WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A DNS Analysis of the Keenadu Backdoor Network

Threat Report

Table of Contents

Executive Report

A backdoor dubbed “Keenadu” has been identified in the firmware of devices from various Android smartphone brands. Researchers believe the infection stemmed from a malicious static library linked with libandroid_runtime.so during the firmware build phase. In other cases, the compromised firmware was delivered via OTA updates.

Keenadu is a multistage loader that grants its operators unrestricted ability to control victims’ devices remotely. Its payloads include hijacking search engines, monetizing new app installs, and stealthily interacting with ad elements.

Securelist published several network IoCs related to the threat. And after extracting domains from subdomains identified as IoCs and weeding out legitimate domains from their list, we further analyzed 29 IoCs comprising five subdomains, 20 domains, and four IP addresses, which allowed us to uncover these findings:

- 339 unique client IP addresses communicated with three of the domains tagged as IoCs
- Three of the domains dubbed as IoCs seem to have been registered with malicious intent from the get-go
- 61 distinct potential victim IP addresses communicated with two of the IP addresses named as IoCs
- 80 email-connected domains, 12 of which turned out to be malicious
- Eight additional IP addresses, four of which have already been weaponized for various attacks
- 52 IP-connected domains, two of which already figured in malicious campaigns
- 69 string-connected domains

Studying the DNS Footprint of the Subdomain IoCs

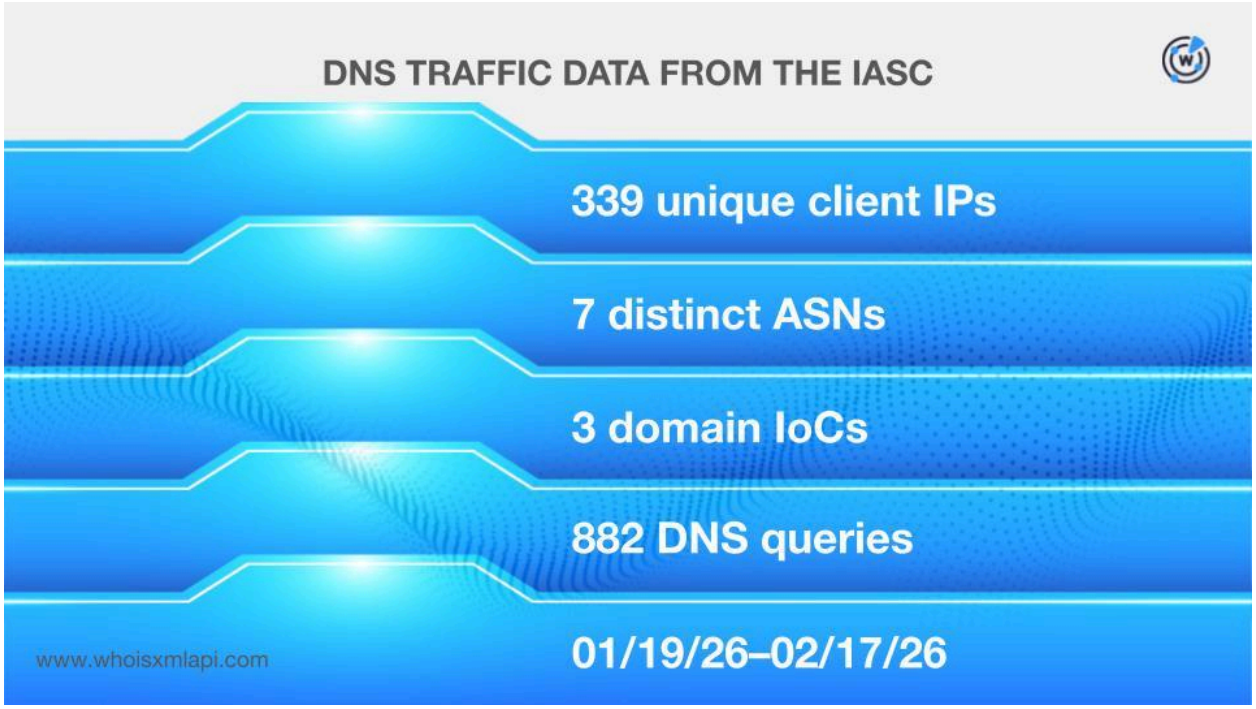
According to the results of our queries for the five subdomains identified as IoCs on the WhoisXML API MCP Server, all of them have already been flagged as malware between 19 February to 12 March 2026.

