Deep Dive: 3 Lazarus RATs Caught in Our DNS Trap

Table of Contents

Executive Report

Fox-IT and the NCC Group have conducted multiple incident response cases involving a Lazarus subgroup specifically targeting organizations in the financial and cryptocurrency sectors. The subgroup has been linked to AppleJeus, Citrine Sleet, UNC47363, and Gleaming Pisces and uses different remote access Trojans (RATs) known as "PondRAT5," "ThemeForestRAT," and "RemotePE."

The researchers analyzed the three RATs in great depth in "Three Lazarus RATs Coming for Your Cheese." They also identified 19 domains and two IP addresses as indicators of compromise (IoCs) in the process.

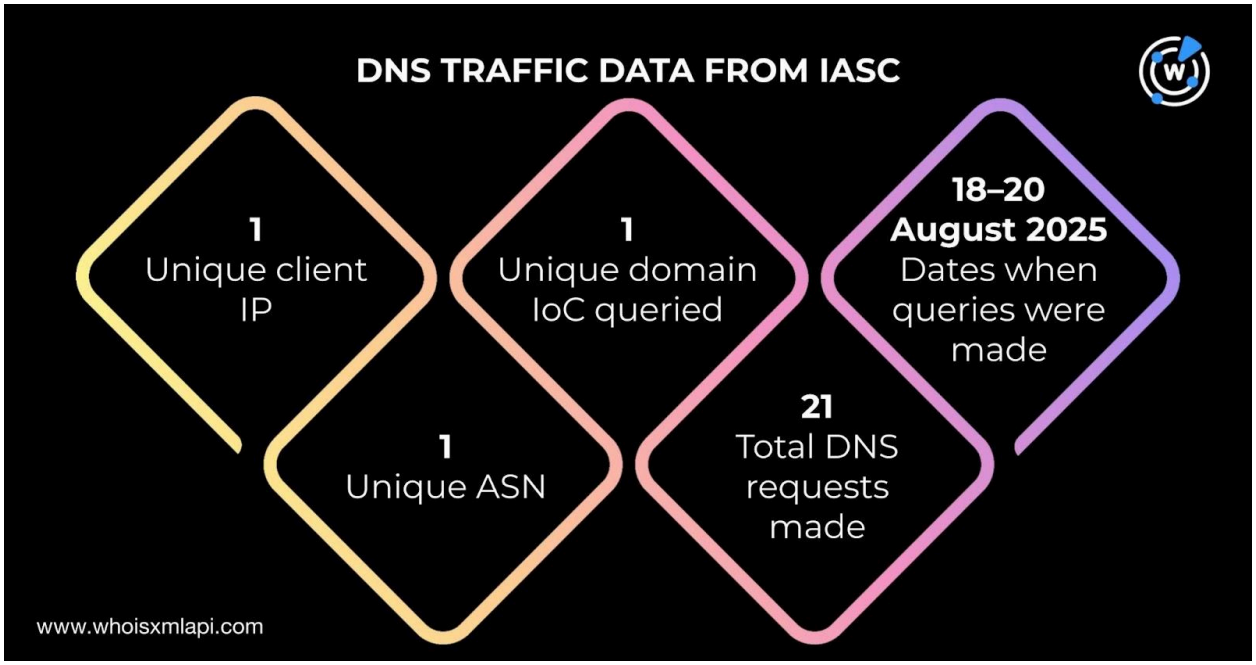
WhoisXML API dug deeper into the three RATs' DNS infrastructure, which led to these discoveries:

- One unique client IP address communicated with one distinct domain IoC based on sample traffic data from the Internet Abuse Signal Collective (IASC)
- Two unique alleged victim IP addresses communicated with two distinct IP IoCs according to sample IASC traffic data
- One of the domain IoCs was dubbed likely to turn malicious 189 days before being tagged as such
- One email-connected domain
- Nine additional IP addresses, eight were malicious
- 57 IP-connected domains
- 259 string-connected domains

