An In-Depth Analysis of the Ashen Lepus AshTag-Enabled Attack

Table of Contents

Executive Report

Palo Alto Networks' Unit 42 tracked and monitored the most recent Ashen Lepus aka WIRTE APT campaign that leveraged a new malware suite they have dubbed "AshTag." The group conducted espionage activities against Arabic-speaking government entities. This time, however, the researchers witnessed a tangible evolution in the group's operational security and TTPs. The actors specifically enhanced their custom payload encryption, infrastructure obfuscation by using legitimate subdomains, and in-memory malware execution to minimize forensic artifacts.

That said, were we able to uncover more potentially connected artifacts using the 12 subdomains Unit 42 has identified as IoCs.

We extracted 10 unique domains from the 12 subdomains identified as IoCs, bringing our total number of IoCs to analyze to 22. Our in-depth analysis of the AshTag IoCs led to these discoveries:

- 12 subdomains identified as IoCs tagged as malware distributors
- 430 unique client IP addresses that communicated with one of the domains identified as IoCs
- Two domains identified as IoCs deemed likely to turn malicious upon registration 75–752 days before being dubbed as such
- 29 email-connected domains
- One IP address, which turned out to be malicious
- 50 string-connected domains

A Closer Look at the Subdomains Identified as AshTag IoCs

Queries for the 12 subdomains identified as IoCs on Jake AI showed that all of them have been flagged for malware distribution between 13 and 16 December 2025. While 11 of them could not be categorized, one—auth[.]onlinefieldtech[.]com—fell under several categories, including Technology & Computing, Internet, and Business & Finance, along with an unrelated category Style & Fashion.

Domain Information:

- As we saw with the previous query, the parent domain, "onlinefieldtech.com," was registered on April 14, 2025, and the owner's information is private.
- The subdomain "auth.onlinefieldtech.com" resolves to the IP address 164.90.235.245, which is also hosted on DigitalOcean.

Security Analysis:

- **Threat Intelligence:** Just like "apiv2.onlinefieldtech.com," this subdomain, "auth.onlinefieldtech.com," has also been flagged for **malware**. The malicious activity was first seen on December 13, 2025, and last observed on December 16, 2025.
- **Categorization:** This subdomain has been categorized under several topics, including "Technology & Computing," "Internet," and "Business and Finance," but also unrelated categories like "Style & Fashion." This broad and inconsistent categorization can be a red flag, often seen with sites that have been compromised or are used for multiple malicious purposes.

Conclusion:

The fact that another subdomain from "onlinefieldtech.com" has also been recently associated with malware is a very strong indicator that this entire domain is likely malicious. The pattern of behavior across multiple subdomains increases the certainty of this assessment.

I strongly advise you to avoid "auth.onlinefieldtech.com" and any other part of the "onlinefieldtech.com" domain. It is highly probable that it is being used for phishing, malware distribution, or other harmful activities.

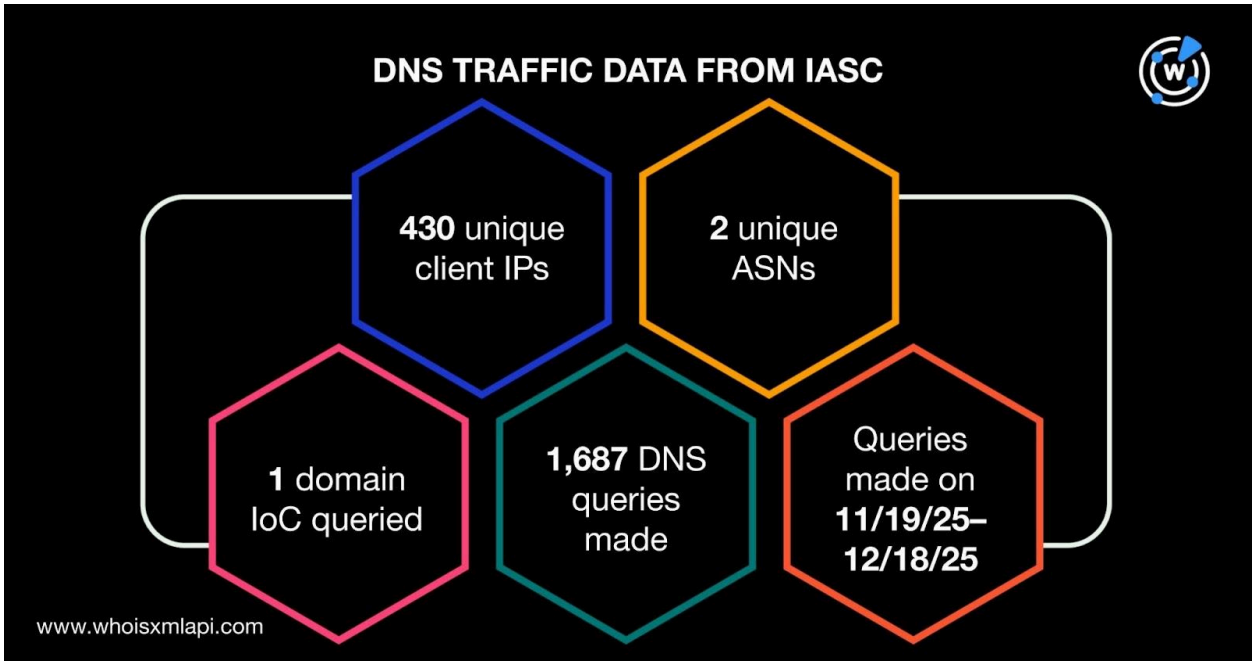
Sample Jake AI result for the subdomain auth[.]onlinefieldtech[.]com