And while three of them were hosted on legitimate cloud servers, it is not uncommon for threat actors to abuse such services for their nefarious gain. It is also worth noting that the remaining two subdomains were hosted on a domain—istaticfiles[.]com—that seems to have been purposely registered to host malicious content.

Divulging DNS Facts about the Domain IoCs

We then sought out more information about the 20 domains that have been identified as IoCs.

Sample network traffic data from the IASC, for one, revealed that 339 unique client IP addresses communicated with three of the domains tagged as IoCs via 882 DNS queries made between 19 January and 17 February 2026. These IP addresses fell under seven distinct ASNs.

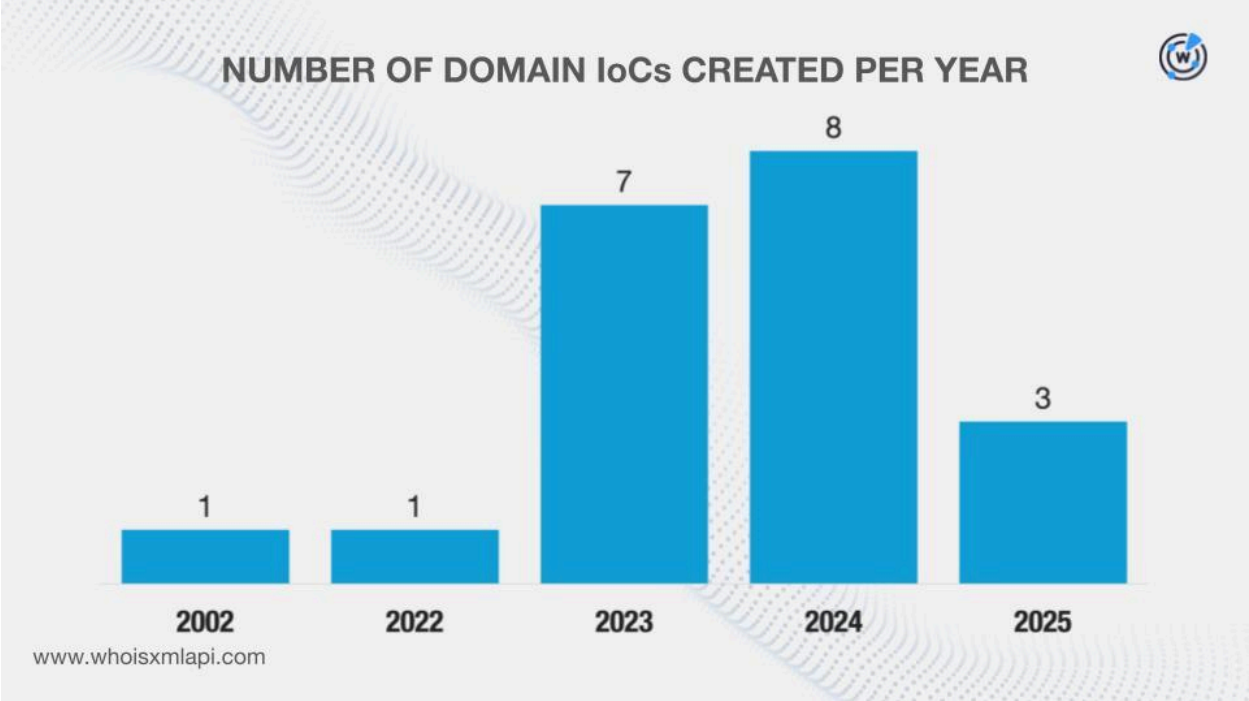


Data from the First Watch Malicious Domains Data Feed, meanwhile, showed that three of the domains dubbed as IoCs were deemed likely to turn malicious 357–628 days before they were dubbed as such on 17 February 2026. Here are more details.

