Going DNS Deep Diving into GhostCall and GhostHire

Table of Contents

Executive Report

BlueNorroff struck again last October, this time setting its sights on tech company execs, venture capitalists, and Web3 developers.

The actors zoomed in on tech company execs' and venture capitalists' macOS devices via GhostCall. They approached victims on Telegram and similar platforms, luring them with potential investments. Targets were invited to Zoom meetings, and once the call ensued, they were tricked into updating Zoom with a malicious script that downloaded a malicious ZIP file. As a result, the victims lost secret files, including crypto wallet information, keychain data, package managers, and infrastructure setups. They also lost details related to cloud and DevOps platforms, along with their notes, API keys for OpenAI, collaboration application data, and credentials stored in browsers, messengers, and Telegram.

In GhostHire, the attackers went after Web3 developers, tricking them into downloading and executing a GitHub repository containing malware disguised as a skill assessment test for recruitment. It did not matter what OS the targets used, the malware worked regardless. Like GhostCall, GhostHire stole sensitive information, including videos and profile images.

Securelist reported that GhostCall and GhostHire were interrelated in that they shared the same infrastructure and identified 39 domains as IoCs. After checking via the WhoisXML API MCP Server using the prompt "Check the domains using WHOIS API, Website Categorization API, and Threat Intelligence API to determine if any of them are legitimate," we found out that all of them were suspicious or downright malicious. As such, all of them figured in our analysis that led to these discoveries:

- 1,345 unique client IP addresses communicated with one of domains identified as IoCs
- Six domains identified as IoCs were bulk-registered with two look-alike domains each

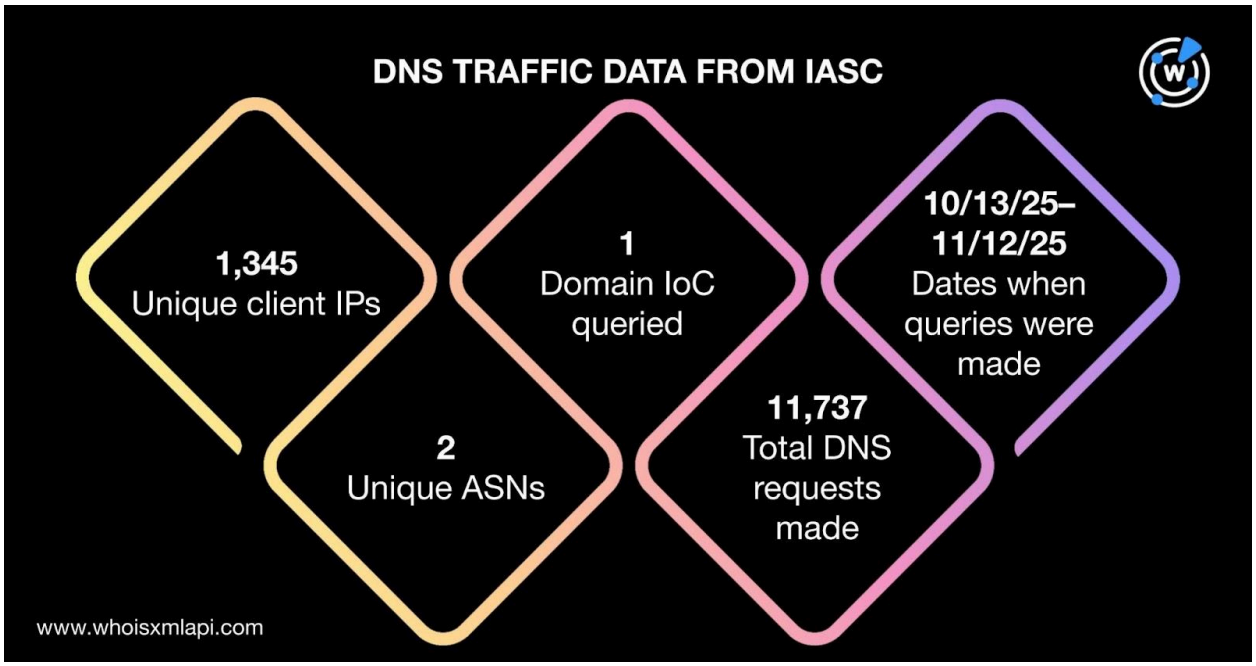
- 11 domains identified as IoCs were deemed likely to turn malicious 266–723 days before they were dubbed as such
- Four email-connected domains, three were found malicious
- 24 IP addresses, 21 were found malicious
- 16 IP-connected domains, six were found malicious
- 993 string-connected domains, 18 were found malicious

