DNS Spotlight: New MITRE ATT&CK Group Entrants as of October 2025

Table of Contents

Executive Report

MITRE has named nine new groups responsible for attacks related to the most abused vulnerabilities from August to October 2025. They identified six Enterprise groups, two Mobile groups, and one ICS group.

We compiled 126 domains as IoCs for five groups—AppleJeus, Contagious Interview, Storm-0501, Water Galura, and Star Blizzard. However, upon further checking via the WhoisXML API MCP Server, only 108 of the domains identified as IoCs were deemed suspicious or outright malicious. Take a look at more details below.

GROUP	NUMBER OF ORIGINAL DOMAIN IoCs	NUMBER OF IoCs ANALYZED
AppleJeus	4	3
Contagious Interview	39	36
Storm-0501	13	7
Water Galura	1	1
Star Blizzard	69	61

We limited our investigation to these domains, along with the 31 IP addresses tagged as IoCs for four groups (UNC3886, Water Galura, MuddyWater, and the Lazarus Group) and five email addresses for the Medusa Group.

Our in-depth analysis led to these discoveries:

- 1,839 unique potential victim IP addresses communicated with four distinct IP addresses identified as IoCs
- Two domains tagged as IoCs were deemed likely to turn malicious 10 days before they were reported as such
- 78 email-connected domains, 11 were found malicious
- Eight additional IP addresses, seven were found malicious
- 196 IP-connected domains, five were found malicious
- 718 string-connected domains, 11 were found malicious

A Closer Look at the IoCs

We began our investigation by looking more closely at the 108 domains, 31 IP addresses, and five email addresses identified as IoCs. Here are more details on the number of IoCs per group.

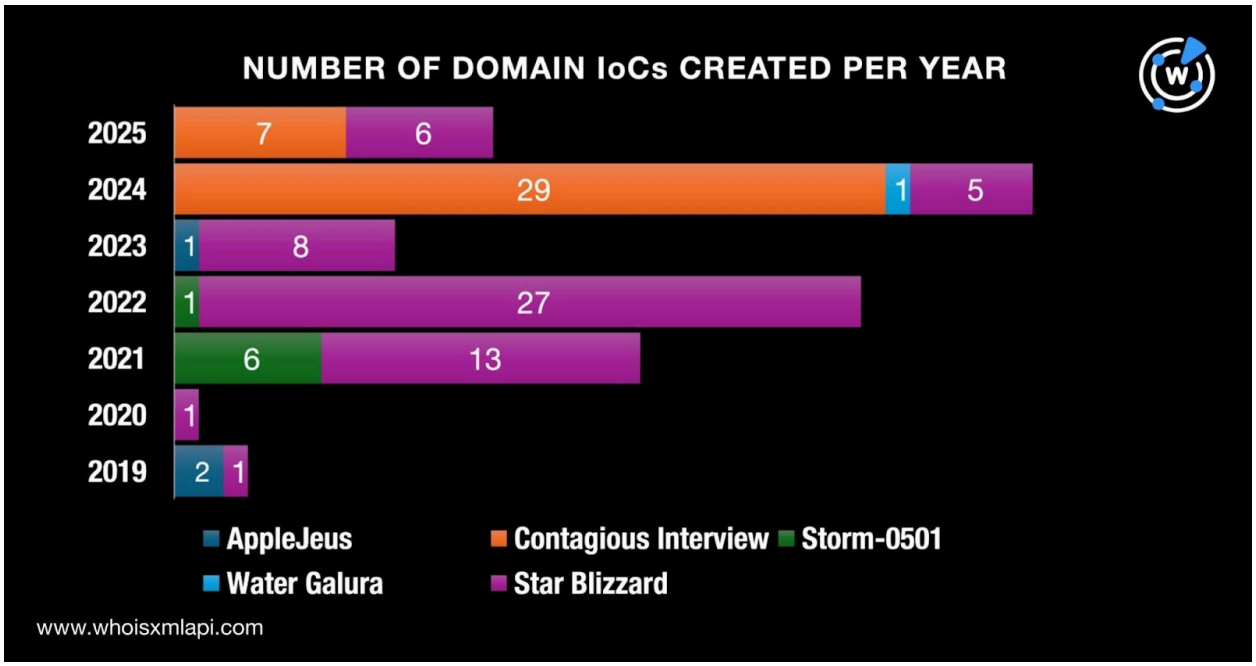
GROUP	NUMBER OF DOMAIN IoCs	NUMBER OF IP IoCs	NUMBER OF EMAIL IoCs
AppleJeus	3	0	0
Contagious Interview	36	0	0
Medusa Group	0	0	5
Storm-0501	7	0	0
UNC3886	0	8	0
Water Galura	1	5	0
MuddyWater	0	3	0
Star Blizzard	61	0	0
Lazarus Group	0	15	0
TOTAL	**108**	**31**	**5**

First, we consulted First Watch Malicious Domains Data Feed to determine if any of the 108 domains identified as IoCs were deemed likely to turn malicious upon registration. Two domains connected to Contagious Interview appeared on the feed 10 days before being dubbed as IoCs. Take a look at more details below.