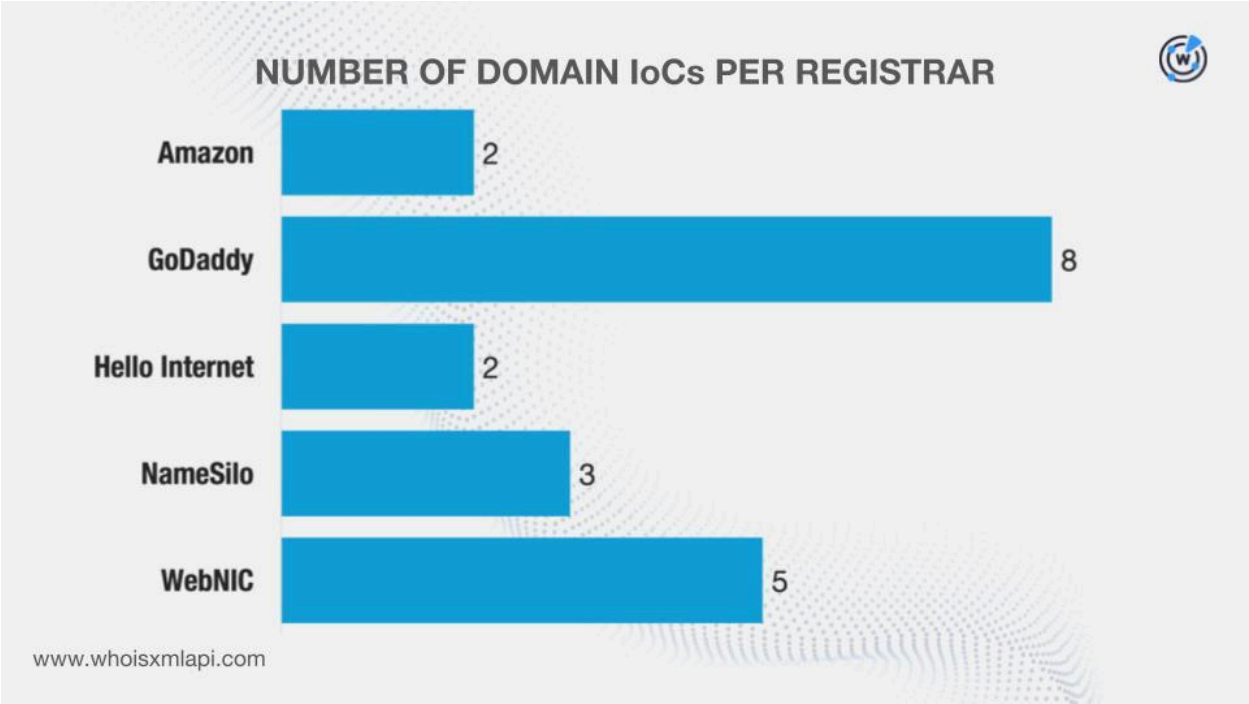
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE THE REPORT DATE
gvvt1[.]com	05/30/24	628
dllpgd[.]click	12/16/24	428
playstations[.]click	02/25/25	357

Next, we queried the domains on WHOIS API and learned that:

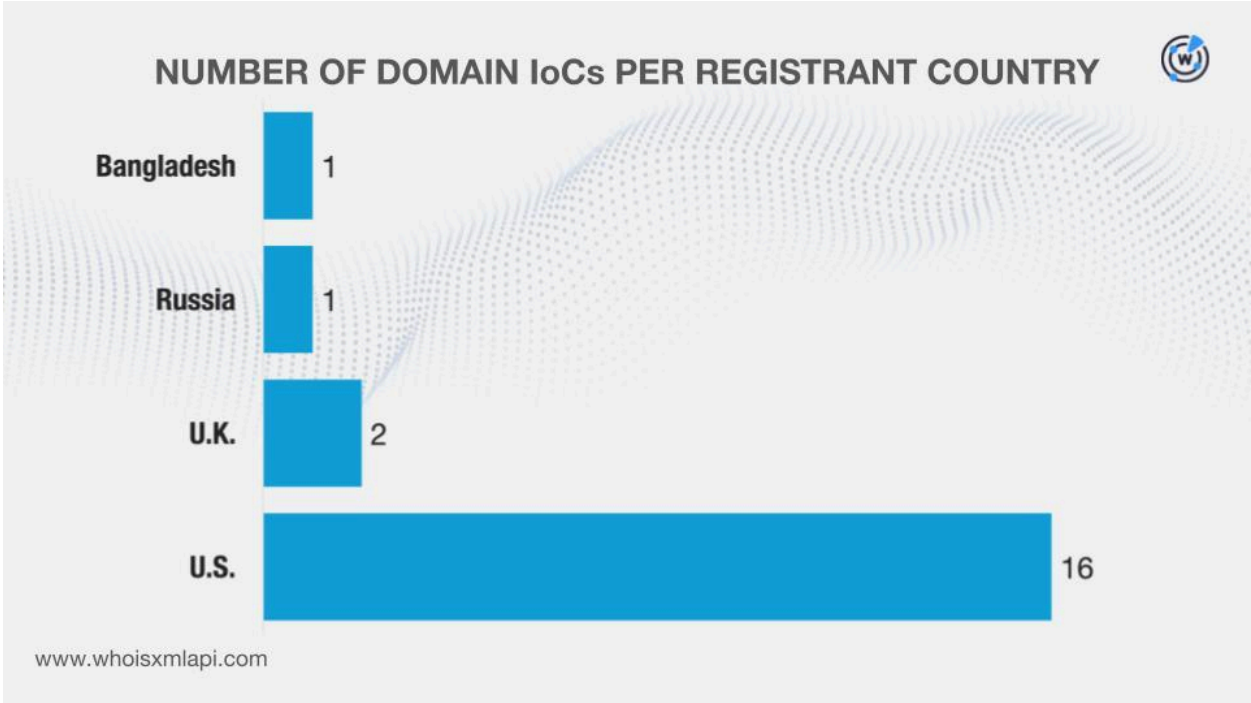
- They were created between 4 March 2002 and 21 November 2025, hinting at the threat actors' preference for old domains.



- They were administered by five different registrars.



- They were registered in four disparate countries.



DNS Chronicle API queries for the domains revealed that 12 recorded 1,245 historical domain-to-IP resolutions over time. Take a look at the five domains with the oldest first resolution dates below.

