venture capital firm 31VENTURES. Those starting with **work.** are also worth looking further into given the string's generic nature.

So far, only one of the string-connected domains—starbucls[.]top—has already been weaponized for an attack. It has already been associated with malware distribution between 2 October 2023 and 1 April 2026.

Final Word

Our DNS deep dive into the Axios supply chain attack IoCs revealed that 16 unique client IP addresses communicated with two of the domain IoCs. Two domain IoCs, meanwhile, appeared in two typosquatting groups with 5–12 members each. And one domain IoC was likely registered with malicious intent 651 days before it was confirmed as malicious.

In addition, 32 distinct IP addresses potentially owned by victims communicated with seven of the IP IoCs.

Finally, we uncovered 1,770 new artifacts comprising 676 email-connected domains, two additional IP addresses, 58 IP-connected domains, and 1,034 string-connected domains. Of these, seven 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

- 021store[.]com
- 022bbs[.]net
- 022store[.]com
- acbbs[.]cn
- acez[.]cn
- agcb[.]com[.]cn
- b2bshequ[.]com
- babalisted[.]com
- babalistednyse[.]com
- caiben[.]net
- cangguan[.]net
- ceju[.]top
- daodianbao[.]net
- dapengche[.]com[.]cn
- darenkaipai[.]com
- e6088[.]com
- ebaijiaoyu[.]com
- ecommerce[.]org[.]cn
- fangchengshi[.]net
- fanyiyuan[.]cn
- fbbbs[.]cn
- game5432[.]com
- game56789[.]com
- game7654[.]com
- h[.]gs[.]cn
- harbinvc[.]com
- hawu[.]top
- ichaohu[.]cn
- iheima[.]club
- iloveu[.]club
- jdfinancial[.]com[.]cn
- jdlogistic[.]cn
- jdshare[.]cn
- kcdbbs[.]com
- kejiqi[.]net
- kkwifi[.]cn
- langhao[.]net
- leboapp[.]com
- ledai365[.]cn
- maijiuweng[.]net
- mbacollege[.]cn
- meice[.]net
- nankingbank[.]com
- nengtu[.]cn
- neqi[.]top
- o[.]tj[.]cn
- ouming[.]net
- oxoxox[.]cn
- p[.]gs[.]cn
- panapple[.]cn
- paze[.]top
- qgbbs[.]cn
- qichebbs[.]net
- qingnianren[.]net
- rbbbs[.]cn
- rjbbs[.]cn
- rrobot[.]net
- sanliu[.]net
- sexadultproducts[.]com
- sfcapital[.]cn
- taobaoyiqu[.]com
- taopinpai[.]net
- tencentbanking[.]com
- ucstore[.]cn
- v[.]gs[.]cn
- vancollection[.]net
- vcangel[.]net
- wandaeb[.]com
- wandaec[.]net
- wandatech[.]cn
- xbcapital[.]com
- xdbbs[.]cn
- xfbbs[.]cn
- yahi[.]net

- yaocaidian[.]net
- yaoyaosi[.]cn
- zaiyunduan[.]cn
- zcbbs[.]net
- zhainvbao[.]com

Sample Additional IP Address

- 160[.]16[.]200[.]77

Sample IP-Connected Domains

- 2aventures[.]com
- 2bd[.]net
- 3dbros[.]net
- abrisoal[.]com
- acm1petardox3232x[.]org
- aircapture[.]net
- barknbike[.]com
- callnrwise[.]com
- cheaprider[.]com
- cliffside[.]ventures
- darbyforcprd[.]com
- darbyforcprd[.]org
- euphoriacollective[.]net
- freedomain[.]one
- goledgergrid[.]com
- hungryhippotrash[.]net
- infrasky[.]net
- jay-ida[.]com
- jo3[.]org
- junkweasel[.]com
- layiokeimesi[.]work[.]gd
- leevik[.]net
- legalexceptional[.]com
- mailoutgoing[.]com
- make-hex-32332e3235342e3136372e323136-rr[.]1u[.]ms
- minishues[.]com
- nwfitwork[.]com
- nwfitwork[.]org
- nxivm[.]net
- pangpangxia[.]top
- pixelmonmmo[.]net
- pnbnursery[.]com
- realestatedatanetwork[.]net
- redatahub[.]net
- redatanet[.]net
- secondshop[.]store
- simsanta[.]net
- skurwysyn[.]net
- thejeffah[.]info
- tikitroys[.]com
- tvdhoenn[.]net
- urbanbio[.]org
- whachaneed[.]com
- wilderwoven[.]net
- wilderwoven[.]org
- xrnightblue[.]run[.]place

Sample String-Connected Domains

- 31ventures[.]co
- 31ventures[.]com
- 31ventures[.]io
- dnx[.]ae
- dnx[.]aero
- dnx[.]agency
- sfrclak[.]ph
- sfrclak[.]ws
- starbucls[.]autos
- starbucls[.]ca
- starbucls[.]co[.]uk
- work[.]ac

- work[.]ac[.]cn
- work[.]ac[.]nz