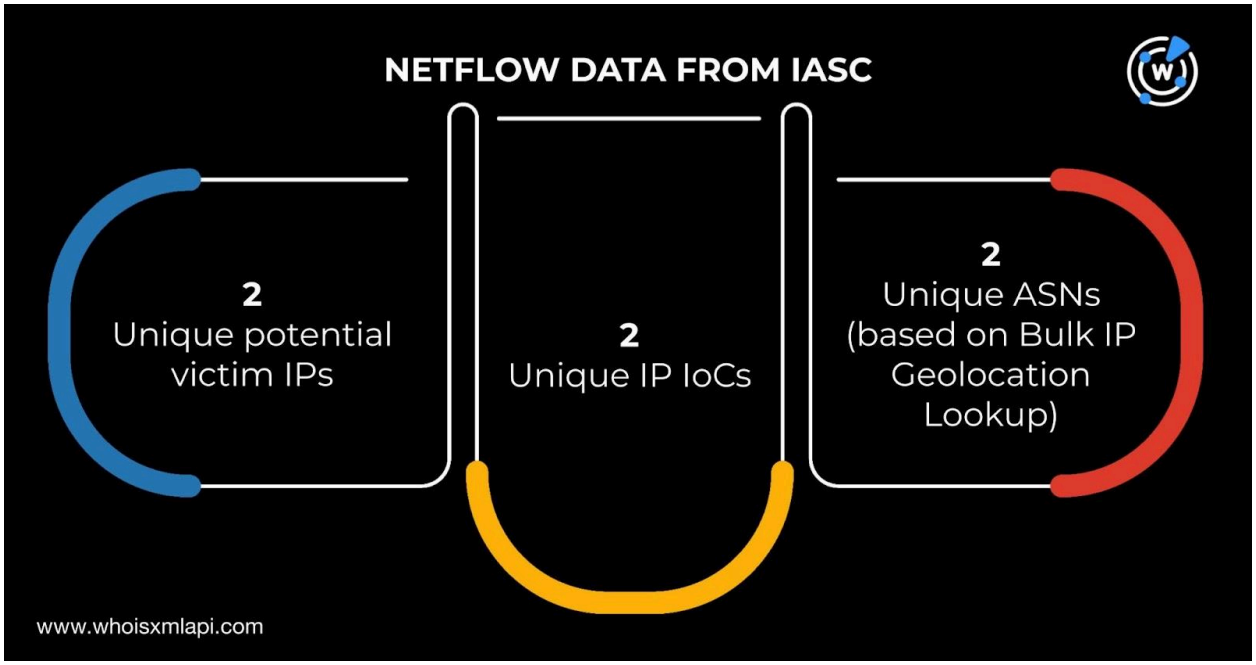
More Insights into the IoCs

Facts about the IASC Data

Sample network traffic data from IASC showed that one unique client IP address under one distinct Autonomous System number (ASN) queried one unique domain IoC via 21 DNS queries between 18 and 20 August 2025.



Sample network traffic IASC data also revealed that two unique alleged victim IP addresses communicated with two distinct IP IoCs under two unique ASNs based on the results of a Bulk IP Geolocation Lookup query.