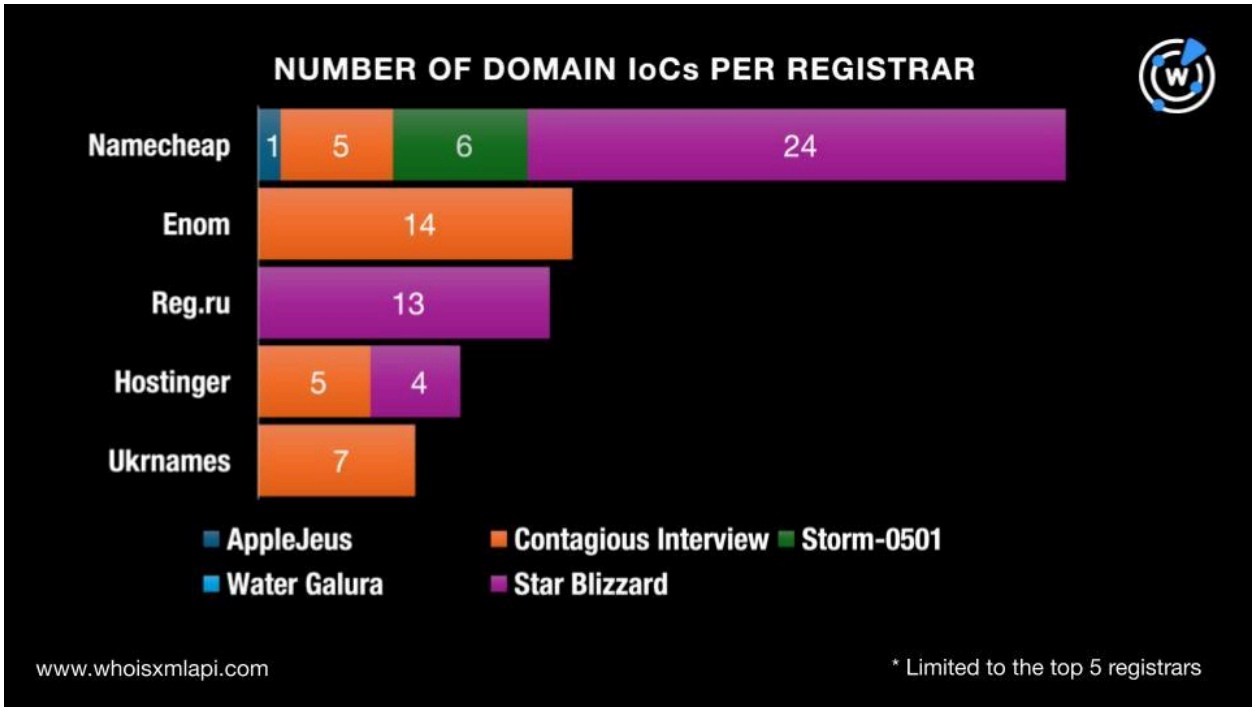
DOMAIN IoC	FIRST WATCH DATE	REPORTING DATE	NUMBER OF DAYS DEEMED MALICIOUS PRIOR TO REPORTING
complexassess[.]com	6 January 2025	16 January 2025	10
intro-crypto-assess[.]com	6 January 2025	16 January 2025	10

Next, we queried the 108 domains identified as IoCs on WHOIS API and Domain Info API and found out that:

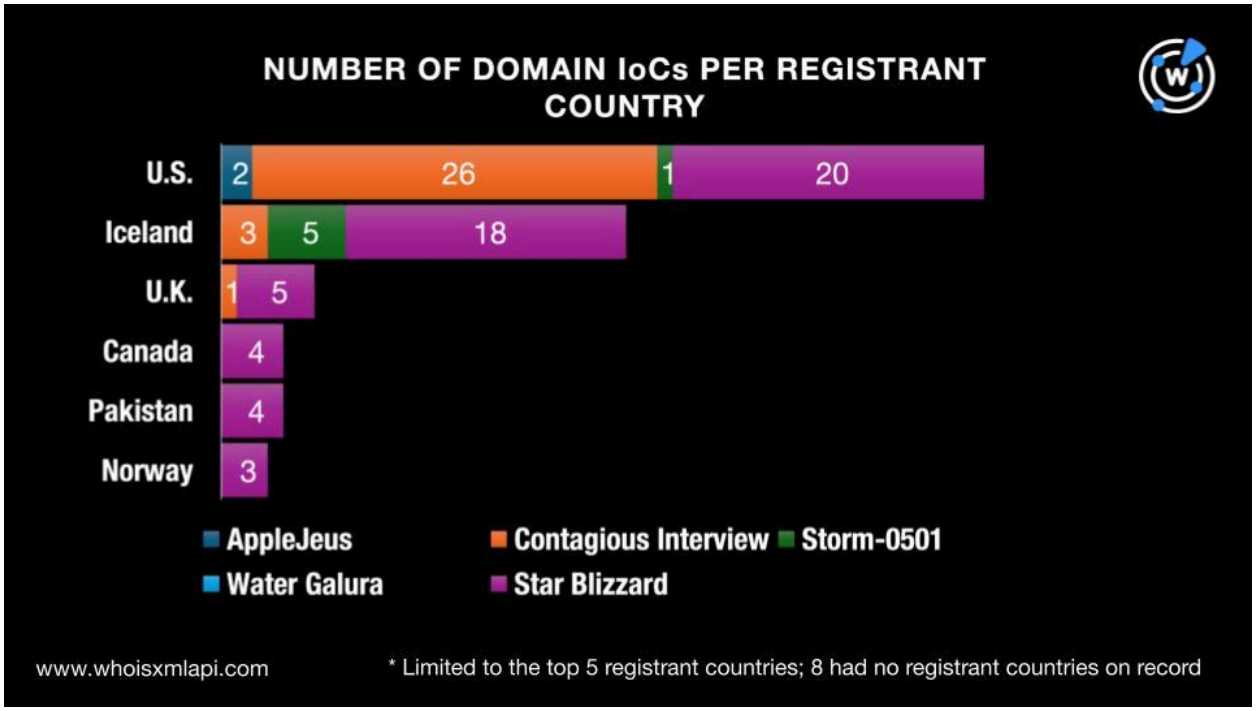
- They were created between 11 August 2019 and 6 November 2025. Specifically, 35 domains were created in 2024, 28 in 2022, 19 in 2021, 13 in 2025, nine in 2023, three in 2019, and one in 2020. Here is a domain volume breakdown by group.