A Closer Look at the IoCs

We began our inquiry into GhostCall and GhostHire by looking more closely at the IoCs. We used both external and internal data to do that.

Data from the IASC

Sample network traffic data from the IASC showed that 1,345 unique client IP addresses under two distinct ASNs communicated with one of the domains identified as IoCs via 11,737 DNS requests made between 13 October and 12 November 2025.



Data from WhoisXML API

To gather more information, we queried the 39 domains identified as IoCs on First Watch Malicious Domains Data Feed and discovered that 11 of them were deemed likely to turn malicious 266–723 days before they were dubbed as such on 28 October 2025. Take a look at the details for five examples below.

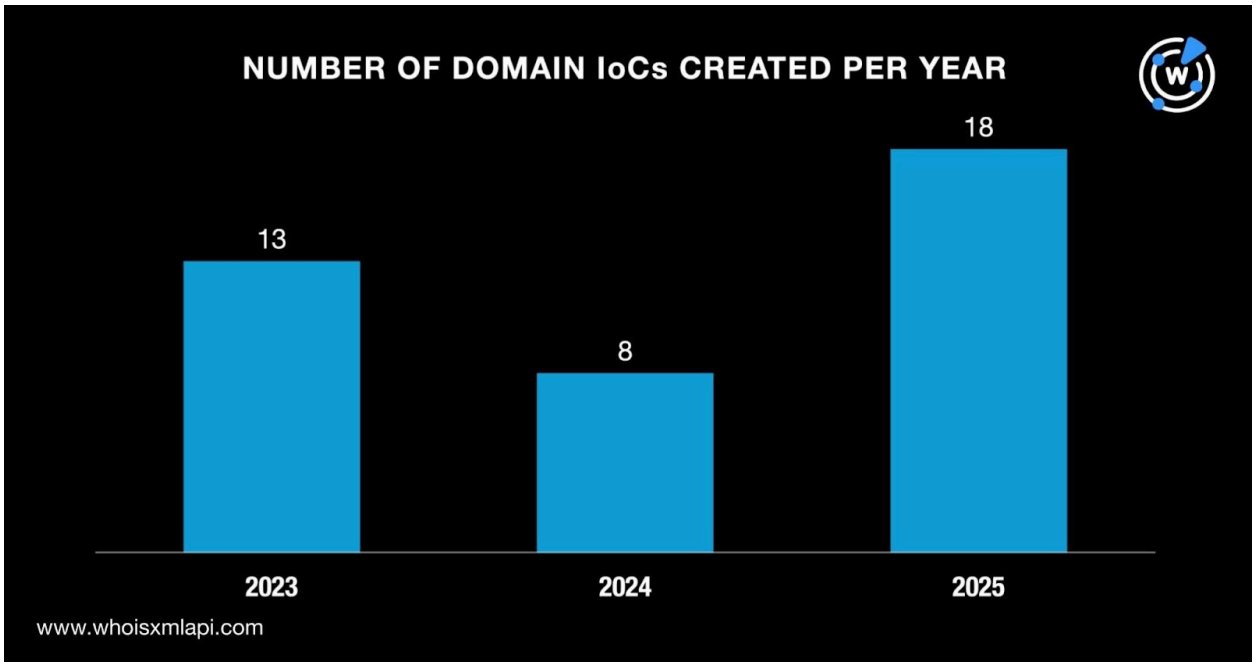
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS PRIOR TO 28 OCTOBER 2025
instant-update[.]online	3 November 2023	725
urgent-update[.]cloud	3 November 2023	725
autoupdate[.]online	5 November 2023	723
security-update[.]xyz	5 November 2023	723
systemupdate[.]cloud	5 November 2023	723