Further Analysis of the 10 Domains Identified as AshTag IoCs

We began our investigation by querying the 10 domains identified as IoCs on the WhoisXML API MCP Server, which revealed that none of them were owned by legitimate entities.

Sample IASC network traffic data for the 10 domains identified as IoCs showed that 430 unique client IP addresses under two distinct ASNs communicated with the domain IoC

api[.]softmatictech[.]com via 1,687 DNS queries between 19 November and 18 December 2025.

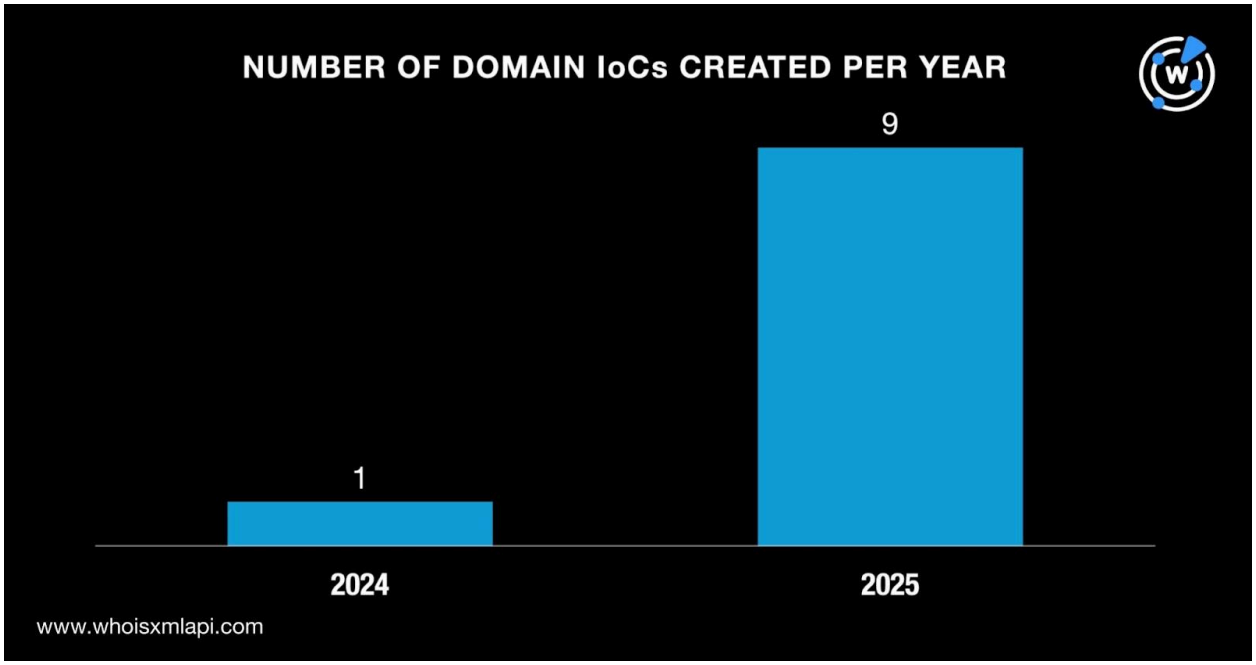


In addition, the results of our First Watch Malicious Domains Data Feed queries showed that two domains identified as IoCs were deemed likely to turn malicious 75–752 days before being dubbed as such on 11 December 2025.