- They were split among 23 registrars topped by Namecheap, which accounted for 36 domains. Enom took second place with 14 domains, followed by Reg.ru with 13. Take a look at the breakdown by group below.



- While eight domains did not have registrant countries on record, the remaining 100 were registered in 12 countries. The top 3 countries were the U.S. with 49 domains, Iceland with 26, and the U.K. with six. Here is a detailed breakdown per group.

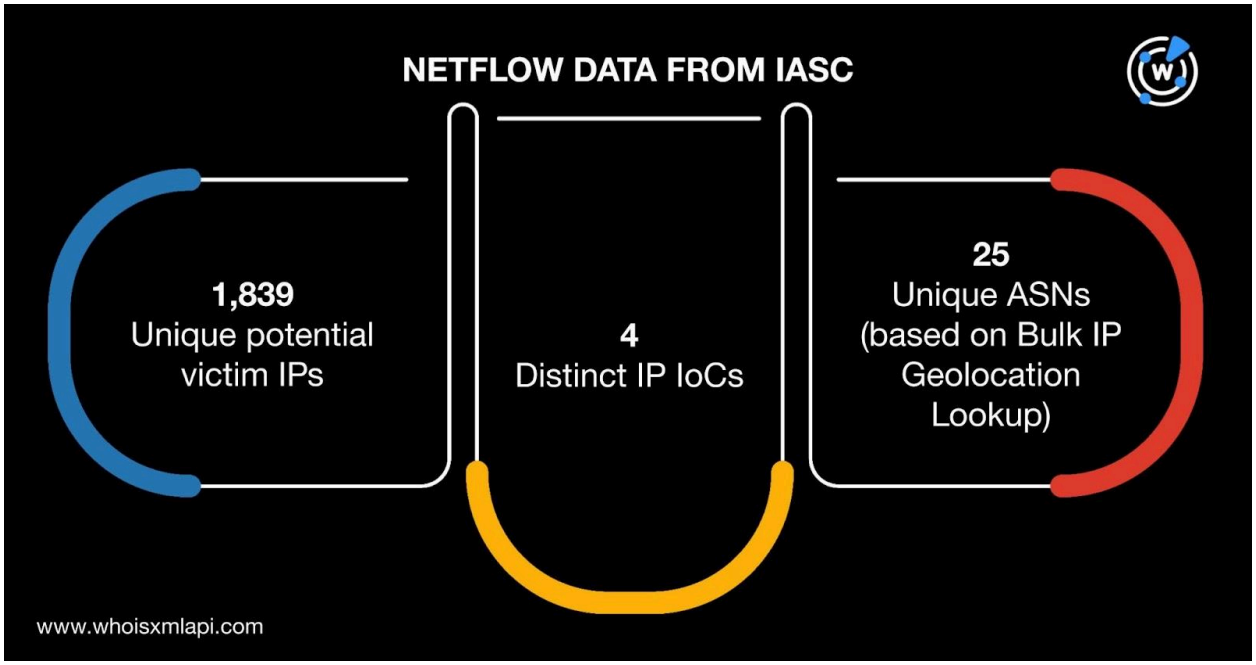


A DNS Chronicle API query for the 108 domains identified as IoCs showed that 97 had historical domain-to-IP resolutions. Together, they posted 2,022 resolutions over time starting on 5 February 2017 (i.e., recorded for Star Blizzard IoC cloud-docs[.]com). Take a look at more information for five examples below.

GROUP	DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
Star Blizzard	cloud-docs[.]com	299	02/05/17	10/09/25
Star Blizzard	doc-viewer[.]com	15	06/09/17	07/07/17
Star Blizzard	documents-cloud[.]com	57	07/07/17	04/03/23
Star Blizzard	cloud-storage[.]live	43	10 December 2017	05/14/24
Contagious Interview	vinterview[.]org	107	03/12/18	03/07/25