We also checked if any of the 39 domains identified as IoCs were bulk-registered with look-alikes via Typosquatting Data Feed and found out that six—system-update[.]xyz, systemupdate[.]cloud, autoupdate[.]online, autoupdate[.]xyz, flashstore[.]sbs, and ms-live[.]us—were part of five typosquatting groups with three domains each. Note that autoupdate[.]online and autoupdate[.]xyz were part of the same group. And they were registered between 22 October 2023 and 6 September 2025. Here are more details.

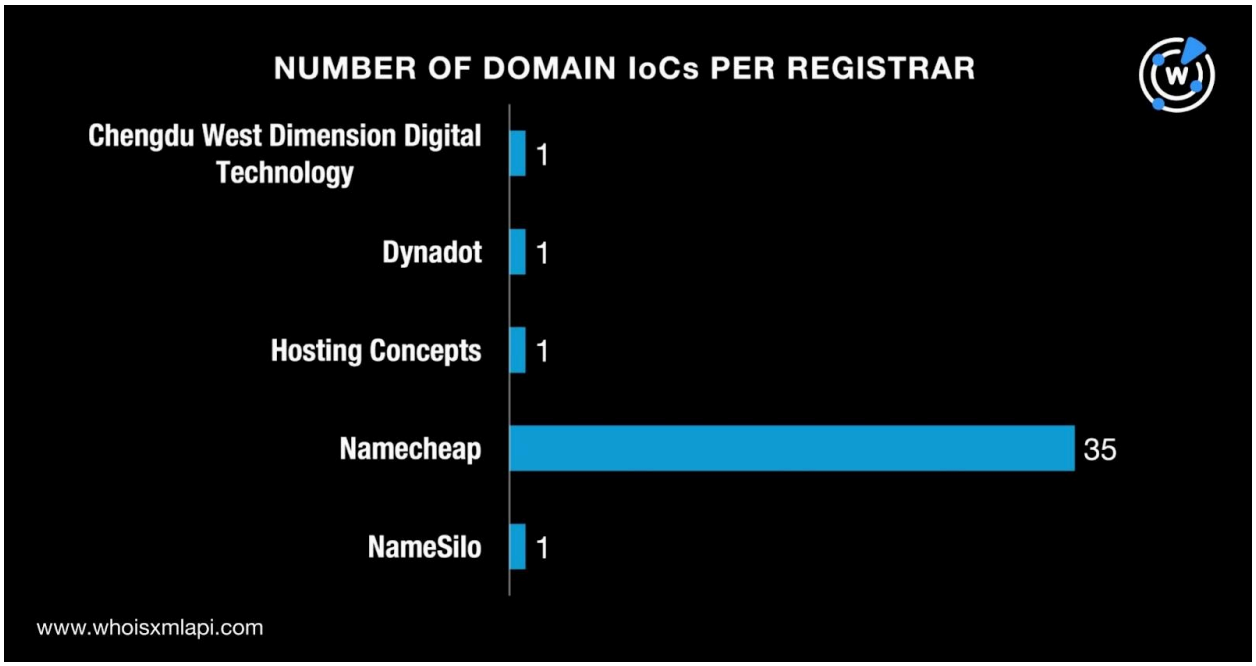
DOMAIN IoC	NUMBER OF LOOK-ALIKES	REGISTRATION DATE
system-update[.]xyz	2	22 October 2023
systemupdate[.]cloud	2	6 November 2023
autoupdate[.]online	2 (including another IoC autoupdate[.]xyz)	6 November 2023
autoupdate[.]xyz	2 (including another IoC autoupdate[.]online)	6 November 2023
flashstore[.]sbs	2	28 May 2025
ms-live[.]us	2	6 September 2025