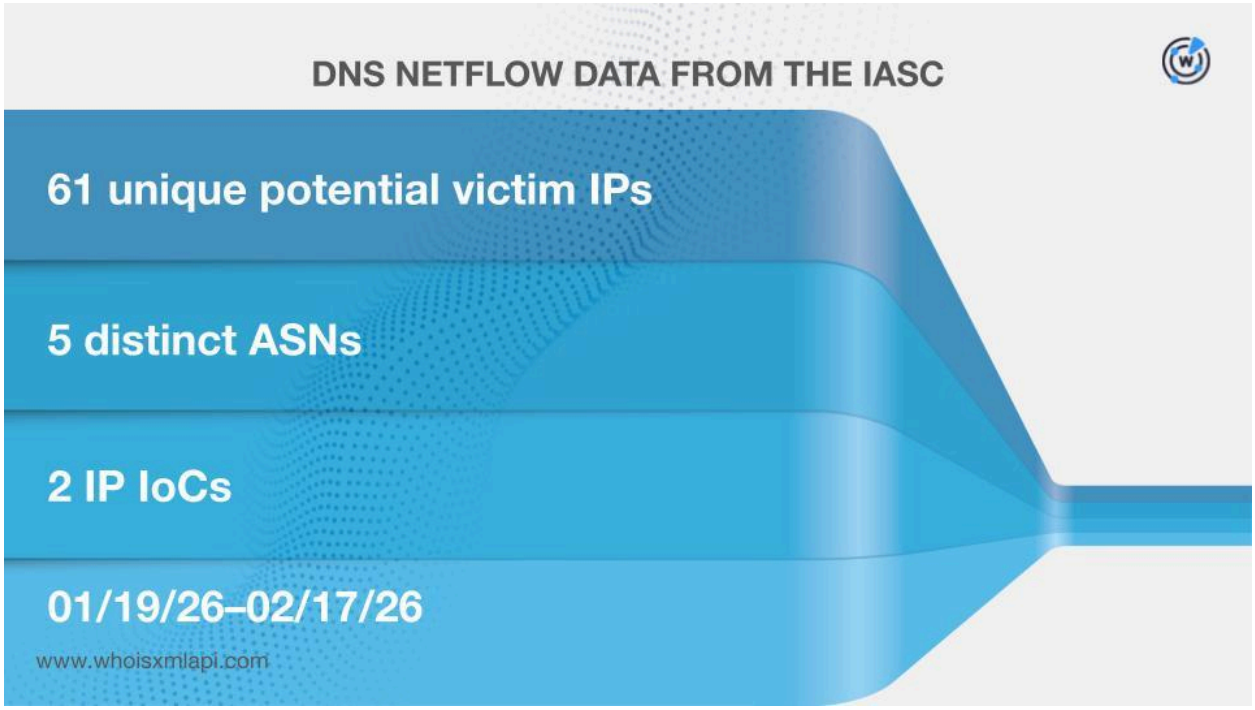
DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
gsonx[.]com	106	08/12/17–02/07/24
fbgraph[.]com	47	08/16/19–12/31/25
proczone[.]com	42	01/09/21–02/09/22
keepgo123[.]com	30	01/28/22–04/02/24
istaticfiles[.]com	190	06/28/23–02/09/26

It is also interesting to note that many domains, five to be exact, first resolved to IP addresses sometime in 2023.

Investigating the DNS Infrastructure of the IP IoCs

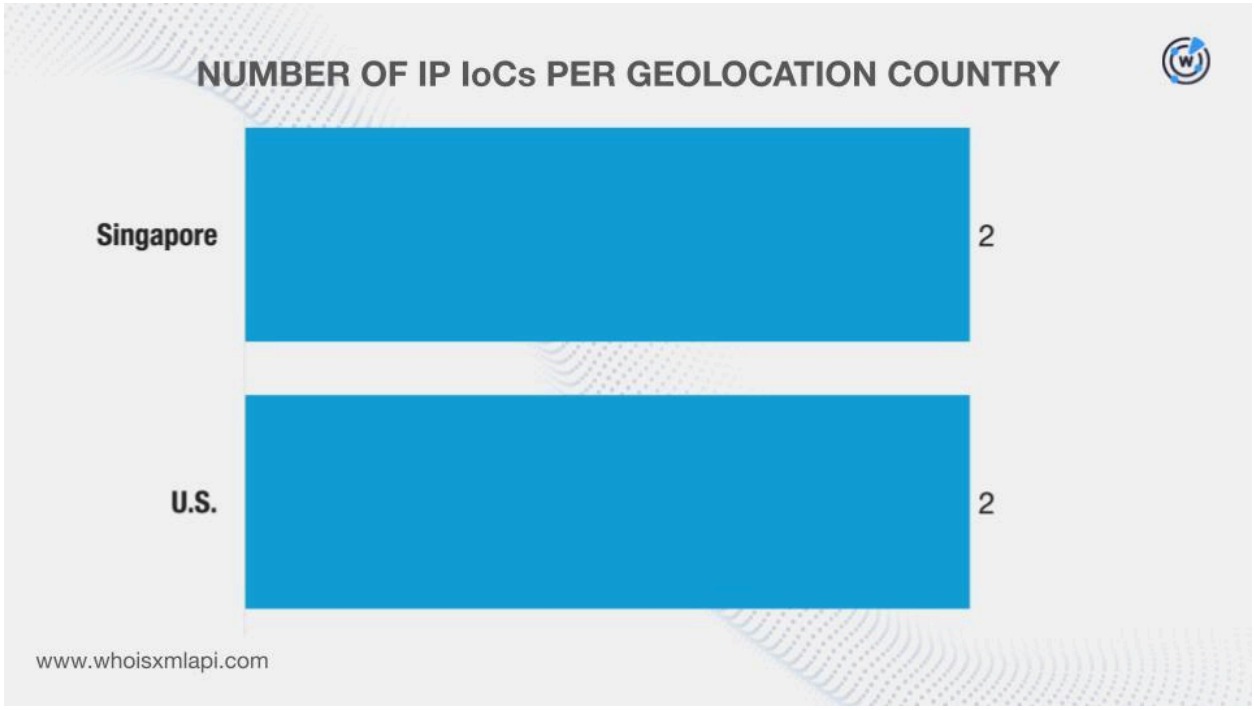
Next, we focused on the four IP addresses identified as IoCs.