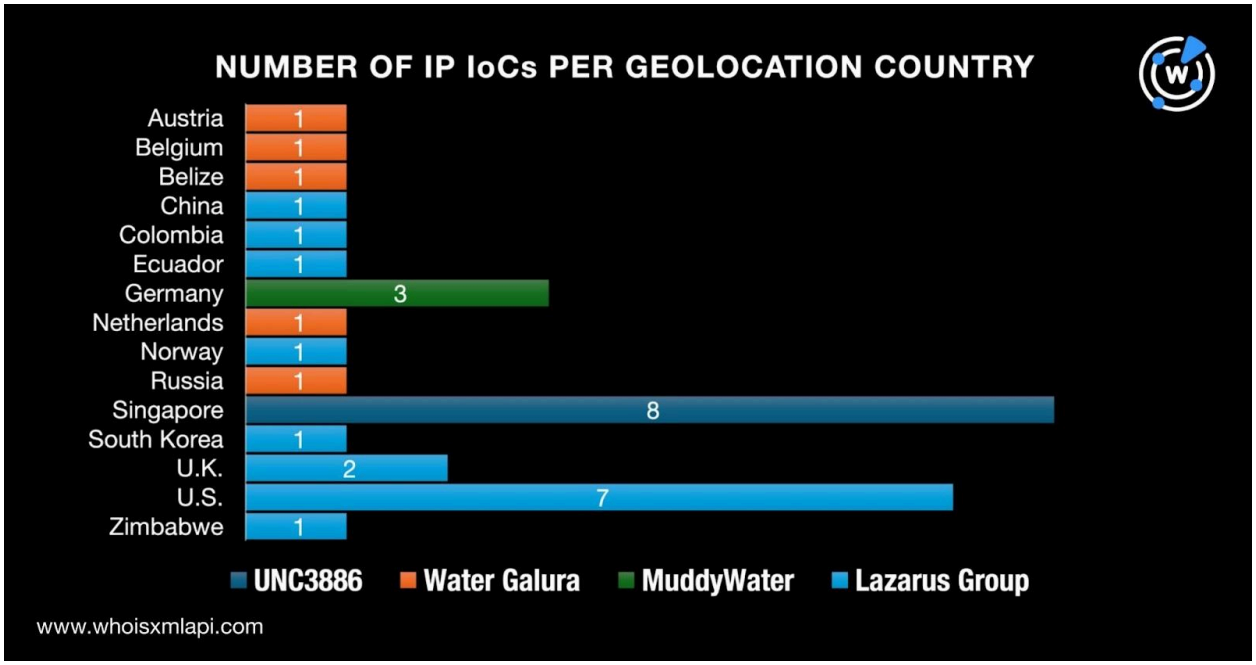
We then zoomed in on the 31 IP addresses identified as IoCs. Sample network traffic data from the IASC revealed that from 9 September to 13 November 2025, 1,839 unique potential victim IP addresses communicated with four of them.

The 1,839 IP addresses fell under 25 ASNs according to the results of a Bulk IP Geolocation Lookup query.

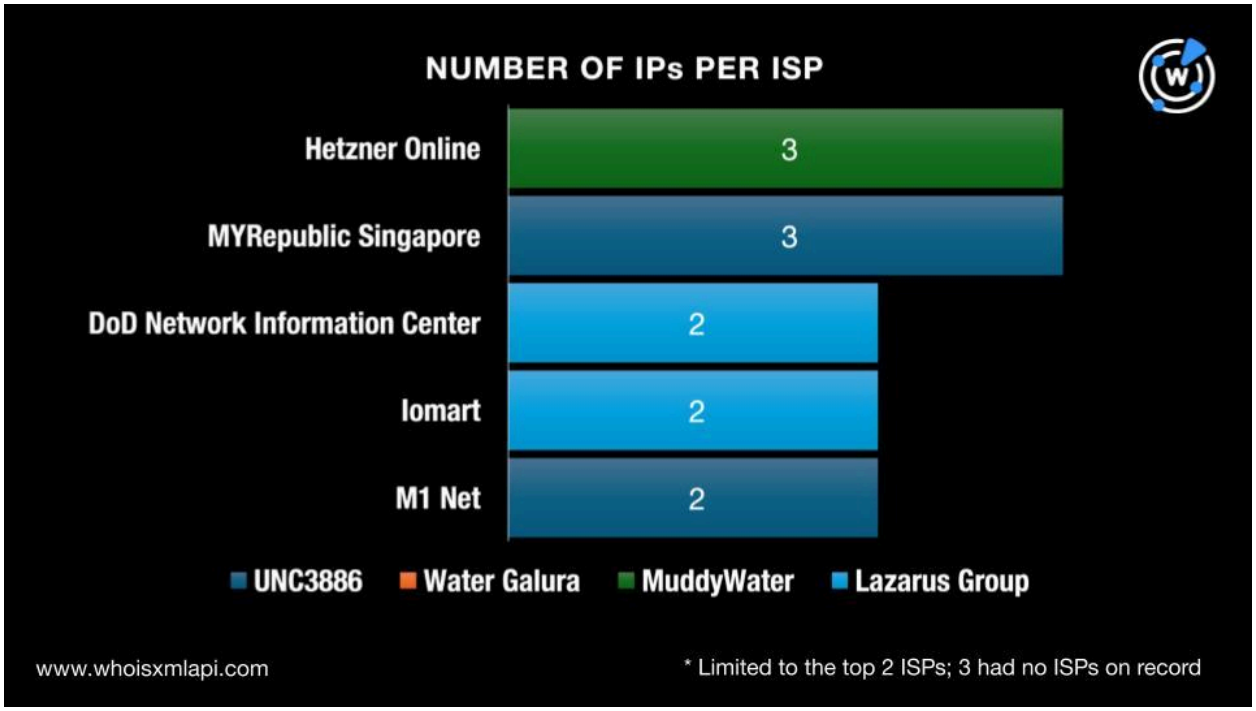


Next, we queried the 31 IP addresses identified as IoCs on Bulk IP Geolocation Lookup and found out that:

- They were scattered across 15 countries led by Singapore, which accounted for eight IP addresses. The U.S. came in second place with seven IP addresses. Germany completed the top 3 with three IP addresses. Take a look at a detailed breakdown by group below.