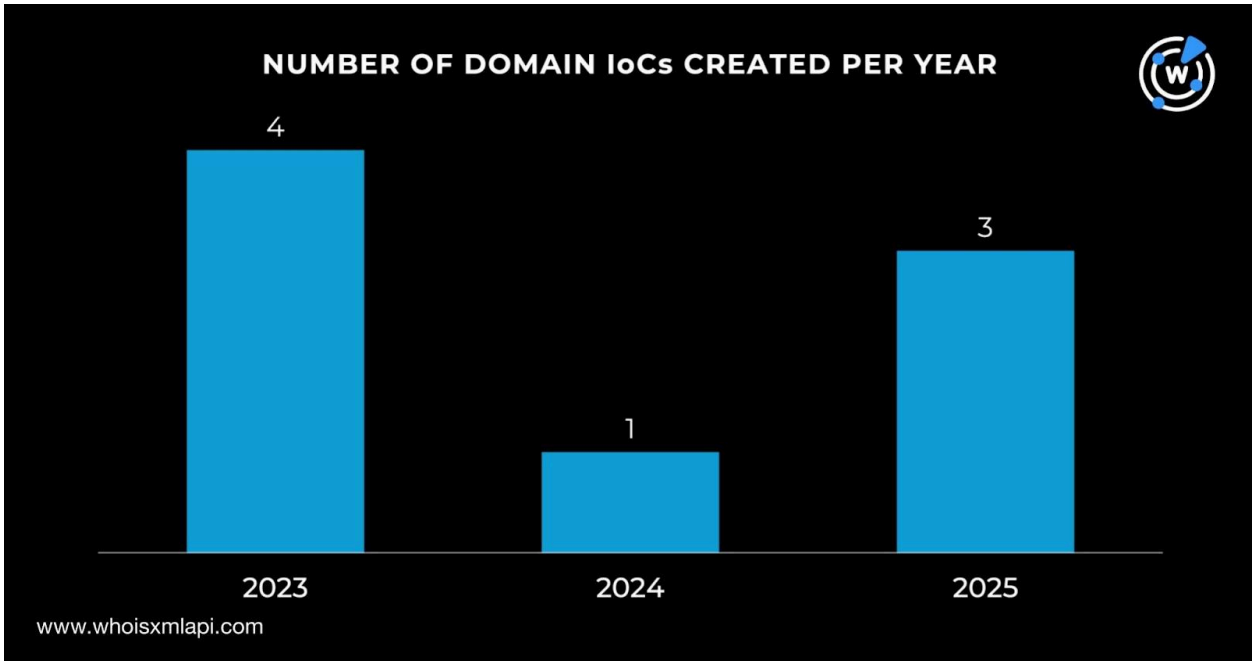


More Information from Our Tools

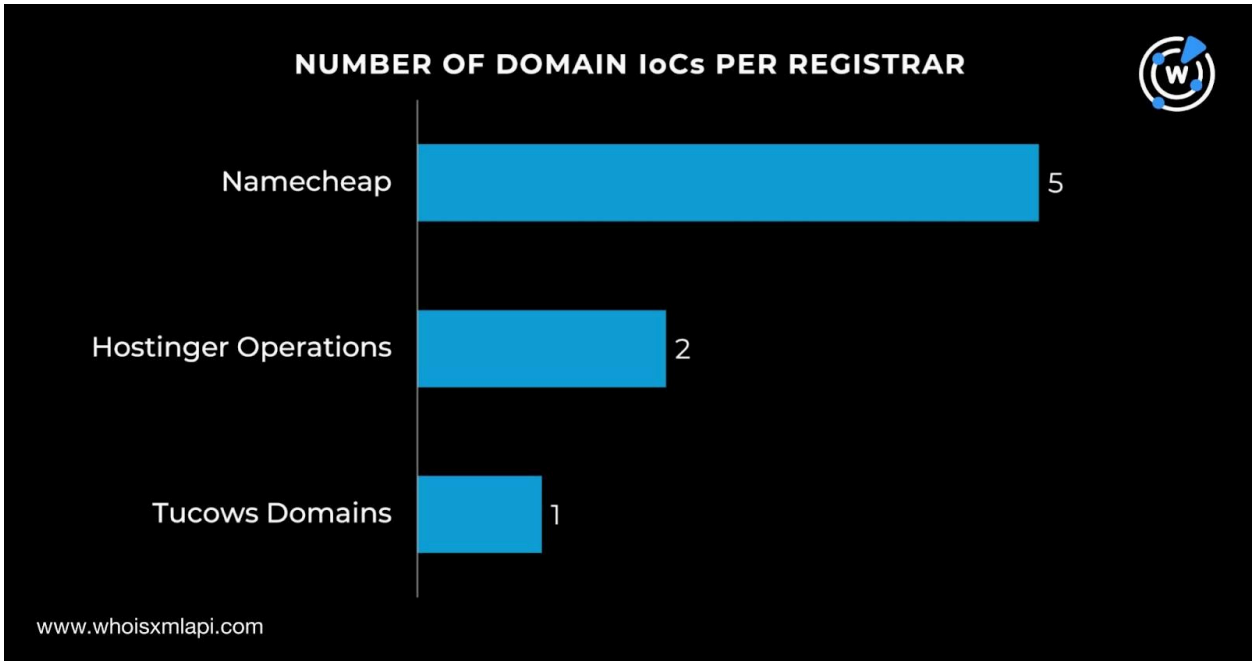
The First Watch Malicious Domains Data Feed query results for the 19 domains tagged as IoCs showed that one domain IoC—keondigital[.]com—was dubbed likely to turn malicious 189 days before it was identified as such on 1 September 2025. It was specifically added to First Watch on 24 February 2025.