Next, we queried the 39 domains identified as IoCs on WHOIS API and found out that only 28 had current WHOIS records. However, Domain Info API did allow us to fill in the details for the remaining 11 domains. The results showed that:

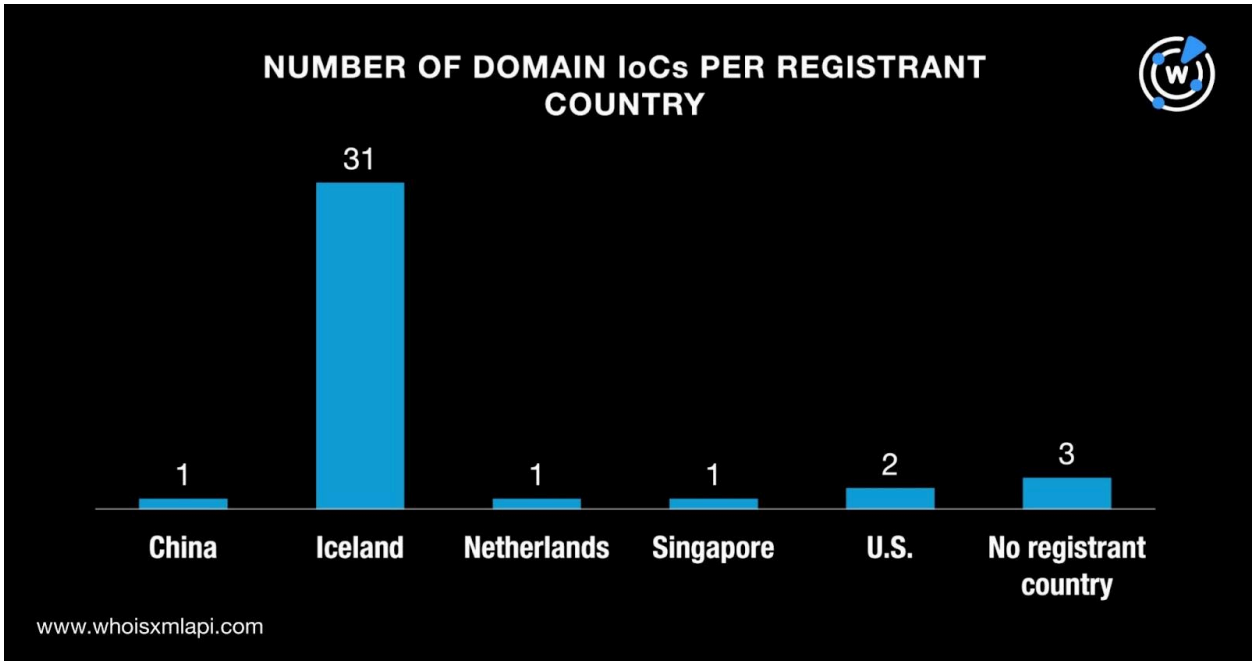
- They were created between 31 May 2023 and 19 October 2025. Specifically, 13 domains were created in 2023, eight in 2024, and 18 in 2025.



- They were administered by five registrars led by Namecheap, which accounted for 35 domains. One domain each fell under the purview of Chengdu West Dimension Digital Technology, Dynadot, Hosting Concepts, and NameSilo.



- While three of the domains did not have registrant countries on record, the remaining 36 were split among five countries. Thirty-one domains were registered in Iceland; two in the U.S.; and one each in China, the Netherlands, and Singapore.



A DNS Chronicle API query for the 39 domains identified as IoCs revealed that 36 had 1,034 historical domain-to-IP resolutions over time. The domain writeup[.]live posted the oldest resolution on 17 August 2018. Here are details for five examples.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
web071zoom[.]us	179	21 April 2025	30 October 2025
writeup[.]live	126	17 August 2018	29 October 2025
real-update[.]xyz	113	12 April 2019	13 July 2025
filedrive[.]online	108	20 October 2019	7 July 2023
secondshop[.]online	66	1 October 2020	29 October 20/25

The Hunt for New Artifacts

We began our search for new artifacts by querying the 39 domains identified as IoCs on WHOIS History API and discovered that 25 had email addresses in their historical WHOIS

records. In fact, they had 29 unique email addresses, four of which turned out to be public addresses.