- While three IP addresses did not have ISPs on record, the remaining 28 were administered by 21 ISPs. The top ISPs were Hetzner Online and MYRepublic Singapore, which tied in first place, accounting for three IP addresses each. Here is a volume breakdown by group.



A DNS Chronicle API query for the 31 IP addresses identified as IoCs revealed that 19 had historical IP-to-domain resolutions. In sum, they recorded 5,451 resolutions starting on 4 February 2017. Take a look at five examples below.

GROUP	IP IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
Lazarus Group	84[.]49[.]242[.]125	259	02/04/17	08/11/24
MuddyWater	148[.]251[.]204[.]131	1,000	02/05/17	11/22/24
Lazarus Group	112[.]175[.]92[.]57	3,000	02/05/17	04/28/17
Lazarus Group	128[.]200[.]115[.]228	258	02/05/17	08/12/24
Lazarus Group	81[.]94[.]192[.]147	29	02/06/17	05/20/17

After that, we zoomed in on the five email addresses identified as IoCs. Jake AI checks using the prompt “What can you tell me about [email IoC]?”

Based on the information from the tools, here's what I can tell you about "key.medusa.serviceteam@protonmail.com":

Email Validity:

- The email address format is correct and it uses a valid domain, "protonmail.com".
- It's a free email service provided by ProtonMail.
- However, the system could not verify that this specific email address can receive mail. This could mean the address doesn't exist or isn't currently active.

Location and Provider:

- The email service is hosted by Proton AG in Frankfurt, Germany.

Domain Registrations:

- This email address has not been found in any WHOIS records, meaning it has not been used to register any domains.

In short, while the email address is from a known provider, it may not be an active email address. It has no history of being used to register any websites.

Sample Jake AI result for an email IoC search

The results showed that while all five email addresses were valid, none seem to be currently active nor were used to register any domains. Take a look at the specifics below.

EMAIL IoC	VALIDITY AND DETAILS	DOMAIN REGISTRATION USAGE
key[.]medusa[.]serviceteam@protonmail[.]com	Valid Free email Does not exist or inactive	Not used to register any domain
mds[.]svt[.]breach@protonmail[.]com	Valid Free email Does not exist or inactive	Not used to register any domain
mds[.]svt[.]mir2@protonmail[.]com	Valid Free email Does not exist or inactive	Not used to register any domain

medusa[.]support@onionmail[.]org	Valid Private email Does not exist or inactive	Not used to register any domain
MedusaSupport@cock[.]li	Valid Free and disposable email Does not exist or inactive	Not used to register any domain

Given the details above, from here on out, the five email addresses identified as IoCs will not figure in the rest of our analysis.

The Hunt for New Artifacts

After learning more about the IoCs, we sought to uncover new artifacts connected to the featured groups. We first queried the 108 domains identified as IoCs on WHOIS History API and discovered that 50 had email addresses in their historical WHOIS records. We found 191 unique email addresses in all.

Upon closer examination, we identified 18 public email addresses. We queried them on Reverse WHOIS API and found out that while none of them appeared in current WHOIS records, 11 did show up on historical WHOIS records. We were, in fact, able to gather 78 email-connected domains after duplicates and those already tagged as IoCs were filtered out.

Threat Intelligence API queries for the 78 email-connected domains revealed that 11 have already figured in various attacks. Here are five examples.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
bsc-dash[.]us	Malware distribution	07/23/25–11/07/25
callapp[.]us	Malware distribution	07/23/25–11/07/25
callservice[.]us	Malware distribution	02/05/25–11/07/25
infuy[.]us	Malware distribution	07/23/25–11/07/25
linkedinservice[.]us	Malware distribution	07/23/25–11/07/25