We then queried the 19 domains tagged as IoCs on WHOIS API and discovered that only eight had current WHOIS records. Of these:

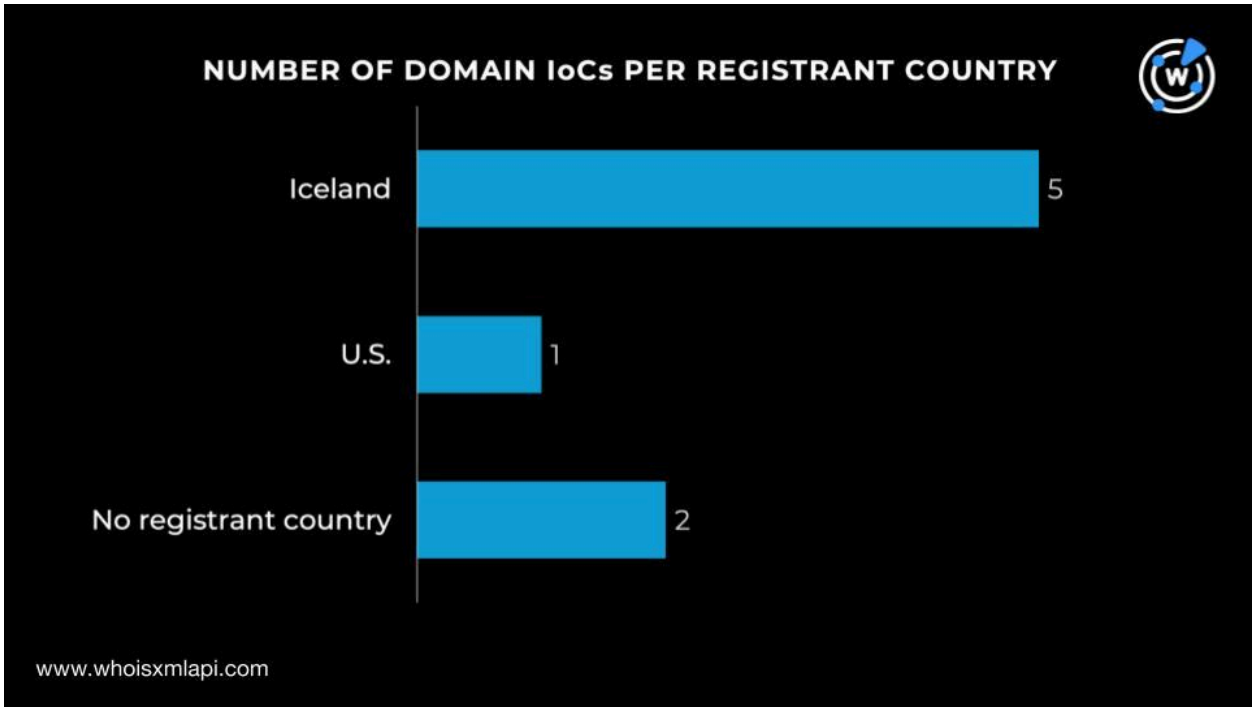
- The domain IoC pypilibrary[.]com had the earliest creation date—18 August 2023—while arcashop[.]org had the latest—18 July 2025. All in all, the eight active domain IoCs were created between 2023 and 2025. Interestingly, two (aes-secure[.]net and azureglobalaccelerator[.]com) had the same creation date (18 September 2023). In addition, another (jdkgradle[.]com) was created within a week as the first two, on 22 September 2023. This could indicate use for the same malicious campaign.



- They were administered by three different registrars led by Namecheap, which accounted for five domain IoCs. Hostinger Operations took the second spot with two domains, followed by Tucows Domains with one domain in third place.



- While two domain IoCs did not have registrant countries on record, the remaining six were registered in two countries. Five were registered in Iceland while one was registered in the U.S.