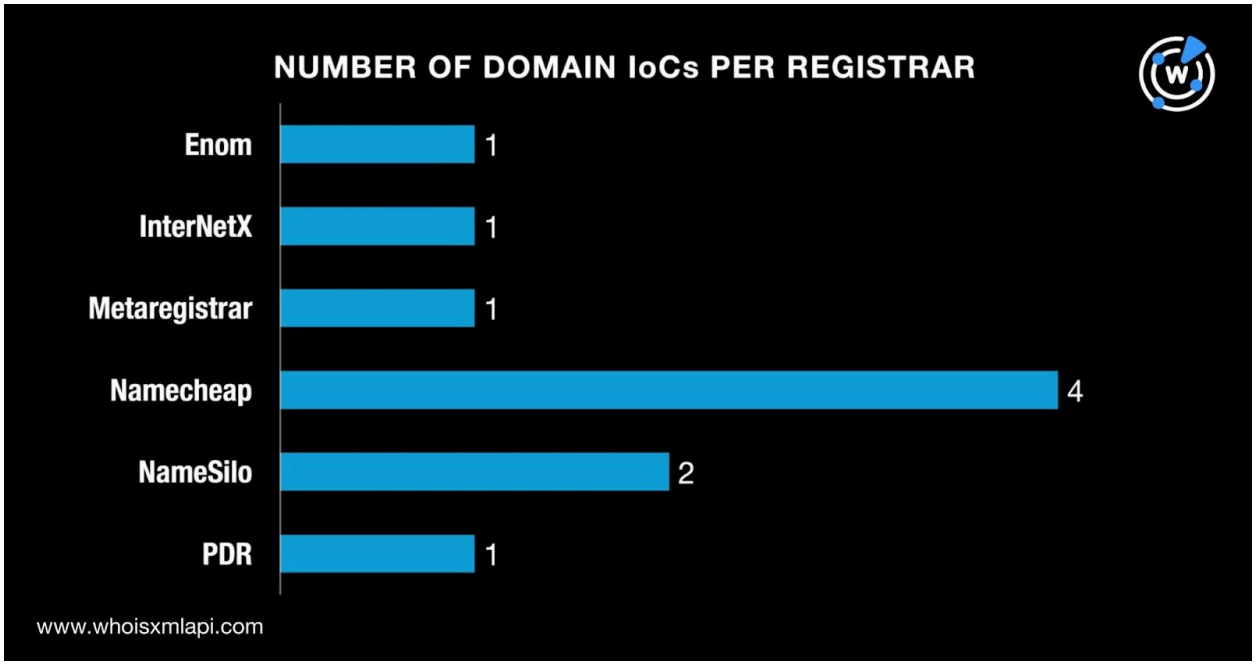
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE REPORT DATE
healthylifefeed[.]com	20 November 2023	752
systemsync[.]info	27 September 2025	75

We then queried the 10 domains identified as IoCs on WHOIS API and discovered that:

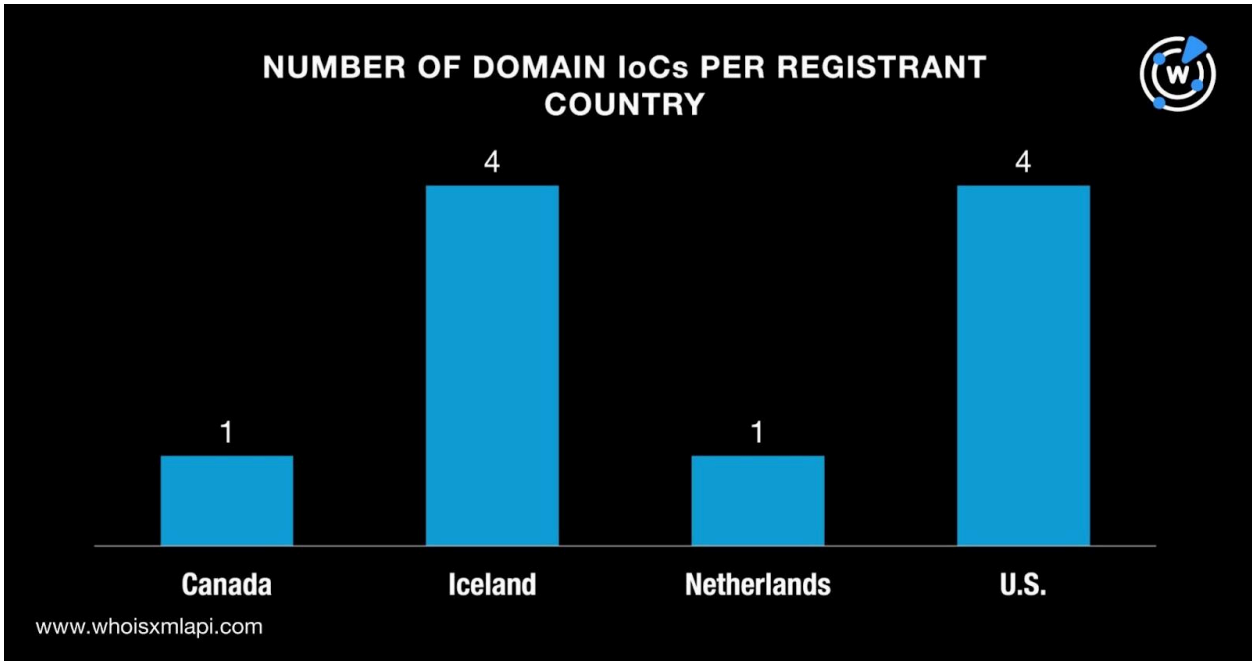
- Nine of them were created in 2025 while one was created in 2024.