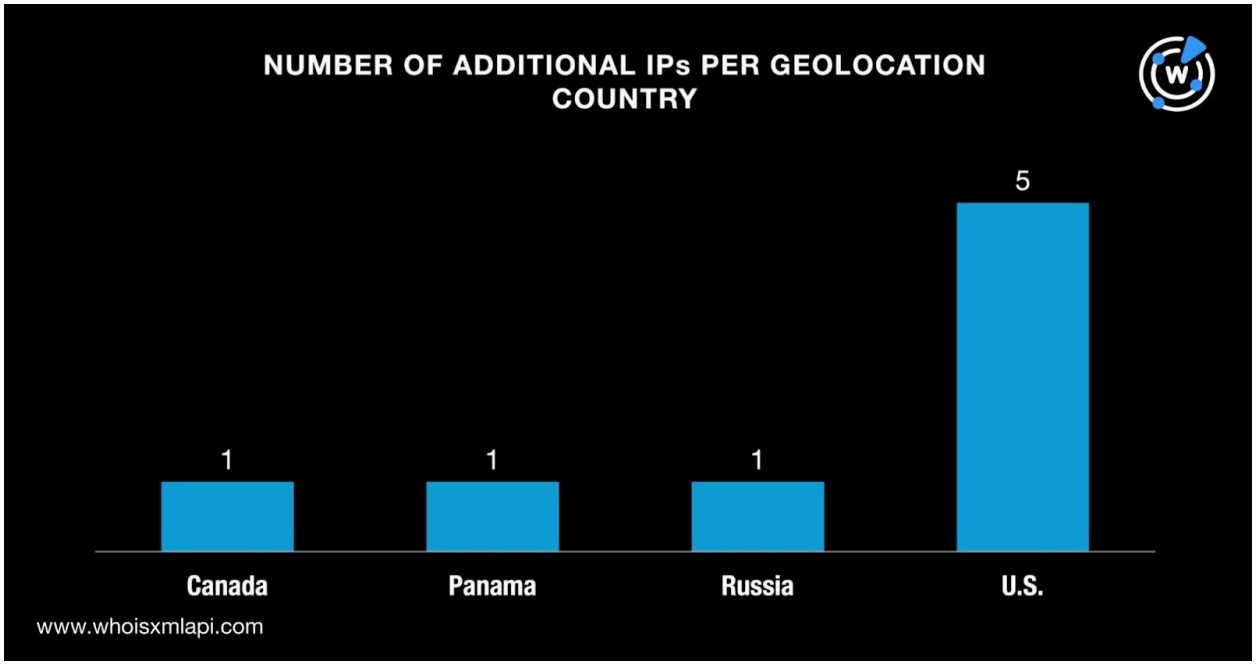
Next, we queried the 108 domains identified as IoCs on DNS Lookup API. We learned that 12 had active IP resolutions. Further scrutiny unveiled eight IP addresses after duplicates and those already tagged as IoCs were filtered out.

A Threat Intelligence API query for the eight additional IP addresses revealed that seven have already been weaponized for attacks. Take a look at three examples below.

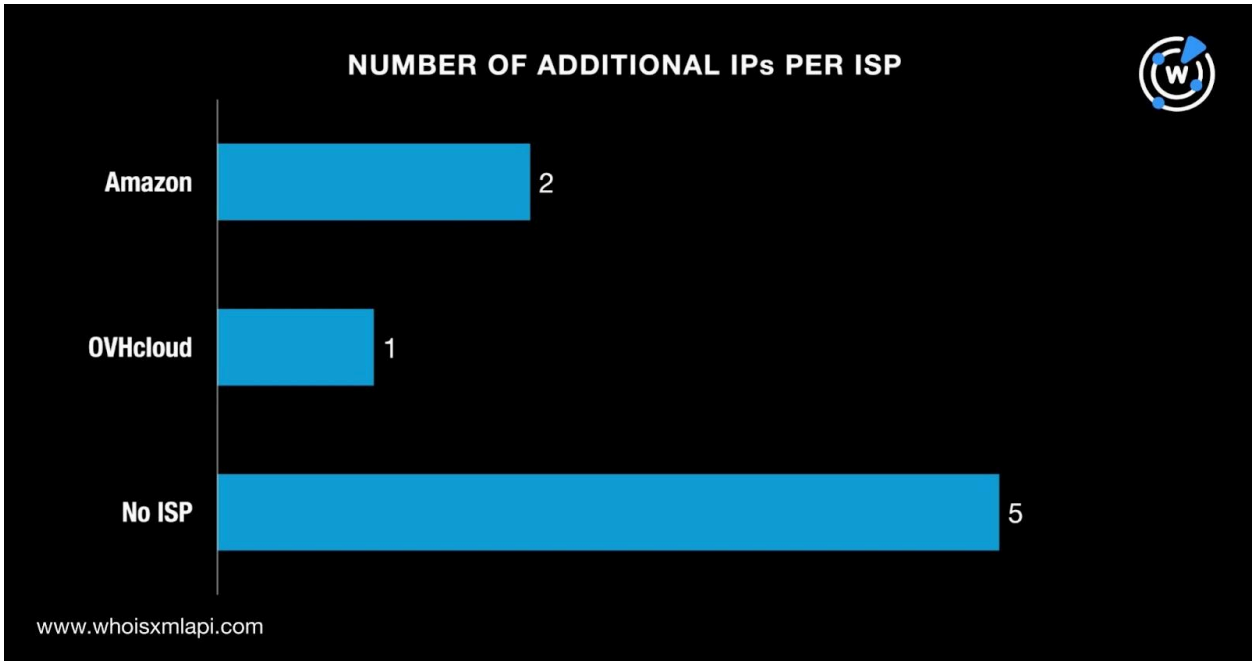
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
13[.]223[.]25[.]84	Phishing Malware distribution C&C Generic threat Spamming Suspicious activity	08/07/25–11/08/25 08/07/25–11/07/25 08/07/25–11/07/25 08/07/25–11/02/25 09/17/25–10/27/25 08/08/25–09/16/25
54[.]243[.]117[.]197	Phishing C&C Malware distribution Generic threat Spamming Suspicious activity	08/07/25–11/08/25 08/07/25–11/07/25 08/07/25–11/07/25 08/07/25–11/02/25 09/17/25–10/27/25 08/08/25–09/16/25
98[.]124[.]224[.]17	Malware distribution Phishing Generic threat	03/29/23–11/07/25 03/21/23–10/16/25 03/28/23–10/13/25

To know more about the eight additional IP addresses, we queried them on Bulk IP Geolocation Lookup and discovered that:

- They were split among four geolocation countries with the U.S. accounting for a majority, five IP addresses to be exact. Note that the U.S. was also the top geolocation country for the IP addresses identified as IoCs.



