Tracing the DNS Footprints of REF7707

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts

Executive Report

The targeted attack campaign REF7707 trailed its sights on the foreign ministry of a South American country in February 2025. According to Elastic Labs, the group behind the campaign has been connected to previous compromises in Southeast Asia.

The REF7707 threat actors reportedly used three new malware families—FINALDRAFT, GUIDLOADER, and PATHLOADER—for the attack. The report of the campaign's in-depth analysis listed 13 indicators of compromise (IoCs) comprising eight domains and five IP addresses.

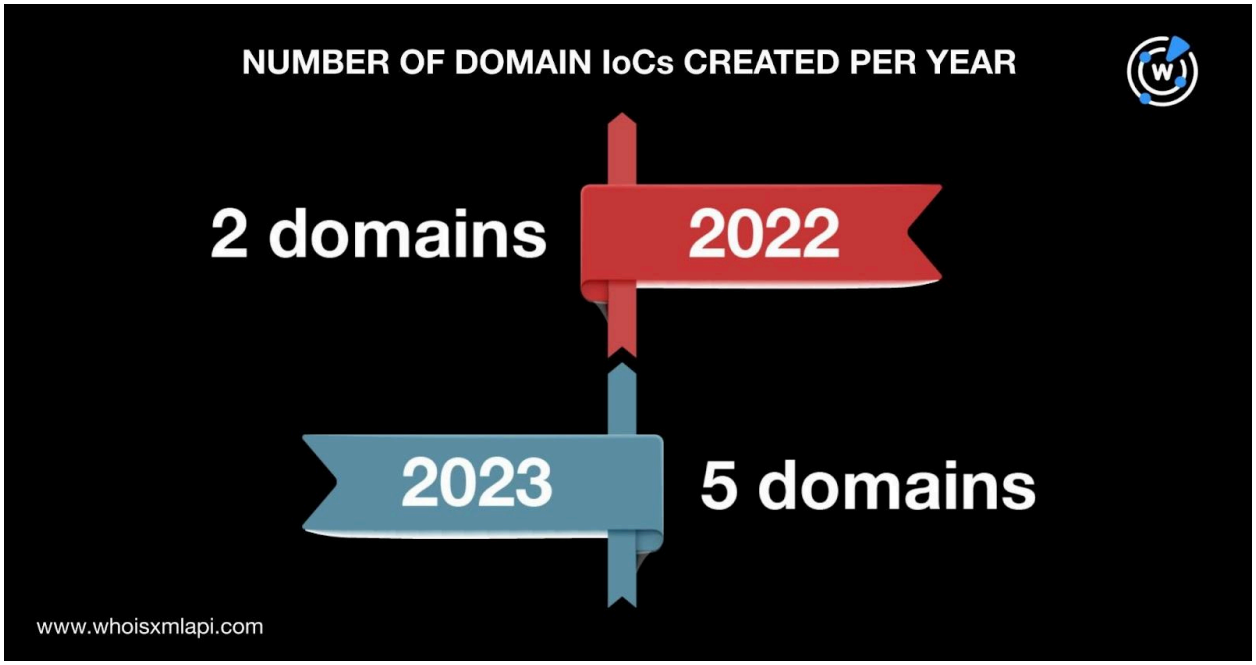
The WhoisXML API research team expanded the current list of IoCs and uncovered connected artifacts, namely:

- 155 email-connected domains
- One IP-connected domain
- 14 string-connected domains