First off, sample network data from the IASC revealed that 61 unique potential victim IP addresses communicated with two of the IP addresses tagged as IoCs between 19 January and 17 of February 2026. The victim IP addresses fell under five distinct ASNs.



Next, we queried the IP addresses on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in two countries. Note that the U.S. was also named as the registrant country of several of the domains tagged as IoCs.



- They were all administered by VPLS.

DNS Chronicle API queries for the IP addresses, meanwhile, showed that all four posted 1,896 historical IP-to-domain resolutions over time. Here are more details.

IP IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	DATES SEEN
110[.]34[.]191[.]81	20	11/29/17–12/20/25
67[.]198[.]232[.]187	934	10/05/19–02/17/26

Hunting for New Artifacts

In this final phase of our investigation, we scoured the DNS for artifacts potentially connected to Keenadu.

We started by querying the 20 domains identified as IoCs on WHOIS History API. We learned that 14 of them had 27 unique email addresses in their historical WHOIS records. Closer scrutiny allowed us to determine that six were public email addresses.

Reverse WHOIS API queries for the public email addresses led to the discovery of 80 unique email-connected domains after those already tagged as IoCs were filtered out.

We then queried the email-connected domains on Threat Intelligence API and found out that 12 have already been weaponized for various attacks. Take a look at five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
fuhidd[.]com	Malware distribution	07/24/25–02/17/26
huulog[.]com	Malware distribution	07/24/25–02/17/26
huuww[.]com	Malware distribution	07/24/25–02/17/26
mtcpmpm[.]com	Malware distribution	07/24/25–02/17/26
mtcprogram[.]com	Malware distribution	07/24/25–02/17/26

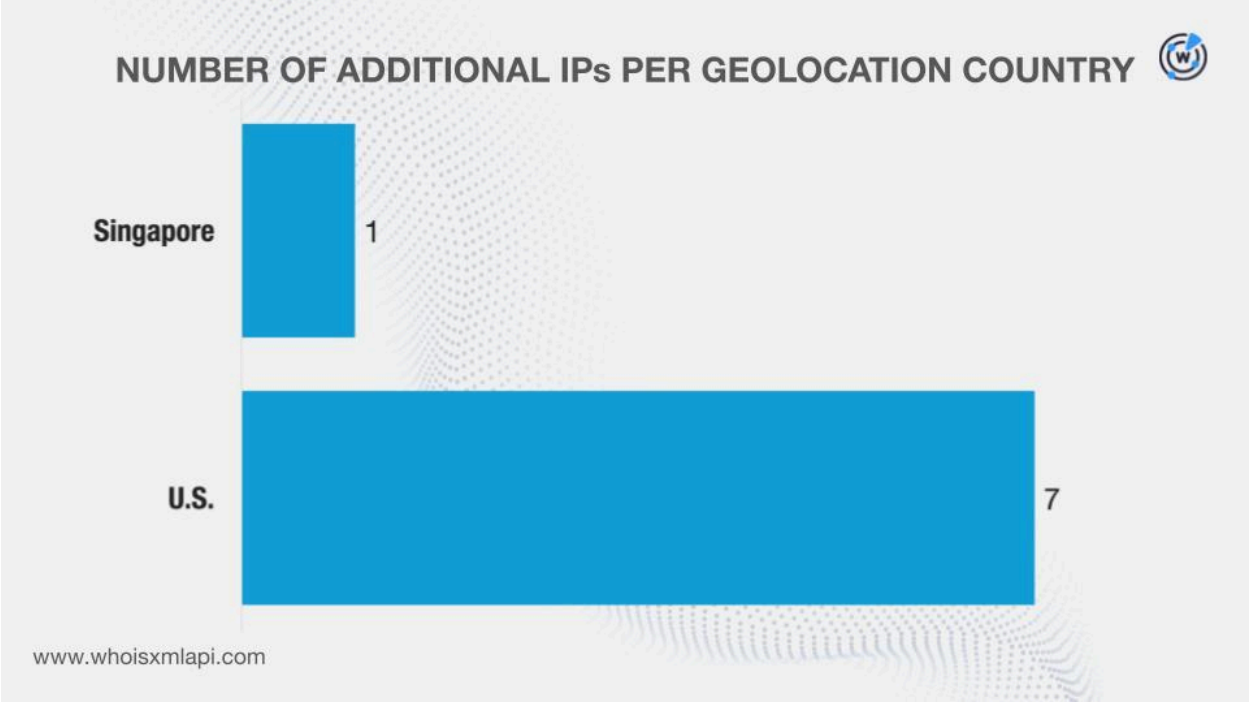
Next, we queried the domains dubbed as IoCs on DNS Lookup API and discovered that five resolved to eight additional IP addresses.