- While five of the IP addresses did not have ISPs on record, two were administered by Amazon and one by OVHcloud.



We now had 39 IP addresses in all—31 identified as IoCs and eight additional—for further analysis. Reverse IP API queries revealed that eight of them could be dedicated hosts. We

learned that together, they hosted 196 IP-connected domains after duplicates, those already tagged as IoCs, and the email-connected domains were filtered out.

Threat Intelligence API queries for the 196 IP-connected domains showed that five have already figured in various attacks. Here are three examples.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
digitpotalent[.]com	Malware distribution	11 January–8 November 2025
extrapowerpharma[.]com	Suspicious activity	5 April 2023–5 November 2025
helpdeskassistance[.]org	Malware distribution	11 January–8 November 2025

As the final step in our search for new artifacts, we extracted 99 unique text strings from the 108 domains identified as IoCs. Using Domains & Subdomains Discovery, we learned that 55 of the strings appeared at the start of other domains. Here are a few examples.

- globalkeystroke.
- hiringinterview.
- interviewnest.
- nvidia-release.
- videoscreening.
- willoassessment.
- markettc.
- screenconnect.
- cloud-docs.
- doc-viewer.
- goo-link.
- mail-docs.
- office-protection.
- pdf-cloud.
- safe-connection.
- webresources.
- y-ml.

Specifically, our searches for the 55 text strings led to the discovery of 718 string-connected domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

A Threat Intelligence API query for the 718 string-connected domains revealed that 11 have already figured in various attacks. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
cloud-storage[.]world	Malware distribution	08/30/24–11/08/25
docs-cache[.]online	Malware distribution	03/09/23–11/08/25
docs-view[.]cloud	Malware distribution	03/09/23–11/08/25
document-share[.]info	Malware distribution	03/09/23–11/08/25
documents-online[.]info	Malware distribution	12/29/24–11/08/25

—

Our in-depth investigation of the nine new groups listed on the MITRE ATT&CK October 2025 Updates page revealed that 1,839 unique potential victim IP addresses communicated with four distinct IP addresses identified as IoCs—109[.]70[.]100[.]1, 148[.]251[.]204[.]131, 186[.]2[.]163[.]10, and 45[.]77[.]39[.]28. We also learned that two domains tagged as IoCs—complexassess[.]com and intro-crypto-assess[.]com—were deemed likely to turn malicious 10 days before they were reported as such.

Our hunt for new artifacts unearthed 1,000 web properties comprising 78 email-connected domains, eight additional IP addresses, 196 IP-connected domains, and 718 string-connected domains. To date, 34 of them have already been weaponized for 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.*

References

We obtained IoC lists from the following reports cited on connected MITRE ATT&CK pages:

- Enterprise
  - AppleJeus
  - Contagious Interview
  - Medusa Group
  - Storm-0501
  - UNC3886
  - Water Galura
- Mobile
  - MuddyWater
  - Star Blizzard
- ICS
  - Lazarus Group

Appendix: Sample Artifacts

Sample Email-Connected Domains

- 1callclaims[.]info
- 1callclaims[.]org
- 4prendiendo[.]com
- ahmedelsayed[.]net
- al7lol[.]com
- anonymous-msg[.]com
- bsc-dash[.]us
- buzzingspot[.]com
- buzzinplace[.]com
- callapp[.]us
- callservice[.]us
- carnivaltriumphdamages[.]com
- dorger[.]net
- dorger[.]org
- dorgerlaw[.]com
- el7lol[.]com
- firstscanimaging[.]com
- firstscanimagingsolutions[.]com
- getbuzzingnow[.]com
- getbuzzinnow[.]com
- illphotography[.]com
- infuy[.]us
- injurycaseadvocates[.]com
- linkedinservice[.]us
- login-yahoo[.]info
- loweraldotnet[.]org
- mail-box[.]online
- mylawadvocates[.]com
- mypostfix[.]online
- nato-documents[.]com
- oash[.]co
- onbizcloud[.]com
- ondorgersoft[.]com
- postfix[.]online
- runningonthecloud[.]com
- safesecurityrgps[.]com
- seaside1113[.]com
- secure-smtp[.]online
- teiegram-support[.]com
- teiegram-verification[.]com
- telegram-alarm[.]com
- versus-dash[.]us
- versus-x[.]us
- versusx[.]us

Sample Additional IP Addresses

- 13[.]223[.]25[.]84
- 190[.]97[.]166[.]164
- 193[.]5[.]65[.]237

Sample IP-Connected Domains

- 47ot67so8b9nz2iu[.]abitibiexpress[.]ca
- 7change[.]net
- 8bdde2a7-b608-40f7-bb8e-9b0acf3cf89b[.]random[.]45-77-39-28[.]plesk[.]page
- abitibiexpress[.]ca
- account-center[.]com
- ai-transcendental[.]com
- bansllpao[.]com
- biohacker-pharma[.]com
- blockchain-suport[.]com