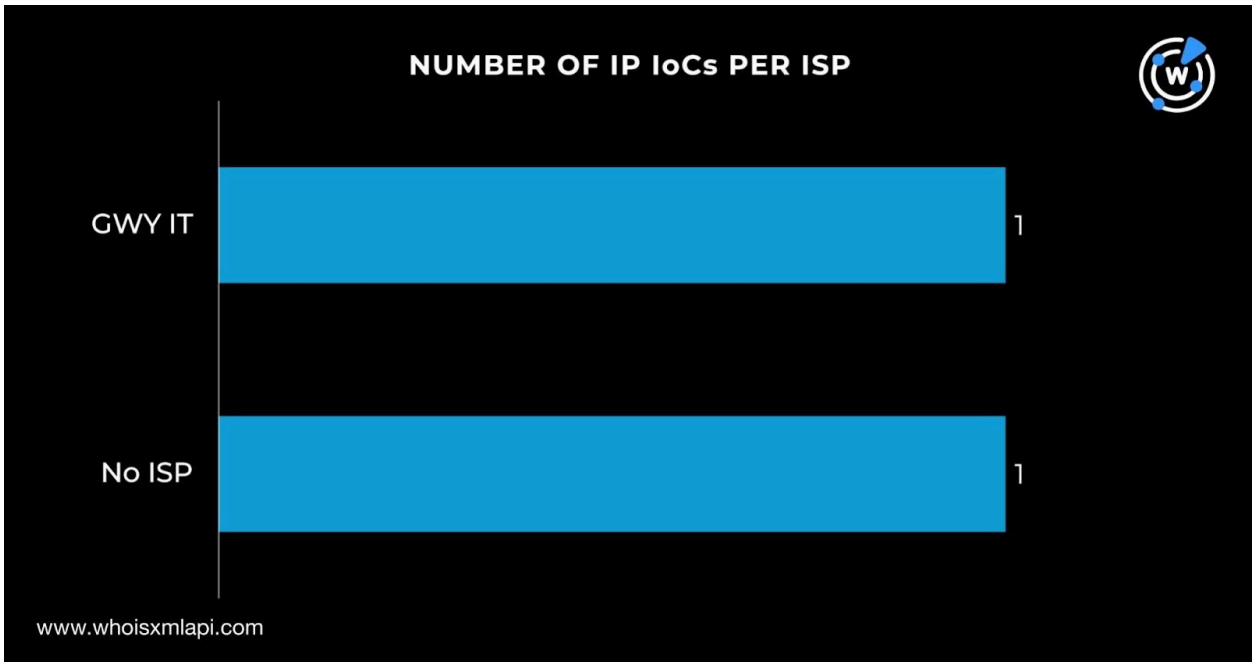


A query for the 19 domains tagged as IoCs on DNS Chronicle API revealed that all had rich DNS histories. They had 665 domain-to-IP resolutions over time since 5 February 2017. This indicates possible use for malicious campaigns between 2017 and 2025. Take a look at specific examples below.

DOMAIN IoC	TOTAL NUMBER OF DOMAIN-TO-IP RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE (prior to data gathering)
arcashop[.]org	125	5 February 2017	23 July 2025
plexisco[.]com	92	6 February 2017	9 January 2023
oncehub[.]co	130	7 May 2020	2 September 2024
lmaxtrd[.]com	8	25 November 2020	13 August 2021
calendly[.]live	74	5 March 2021	18 May 2025

From the table above, we can discern that while the domain IoCs lmaxtrd[.]com, oncehub[.]co, and plexisco[.]com may not be in active use as of this writing, they were certainly so between 2020 and 2021, 2020 and 2024, and 2017 and 2023, respectively. These dates could potentially be connected to their weaponization for attacks.

Next, we queried the two IP addresses tagged as IoCs on Bulk IP Geolocation Lookup and found out that while they were both geolocated in the U.S. (consistent with the list of registrant countries), only one had an ISP on record—GWY IT.



A DNS Chronicle API query for the two IP addresses tagged as IoCs showed that both had DNS histories. Together, they had 685 IP-to-domain resolutions over time. Specifically, the IP address 192[.]52[.]166[.]253 posted 682 resolutions from 6 February 2017 to 4 September 2025. Note the similarity in timing, spanning 2017 to 2025, with some of the domain IoCs.

Unearthing New Artifacts

We began our search for new artifacts by querying the 19 domains tagged as IoCs on WHOIS History API. We found out that 14 had 24 unique email addresses in their historical WHOIS records. Only one of the email addresses was public.

We then queried the public email address on Reverse WHOIS API and discovered that while it did not appear in any other domain's current WHOIS record, it was found in the historical

WHOIS record of one email-connected domain—kmc-ksa[.]com—after duplicates and those already identified as IoCs were filtered out.