Threat Intelligence API queries for the additional IP addresses revealed that four have already figured in various malicious campaigns. Here are more details.

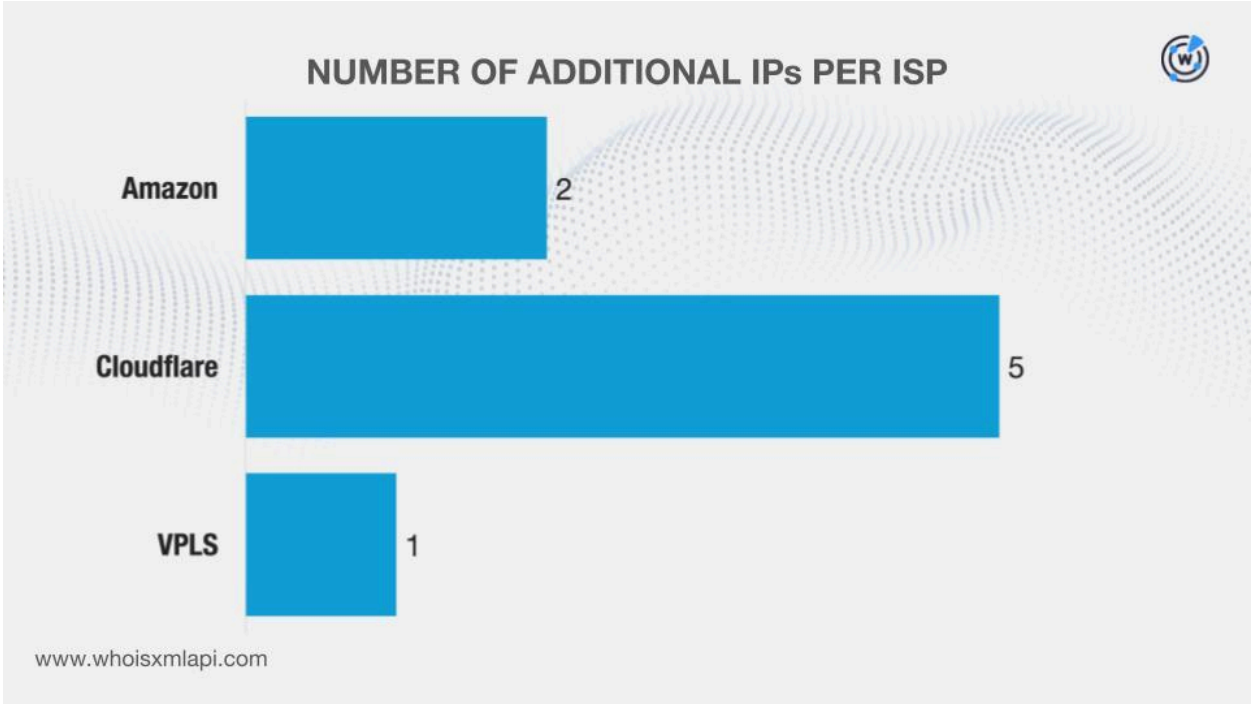
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
104[.]21[.]87[.]166	Malware distribution Phishing	08/22/25–02/17/26 01/31/24–12/23/25
172[.]67[.]144[.]175	Malware distribution Phishing	08/22/25–02/17/26 01/31/24–12/23/25