- canadianclubofchicago[.]org
- cardsavants[.]com
- ccleanappsmil[.]com
- d40abfa7-330c-434b-a658-b923be2d844d[.]random[.]abitibiexpress[.]ca
- darkpisces[.]com
- db[.]abitibiexpress[.]ca
- emdrklt[.]com
- extrapowerpharma[.]com
- fakeidfix[.]com
- fartlife[.]info
- fayqan[.]cfd
- gamersleak[.]com
- globalsecurty[.]com
- goblinfoot[.]com
- helpdeskassistance[.]org
- hhwemail[.]com
- hibiscus-trade[.]com
- inalfa[.]cfd
- infoactconstante[.]com
- insdriveupdates-360[.]com
- jobinterviewguide[.]org
- kraneaum[.]com
- l0g-inf[.]com
- lehmanengineer[.]com
- libidiol[.]com
- mail-verify[.]net
- mail[.]helpdeskassistance[.]org
- maksimus[.]net
- nateosante[.]cam
- naturalbiolab[.]net
- news-center[.]net
- ohiofireinstaller[.]com
- peptidekoning[.]nl
- prometheandynamics[.]net
- r-wb[.]icu
- recovery-system[.]net
- redleafgroup[.]ca
- saunamaailm[.]cc
- sempermailme[.]com
- service-portals[.]com
- telega-messenger[.]ru
- theoldgrovefarmstead[.]ph
- thepesttechnicians[.]com
- update-aussuper[.]com
- uspaydayloansff[.]com
- uwaoma[.]cc
- valentine2019[.]strangled[.]net
- we12[.]buzz
- web-login-drive[.]com
- webdisk[.]alcoclub[.]net
- xxfllter[.]com
- yunmbacufe[.]com

Sample String-Connected Domains

- cloud-docs[.]ca
- cloud-docs[.]ch
- cloud-docs[.]cloud
- cloud-mail[.]app
- cloud-mail[.]be
- cloud-mail[.]best
- cloud-storage[.]app
- cloud-storage[.]asia
- cloud-storage[.]at
- doc-viewer[.]website
- doc-viewer[.]zip
- docs-cache[.]online
- docs-drive[.]com
- docs-drive[.]fr
- docs-drive[.]gives
- docs-forwarding[.]com
- docs-forwarding[.]ws
- docs-info[.]org
- docs-info[.]tk
- docs-view[.]be

- docs-view[.]biz
- docs-view[.]cloud
- document-online[.]co[.]uk
- document-online[.]com
- document-online[.]fr
- document-share[.]cloud
- document-share[.]com
- document-share[.]info
- document-view[.]com
- document-view[.]online
- document-view[.]ph
- documents-cloud[.]xyz
- documents-online[.]co[.]uk
- documents-online[.]com
- documents-online[.]de
- documents-pdf[.]com
- documents-preview[.]net
- documents-preview[.]ph
- documents-preview[.]tk
- documents-view[.]com
- documents-view[.]site
- drive-docs[.]cloud
- drive-docs[.]info
- drive-docs[.]online
- drive-share[.]blog
- drive-share[.]click
- drive-share[.]co[.]uk
- globalkeystroke[.]ph
- globalkeystroke[.]ws
- goo-link[.]com
- goo-link[.]ru
- hiringinterview[.]com
- hiringtalent[.]be
- hiringtalent[.]ch
- hiringtalent[.]co
- interviewnest[.]ai
- interviewnest[.]com
- interviewnest[.]in
- mail-docs[.]com
- mail-docs[.]ml
- mail-docs[.]org
- markettc[.]com
- nvidia-release[.]cloud
- nvidia-release[.]ph
- nvidia-release[.]ws
- office-protection[.]com
- office-protection[.]fr
- office-protection[.]info
- office365-online[.]ch
- office365-online[.]cloud
- office365-online[.]co[.]uk
- officeonline365[.]com
- officeonline365[.]com[.]br
- officeonline365[.]de
- online-document[.]cf
- online-document[.]cloud
- online-document[.]com
- online-storage[.]at
- online-storage[.]biz
- online-storage[.]ch
- online365-office[.]live
- onlinecloud365[.]com
- pdf-cloud[.]biz
- pdf-cloud[.]cf
- pdf-cloud[.]co
- pdf-docs[.]click
- pdf-docs[.]com
- pdf-docs[.]fr
- pdf-shared[.]com
- pdf-shared[.]gq
- protect-link[.]biz
- protect-link[.]cc
- protect-link[.]co
- protection-link[.]com
- protection-link[.]com[.]do
- protection-link[.]fr
- protection-office[.]com
- protection-office[.]ph
- protectionmail[.]com
- protectionmail[.]org

- protectionmail[.]services
- proton-docs[.]online
- proton-docs[.]ru
- proton-viewer[.]ws
- safe-connection[.]co[.]uk
- safe-connection[.]com
- safe-connection[.]de
- screenconnect[.]ai
- screenconnect[.]app
- screenconnect[.]arab
- secureoffice[.]app
- secureoffice[.]au
- secureoffice[.]biz
- videoscreening[.]co[.]uk
- videoscreening[.]com
- videoscreening[.]dk
- vinterview[.]ai
- vinterview[.]ca
- vinterview[.]cn
- webresources[.]best
- webresources[.]biz
- webresources[.]blog
- willoassessment[.]co[.]uk
- willointerview[.]app
- willointerview[.]co[.]uk
- willointerview[.]info
- willotalent[.]app
- willotalent[.]art
- willotalent[.]cam
- willotalents[.]com
- wtalents[.]agency
- wtalents[.]co[.]uk
- wtalents[.]com
- y-ml[.]cn
- y-ml[.]com
- y-ml[.]info