While none of the four public email addresses were found in other domains' current WHOIS records based on the results of a Reverse WHOIS API query, they did show up on the historical WHOIS records of four email-connected domains after duplicates and those already tagged as IoCs were filtered out.

A Threat Intelligence API query for the four email-connected domains revealed that three were already considered malicious. An example would be sidezoom[.]us, which was used to distribute malware.

Next, we queried the 39 domains identified as IoCs on DNS Lookup API and discovered that 21 actively resolved to 24 unique IP addresses.

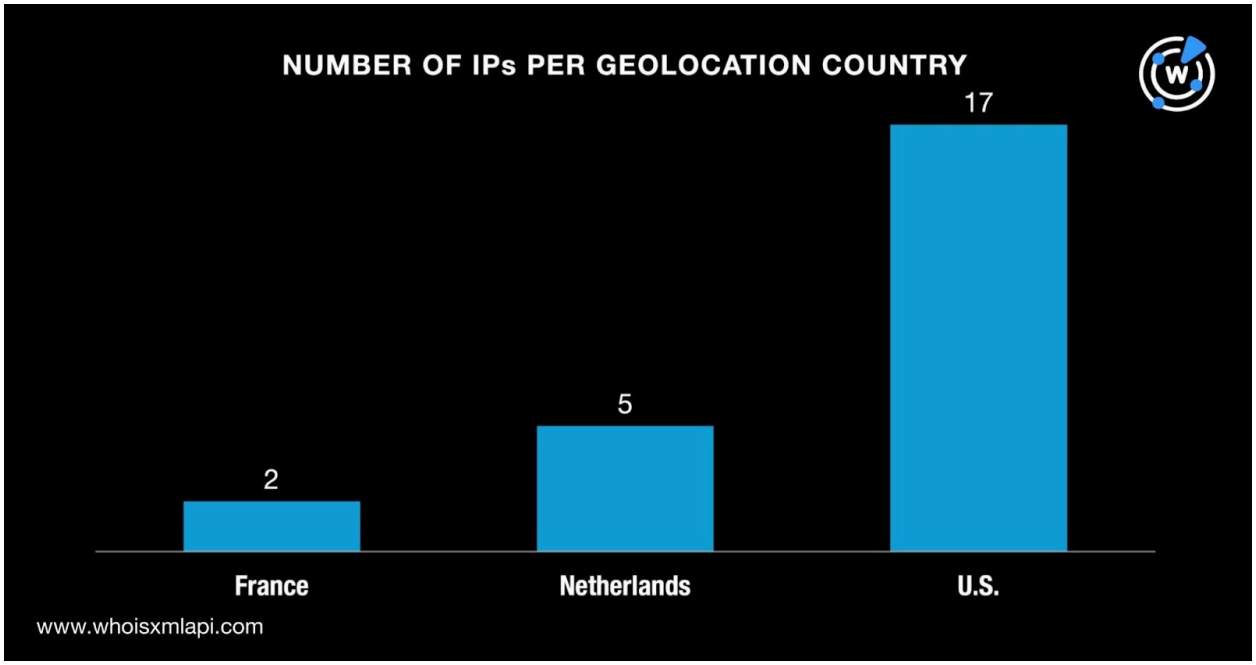
When queried on Threat Intelligence API, we found out that 21 of the IP addresses have already been weaponized for various attacks. Here are five examples.

IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
13[.]248[.]169[.]48	Malware distribution Phishing Suspicious activity Spamming Generic threat Command and control (C&C)	03/29/23–10/31/25 03/28/23–10/31/25 04/05/23–10/30/25 04/14/23–10/27/25 03/28/23–10/26/25 04/05/23–10/25/25
76[.]223[.]54[.]146	Malware distribution Phishing Suspicious activity Spamming Generic threat C&C	03/29/23–10/31/25 03/28/23–10/31/25 04/05/23–10/30/25 04/14/23–10/27/25 03/28/23–10/26/25 04/05/23–10/25/25
172[.]236[.]126[.]142	Malware distribution Phishing Generic threat Suspicious activity	10/16/25–10/31/25 10/15/25–10/31/25 10/16/25–10/30/25 10/16/25–10/24/25

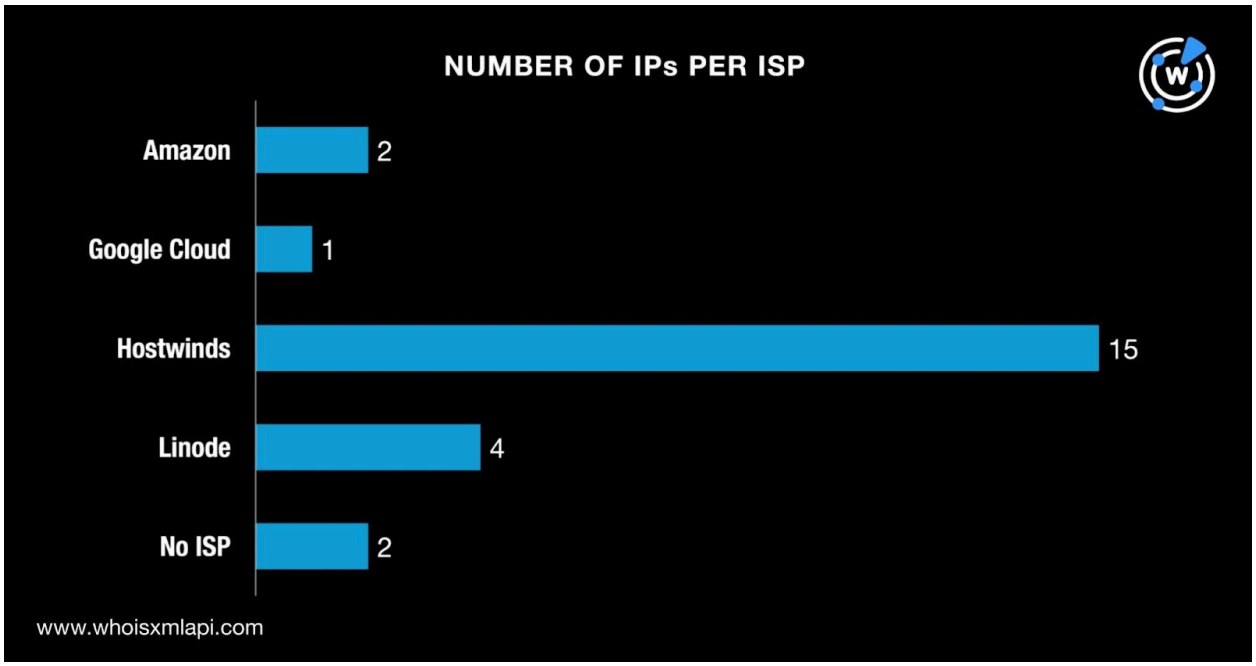
172[.]236[.]126[.]145	Phishing Malware distribution Generic threat Suspicious activity	10/15/25–10/31/25 10/16/25–10/31/25 10/16/25–10/30/25 10/16/25–10/24/25
172[.]236[.]126[.]225	Phishing Malware distribution Generic threat Suspicious activity	10/15/25–10/31/25 10/16/25–10/31/25 10/16/25–10/30/25 10/16/25–10/24/25

In a bid to gather more information about the 24 IP addresses, we queried them on Bulk IP Geolocation Lookup. The results showed that:

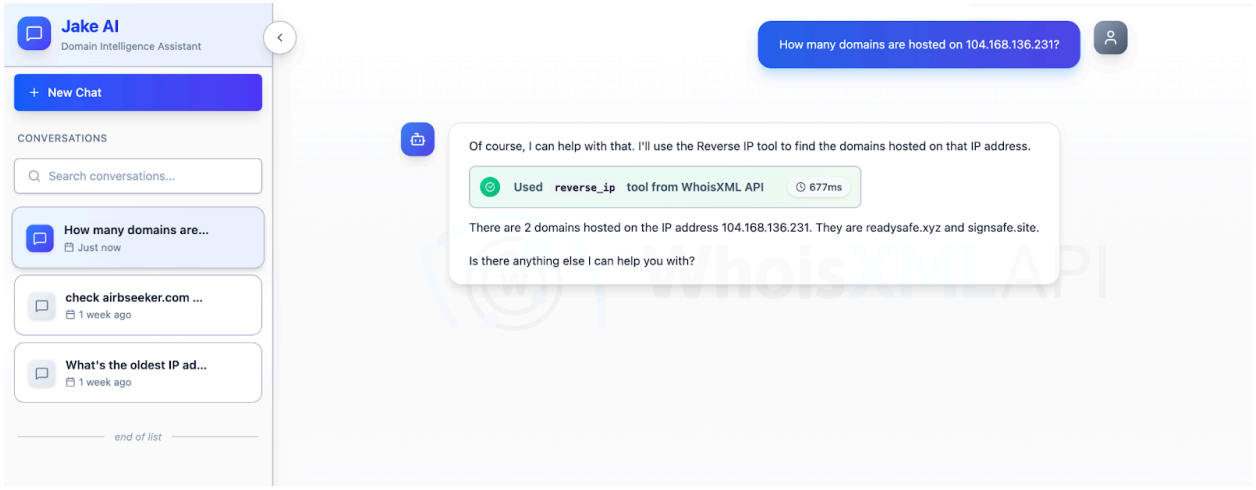
- They were split among three geolocation countries led by the U.S., which accounted for 17 IP addresses. And while five IP addresses originated from the Netherlands, two hailed from France.



- While two IP addresses did not have ISP data on record, the remaining 22 were distributed among four ISPs. Fifteen IP addresses were administered by Hostwinds, four by Linode, two by Amazon, and one by Google Cloud.



Next, we queried the 24 IP addresses on Jake AI to determine which could be dedicated hosts. We used the prompt “How many domains are hosted on 104.168.136.231?” for each IP address and discovered that 17 could be dedicated hosts.



Sample Jake AI query result

Upon closer examination, the 17 possibly dedicated IP addresses hosted 16 IP-connected domains after duplicates, those already tagged as IoCs, and the email-connected domains were filtered out.

A Threat Intelligence API query for the 16 IP-connected domains revealed that six have already figured in various attacks. Here are three examples.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
mylingocoin[.]com	Malware distribution	9 August–30 October 2025
newwebapi[.]us	Malware distribution	27 August–30 October 2025
upload-test[.]xyz	Malware distribution	20 June–30 October 2025

To complete our investigation, we scrutinized the 39 domains identified as IoCs and determined that they started with 34 unique text strings. We then used Domains & Subdomains Discovery to check if other domains began with them. We learned that 993 string-connected domains started with these 31 strings:

- alwayswait.
- autoupdate.
- awaitingfor.
- clearit.
- cloud-server.
- commoncome.
- datatabletemplate.
- dataupload.
- face-online.
- file-server.
- filedrive.
- firstfromsep.
- flashserve.
- flashstore.
- image-support.
- instant-update.
- ms-live.
- readysafe.
- real-update.
- safefor.
- safeup.
- safeupload.
- secondshop.
- security-update.
- signsafe.
- system-update.
- systemupdate.
- updatecheck.
- urgent-update.
- web071zoom.
- writeup.

We filtered out duplicates, those already tagged as IoCs, and the email- and IP-connected domains, of course.