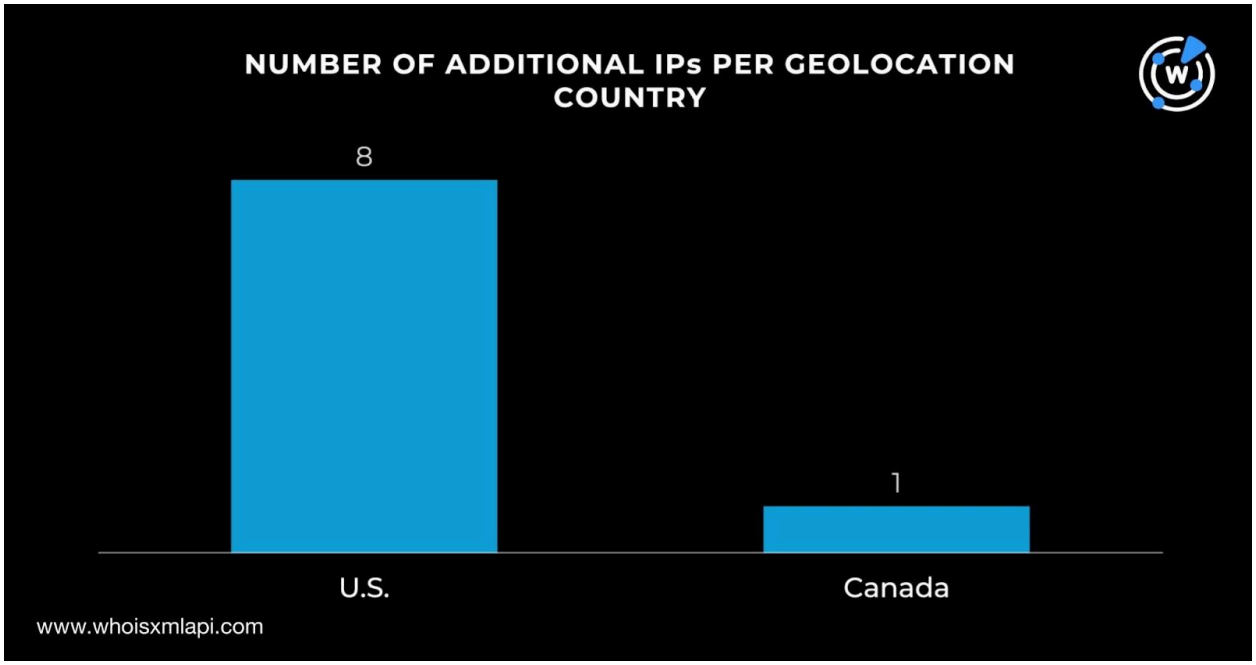
Next, a DNS Lookup API query for the 19 domains tagged as IoCs revealed that nine actively resolved to nine unique additional IP addresses after duplicates and those already identified as IoCs were filtered out.

A Threat Intelligence API query for the nine additional IP addresses showed that eight have already been flagged as malicious in connection to various threats. Here are a few examples.

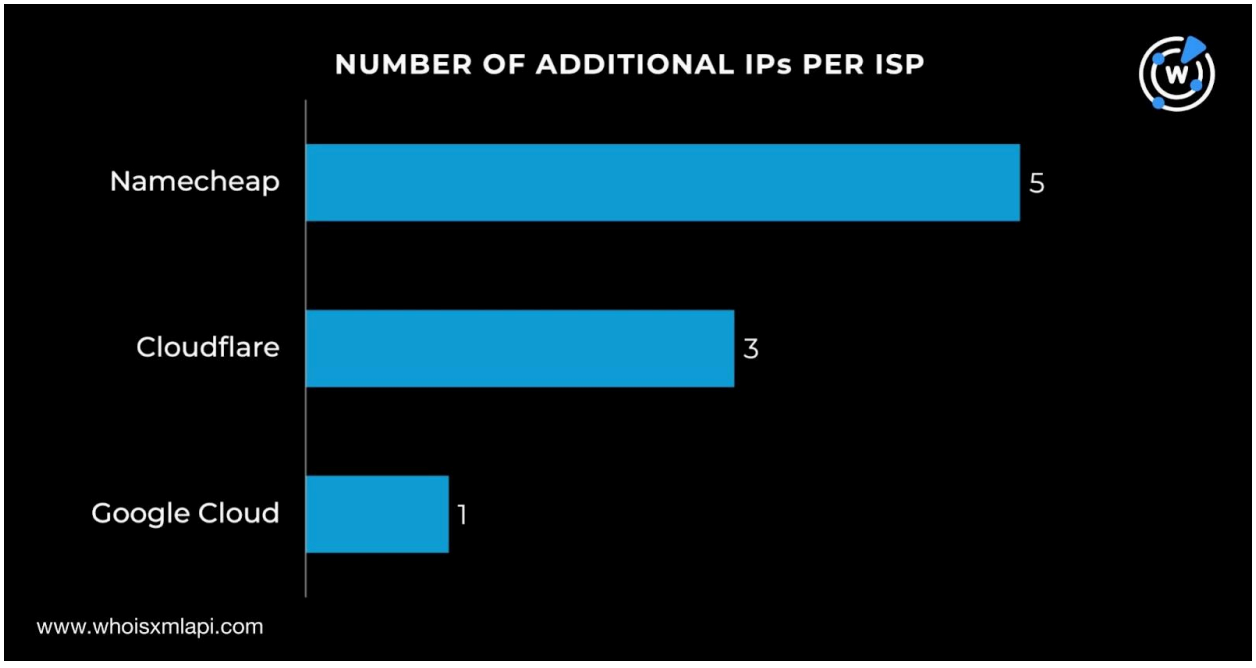
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT
23[.]227[.]38[.]67	Phishing Generic threat Malware distribution Suspicious activity Command and control (C&C)
34[.]111[.]179[.]208	Malware distribution Generic threat Phishing Attack
172[.]67[.]204[.]8	Phishing Generic threat Malware distribution