A Bulk IP Geolocation Lookup for the additional IP addresses, meanwhile, showed that:

- They were geolocated in two countries—the same ones the IoCs originated from.



- Unlike the IoCs, however, only one was administered by VPLS. The remaining seven were split between two other ISPs.



We now had 12 IP addresses on hand, which we queried on Reverse IP API. We determined that seven could be dedicated hosts. Together, they hosted 52 unique IP-connected domains after those already named as IoCs and the email-connected domains were filtered out.

Threat Intelligence API queries for the IP-connected domains revealed that two were already considered malicious. The domain dllpgd[.]click, for instance, has been associated with malware distribution between 22 January and 17 February 2026.

After that, we extracted unique text strings from the domains classified as IoCs. Our Domains & Subdomains Discovery searches enabled us to determine that domains other those already categorized as IoCs started with these three strings:

- fbgraph.
- gsonx.
- playstations.

This step led to the discovery of 69 unique string-connected domains after those already identified as IoCs and the email- and IP-connected domains were filtered out. Note that these domains only serve to reflect the overall popularity of the strings extracted from the IoCs. As such, determining their legitimacy may require further investigation.

What Our Analysis Revealed

Our DNS deep dive into the Keenadu network IoCs revealed that 339 unique client IP addresses communicated with three of the domains identified as IoCs. We also learned that three domains tagged as IoCs were deemed likely to turn malicious as soon as they were registered. In addition, 61 distinct potential victim IP addresses communicated with two of the IP addresses dubbed as IoCs.

We also unearthed 209 new artifacts comprising 80 email-connected domains, eight additional IP addresses, 52 IP-connected domains, and 69 string-connected domains. It is also worth noting that to date, 18 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 Email-Connected Domains

- fuhidd[.]com
- huulog[.]com
- huuww[.]com
- mtcpmpm[.]com
- mtcprogram[.]com
- mtcpuouo[.]com
- pasiont[.]com
- retrofitxer[.]com
- yydsma[.]com
- yydsmb[.]com
- yydsmd[.]com
- yydsmr[.]com

Sample Additional IP Addresses

- 104[.]21[.]87[.]166
- 172[.]67[.]144[.]175
- 18[.]204[.]68[.]18
- 18[.]206[.]233[.]238

Sample IP-Connected Domains

- dllpgd[.]click
- dllpgd[.]click
- aifacecloud[.]com
- cms[.]aifacetechx[.]com
- connectivity[.]tubitvstatic[.]com
- connectivity[.]tubitvstatic[.]com
- dailyanddeals[.]shop
- facamer[.]com
- facamer[.]com
- fbgraph[.]com
- fbgraph[.]com
- fbwestinfo[.]com
- fbwestinfo[.]com
- firebaseaio[.]com
- firebaseaio[.]com
- firebasestatic[.]com
- firebasestatic[.]com
- ga-i[.]goaimb[.]com
- ga-i[.]goaimb[.]com
- ggtvgraph[.]com
- ggtvgraph[.]com
- gmpicnav[.]com
- gmpicnav[.]com
- gmsstatics[.]com

Sample String-Connected Domains

- fbgraph[.]ga
- fbgraph[.]info
- fbgraph[.]xyz
- gsonx[.]cn
- gsonx[.]my
- gsonx[.]vip
- playstations[.]app
- playstations[.]blog
- playstations[.]ca