A Threat Intelligence API query for the 993 string-connected domains revealed that 18 have already figured in various attacks. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
alwayswait[.]online	Malware distribution	09/12/23–10/29/25
autoupdate[.]com[.]ua	Malware distribution	05/04/24–10/30/25
commoncome[.]site	Malware distribution	01/05/24–10/29/25
file-server[.]co	Malware distribution	03/09/23–10/30/25
ms-live[.]link	Malware distribution	03/09/23–10/30/25

—

Our investigation of GhostCall and GhostHire allowed us to discern that 1,345 unique client IP addresses communicated with one of the domains identified as IoCs. We also found that 11 of the domain IoCs were deemed likely to turn malicious 266–723 days before they were dubbed as such.

Our analysis also led to the discovery of 1,037 new artifacts comprising four email-connected domains, 24 IP addresses, 16 IP-connected domains, and 993 string-connected domains. In addition, we learned that 48 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

- netbit[.]website
- sidezoom[.]us
- web001zoom[.]us

Sample IP Addresses

- 104[.]168[.]136[.]231
- 13[.]248[.]169[.]48
- 142[.]11[.]196[.]220
- 172[.]236[.]126[.]142
- 192[.]119[.]116[.]231
- 23[.]254[.]128[.]114
- 34[.]41[.]139[.]193
- 76[.]223[.]54[.]146
- 83[.]136[.]209[.]195

Sample IP-Connected Domains

- 866dcae7-a392-4525-87c2-752ed84a67b9[.]random[.]larfdsabh[.]pro
- c7410ec2-de31-45ab-befb-ae856538c767[.]random[.]23-254-164-50[.]plesk[.]page
- larfdsabh[.]pro
- mylingocoin[.]com
- netcreditloanusa[.]com
- sdk[.]w22zoom[.]us
- upload-test[.]xyz
- w22zoom[.]us

Sample String-Connected Domains

- alwayswait[.]com
- alwayswait[.]ing
- alwayswait[.]lat
- autoupdate[.]ai
- autoupdate[.]app
- autoupdate[.]au
- awaitingfor[.]com
- awaitingfor[.]ph
- clearit[.]academy
- clearit[.]ai
- clearit[.]app
- cloud-server[.]asia
- cloud-server[.]at
- cloud-server[.]audio
- commoncome[.]site
- datatabletemplate[.]ph
- datatabletemplate[.]ws
- dataupload[.]app
- dataupload[.]arab
- dataupload[.]cc
- face-online[.]co[.]uk
- face-online[.]com
- face-online[.]de
- file-server[.]biz
- file-server[.]cc
- file-server[.]cf
- filedrive[.]ai
- filedrive[.]app

- filedrive[.]biz
- firstfromsep[.]ph
- firstfromsep[.]store
- firstfromsep[.]ws
- flashserve[.]ai
- flashserve[.]ca
- flashserve[.]com
- flashstore[.]ae
- flashstore[.]asia
- flashstore[.]at
- image-support[.]com
- image-support[.]de
- image-support[.]ph
- instant-update[.]ca
- instant-update[.]cloud
- instant-update[.]com
- ms-live[.]ch
- ms-live[.]co
- ms-live[.]co[.]uk
- readysafe[.]app
- readysafe[.]au
- readysafe[.]ca
- real-update[.]com
- real-update[.]info
- safefor[.]art
- safefor[.]cf
- safefor[.]com
- safeup[.]ai
- safeup[.]app
- safeup[.]be
- safeupload[.]app
- safeupload[.]co
- safeupload[.]co[.]uk
- secondshop[.]ai
- secondshop[.]at
- secondshop[.]best
- security-update[.]app
- security-update[.]bid
- security-update[.]biz
- signsafe[.]ai
- signsafe[.]app
- signsafe[.]biz
- system-update[.]bond
- system-update[.]buzz
- system-update[.]center
- systemupdate[.]app
- systemupdate[.]bid
- systemupdate[.]biz
- updatecheck[.]at
- updatecheck[.]buzz
- updatecheck[.]cf
- urgent-update[.]club
- urgent-update[.]com
- urgent-update[.]info
- web071zoom[.]ph
- web071zoom[.]ws
- writeup[.]agency
- writeup[.]ai
- writeup[.]app