A Bulk IP Geolocation Lookup query for the nine additional IP addresses led to these discoveries:

- While eight of them were geolocated in the U.S., one originated from Canada.



- They were administered by three ISPs led by Namecheap, which accounted for five IP addresses. Cloudflare came in second place with three IP addresses while Google Cloud took the third spot with one.



After combining the IP addresses tagged as IoCs with those the domain IoCs resolved to, we had a total of 11 for further analysis.

A Reverse IP API query for the 11 IP addresses revealed that 10 played active hosts to 2,757 domains. Only one of them, however, could be a dedicated host. The possibly dedicated IP address 192[.]52[.]166[.]253 hosted 57 IP-connected domains after duplicates, those already tagged as IoCs, and the email-connected domain were filtered out.

Lastly, we took a closer look at the 19 domains tagged as IoCs and collated 19 unique text strings. Based on Domains & Subdomains Discovery search results, these 10 strings appeared at the start of 259 string-connected domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out:

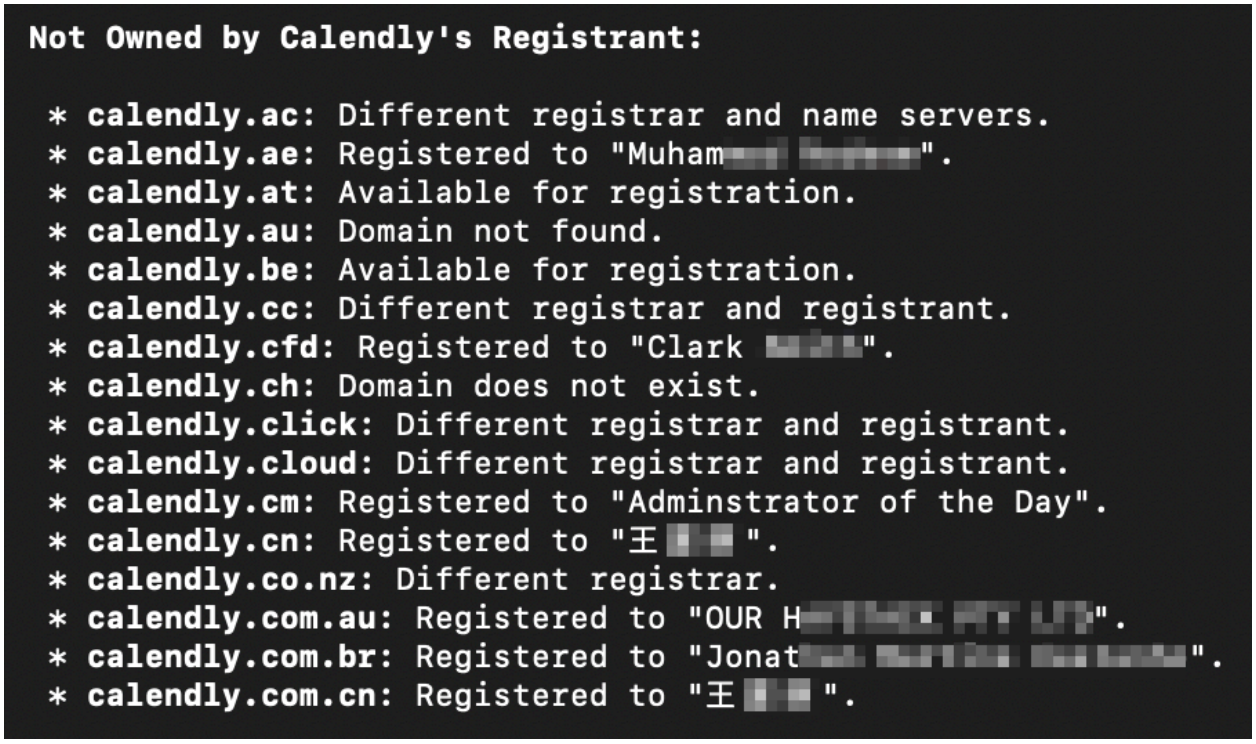
- aes-secure.
- arcashop.
- calendly.
- ftxstock.
- jdkgradle.
- latamics.
- natefi.
- oncehub.
- picktime.
- plexisco.