- Namecheap was the top registrar, accounting for four of the domains. NameSilo accounted for two domains while Enom, InterNetX, Metaregistrar, and PDR administered one domain each.



- Finally, four domains each were registered in Iceland and the U.S. while one each was registered in Canada and the Netherlands.



A DNS Chronicle API query for the 10 domains identified as IoCs, meanwhile, showed that they recorded 1,425 domain-to-IP resolutions over time. The domain technology-system[.]com posted the oldest resolution on 7 February 2017.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
technology-system[.]com	77	02/07/17	08/30/25
healthylifefeed[.]com	225	04/28/17	11/04/17
techtg[.]com	294	04/29/17	05/30/25
widetechno[.]info	556	04/29/17	08/14/25
techupinfo[.]com	95	07/09/18	08/30/24

Next, we began our search for new artifacts by querying the 10 domains identified as IoCs on WHOIS History API and found out that six of them had email addresses in their historical WHOIS records. We uncovered 36 unique email addresses in all. Upon further scrutiny, we determined that nine were public email addresses.

According to the results of our Reverse WHOIS API queries for the nine public email addresses, none of them were present in any other domain's current WHOIS records. All of them, meanwhile, appeared in the historical WHOIS records of 29 unique email-connected domains after those already identified as IoCs were filtered out.

Next, we queried the 10 domains identified as IoCs on DNS Lookup API, which showed that only one—techupinfo[.]com—actively resolved to a single IP address.

A Threat Intelligence API query for the sole IP address revealed that it has already been flagged for various threats—phishing, malware distribution, generic threat, C&C, and suspicious activity.

An IP Geolocation API query for the lone IP address, meanwhile, showed that it was geolocated in the U.S. and administered by Amazon.

Next, we queried the sole IP address on Reverse IP API. We discovered that it was not a dedicated IP address hence, our hunt for IP-connected domains ended.

After that, we extracted 10 unique text strings from the 10 domains identified as IoCs. Based on the results of our Domains & Subdomains Discovery searches, all 10 strings appeared at the start of 50 unique string-connected domains after those already tagged as IoCs and the email- and IP-connected domains were filtered out. They were:

- healthylifefeed.
- medicinefinders.
- onlinefieldtech.
- softmatictech.
- systemsync.
- technoforts.
- technology-system.
- techtg.
- techupinfo.
- widetechno.

—

Our in-depth analysis of the 22 AshTag IoCs revealed that 430 unique client IP addresses under two distinct ASNs communicated with one domain identified as an IoC via 1,687 DNS queries made between 19 November and 18 December 2025. In addition, we discovered that two domains identified as IoCs were deemed likely to turn malicious 75–752 days before they were dubbed as such on 11 December 2025.

On top of all that, we uncovered 80 new artifacts comprising 29 email-connected domains, one IP address, and 50 string-connected domains. One of these additional artifacts has also 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

- 2ccalzature[.]com
- casabella-imbiancature[.]com
- cbaswiss[.]com
- cega-sas[.]com
- dailyinsider[.]us
- dcdasiapac[.]com
- dcgtasia[.]com
- falegnameriapozzoni[.]com
- kaptaanpeshawarichappals[.]com
- liamprofessional[.]com
- medtasia[.]com
- newsletterconservativefighters[.]com
- nutrinewsmag[.]com
- pacstrholdings[.]com
- psholdings[.]com
- rawws[.]com
- rayyanstraders[.]com
- riparazionicasatreviglio[.]com
- tygast[.]com
- waseemwears[.]com
- widetechno[.]net
- zakirtrading[.]jp

Sample String-Connected Domains

- healthylifefeed[.]club
- healthylifefeed[.]online
- healthylifefeed[.]ph
- medicinefinders[.]ph
- medicinefinders[.]se
- medicinefinders[.]us
- onlinefieldtech[.]ws
- systemsync[.]ai
- systemsync[.]cf
- systemsync[.]cloud
- technoforts[.]xyz
- technology-system[.]co
- technology-system[.]de
- technology-system[.]eu
- techtg[.]cn
- techtg[.]co[.]uk
- techtg[.]eu
- techupinfo[.]com[.]br
- techupinfo[.]ph
- techupinfo[.]ws
- widetechno[.]com
- widetechno[.]online
- widetechno[.]ph