We sought to discover more about the look-alikes of the domain IoC calendly[.]live. Some of them could be mimicking calendly[.]com—the legitimate domain of the online appointment scheduling software Calendly. The app had 10 million users, more than 57,000 of whom were businesses, as of the end of 2022. That translates to a huge and growing base of potential victims.

We used the prompt "Which of the domains (list) do not have the same owner as calendly[.]com based on their WHOIS records?" on the WhoisXML API MCP Server. We discovered that these look-alike domains were likely not owned by calendly[.]com's registrant due to the WHOIS record discrepancies stated below.

LOOK-ALIKE DOMAIN	REASON
calendly.ac	Different registrar and name servers
calendly.ae	Different registrant
calendly.cfd	
calendly.cm	
calendly.cn	
calendly.com.au	

calendly.com.br	
calendly.com.cn	
calendly.at calendly.be	Available for registration
calendly.au	Domain not found
calendly.ch	
calendly.cc calendly.click calendly.cloud	Different registrar and registrant
calendly.co.nz	Different registrar



Eight look-alike domains were, however, likely Calendly-owned.

```
Likely Owned by Calendly's Registrant (or their proxy):

 * calendly.ai
 * calendly.asia
 * calendly.biz
 * calendly.blog
 * calendly.ca
 * calendly.co
 * calendly.co.in
 * calendly.co.uk
```

—

Our in-depth analysis of the IoCs related to the three Lazarus RATs revealed that one unique client IP address under one distinct ASN queried one unique domain IoC via 21 DNS queries between 18 and 20 August 2025. Also, two unique alleged victim IP addresses communicated with two distinct IP IoCs under two unique ASNs.

First Watch also showed that one domain IoC—keondigital[.]com—was dubbed likely to turn malicious 189 days before it was identified as such.

We also unearthed 326 new artifacts comprising one email-connected domain, nine additional IP addresses, 57 IP-connected domains, and 259 string-connected domains. To date, eight of these artifacts 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.*

Appendix: Sample Artifacts

Sample Additional IP Addresses

- 104[.]21[.]58[.]123
- 162[.]213[.]255[.]33
- 162[.]213[.]255[.]37
- 23[.]227[.]38[.]67
- 34[.]111[.]179[.]208
- 68[.]65[.]123[.]44

Sample IP-Connected Domains

- 10flash[.]net
- amysfloraldesign[.]com
- catastrophic-injury[.]com
- eieiostudio[.]com
- ftp[.]10flash[.]net
- ftp[.]amysfloraldesign[.]com
- ftp[.]catastrophic-injury[.]com
- kladionice-zderic[.]hr
- mail[.]10flash[.]net
- mail[.]amysfloraldesign[.]com
- mail[.]kladionice-zderic[.]hr
- ns1[.]plentant[.]net
- nuffnangx[.]com
- ohioangler[.]net
- plentant[.]net
- pop[.]10flash[.]net
- pop[.]amysfloraldesign[.]com
- raspberryjam[.]org[.]uk
- regionput[.]com
- rhodes-caribbean[.]com
- satu-mare[.]com
- smtp[.]10flash[.]net
- smtp[.]amysfloraldesign[.]com
- unifiedtradein[.]com
- www[.]amysfloraldesign[.]com
- www[.]kladionice-zderic[.]hr
- www[.]nuffnangx[.]com

Sample String-Connected Domains

- aes-secure[.]com
- aes-secure[.]de
- aes-secure[.]email
- arcashop[.]be
- arcashop[.]cn
- arcashop[.]co
- calendly[.]ac
- calendly[.]ae
- calendly[.]ai
- ftxstock[.]org
- ftxstock[.]xyz
- jdkgradle[.]ph
- jdkgradle[.]ws
- latamics[.]com
- latamics[.]ws
- natefi[.]cat
- natefi[.]com
- natefi[.]com[.]br
- oncehub[.]cm
- oncehub[.]cn
- oncehub[.]com
- picktime[.]app
- picktime[.]at
- picktime[.]cc
- plexisco[.]ph
- plexisco[.]ws