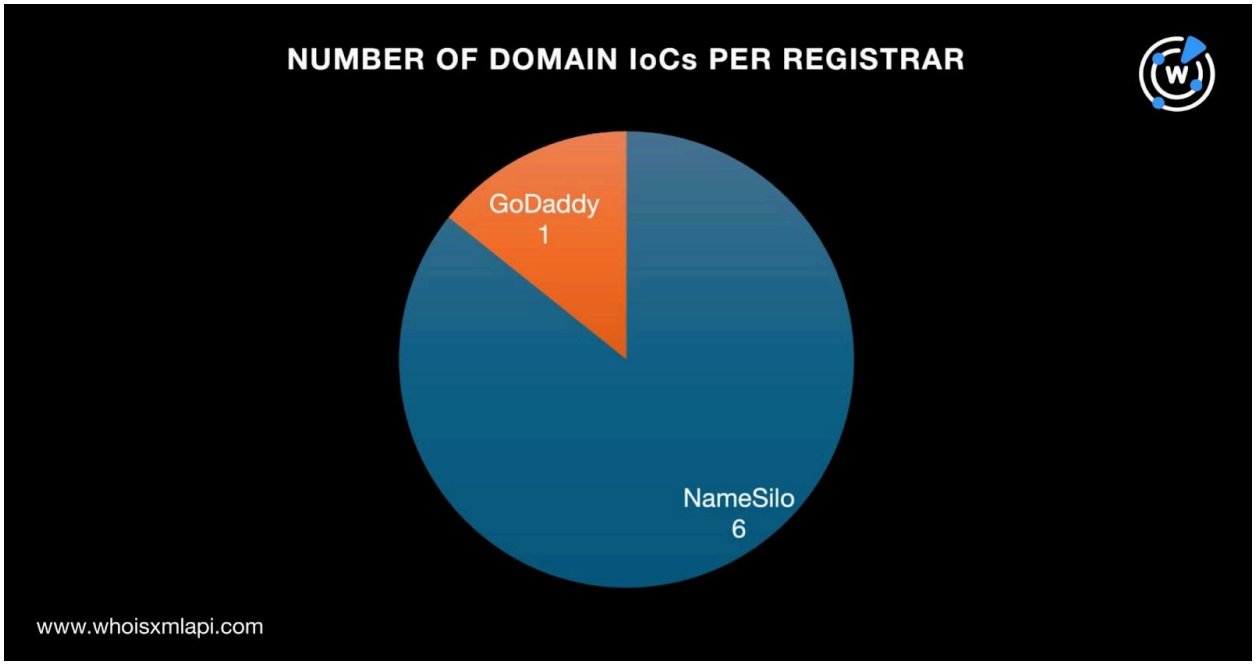
A Closer Look at the REF7707 IoCs

We started our investigation by looking for more information on the IoCs identified by Elastic Labs. First, we queried the eight domains tagged as IoCs on Bulk WHOIS API and found that only seven had current WHOIS records. The query results revealed that:

- All seven domains were somewhat old. Two were created in 2022 while five were created in 2023.



- They were administered by two registrars led by NameSilo, which accounted for six domains. GoDaddy administered one domain.



- All seven domains were registered in the U.S.

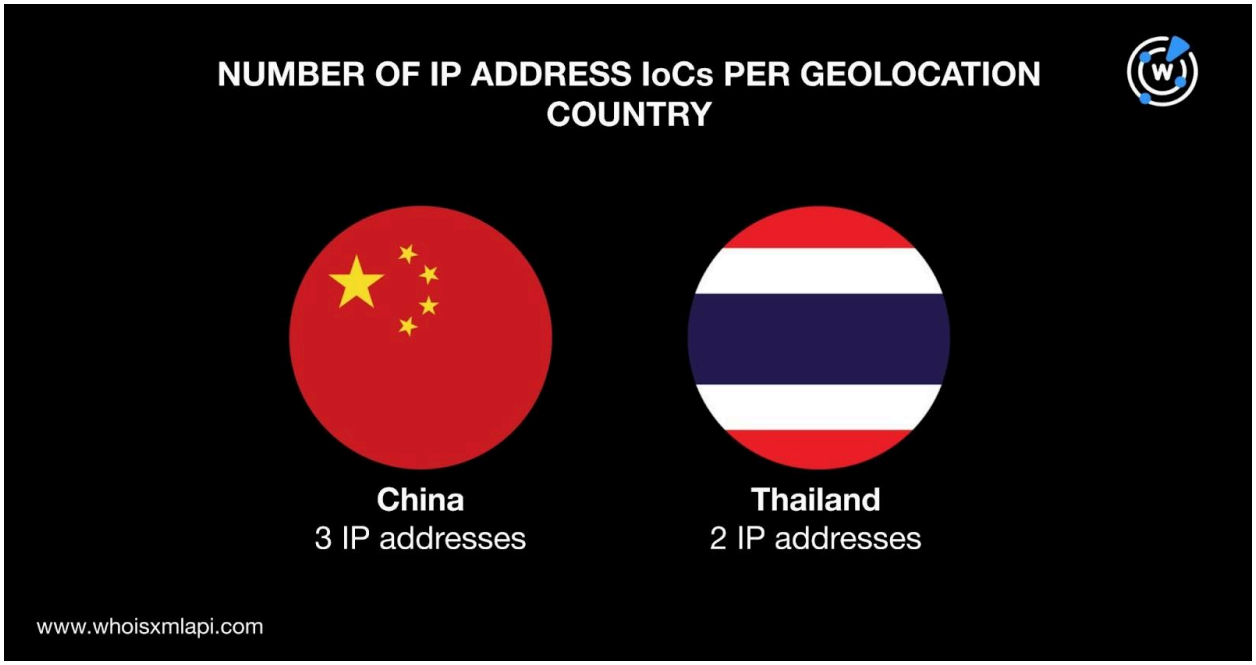
We then queried the eight domains identified as IoCs on DNS Chronicle API and found that five had historical IP resolutions. The five domains recorded 89 IP resolutions over time. The domain d-links[.]net had the oldest first IP resolution date—22 October 2019. The following table shows more details about three other domains.

DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
autodiscovar[.]com	21	27 August 2022
checkponit[.]com	15	28 August 2022
fortineat[.]com	26	27 August 2022

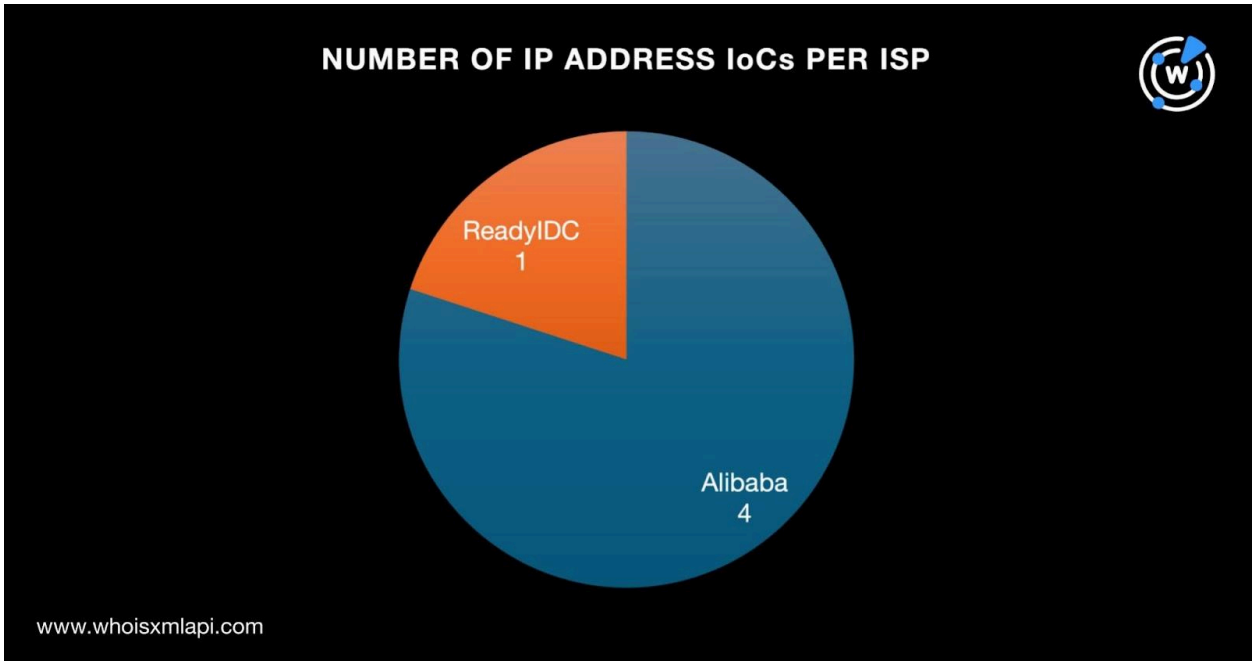
It is interesting to note that four of the five domains with DNS histories first resolved to IP addresses around the same date—between 27 and 28 August 2022.

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

- They were split between two countries led by China, which accounted for three IP addresses. The other two were geolocated in Thailand.



- They were also spread across two ISPs—four were administered by Alibaba and one by ReadyIDC.



We then queried the five IP addresses identified as IoCs on DNS Chronicle API and found that only two had DNS histories. Altogether, they had 21 historical IP resolutions over time. The IP address 47[.]239[.]0[.]216 recorded the oldest IP-to-domain resolution date—19 October 2024.

REF7707 IoC List Expansion Analysis Findings

As our first step toward uncovering possibly connected artifacts, we queried the eight domains identified as IoCs on WHOIS History API. We found 20 email addresses from their historical WHOIS records after duplicates were filtered out. Closer scrutiny revealed that four of them were public email addresses.

We then queried the four public email addresses on Reverse WHOIS API and found that none of them appeared in any other domain's current WHOIS records. So, we dug deeper and discovered that they appeared in the historical WHOIS records of 155 email-connected domains after duplicates and those already identified as IoCs were filtered out.

As the next step, we queried the eight domains identified as IoCs on DNS Lookup API and found that none of them actively resolved to IP addresses. But that did not stop our search for IP-connected domains since we still had five IP addresses that have already been tagged as IoCs.

So, we queried the five IP addresses identified as IoCs on Reverse IP API and discovered that only one—8[.]213[.]217[.]182—had DNS connections. We uncovered one IP-connected domain after duplicates, those already tagged as IoCs, and the email-connected domains were filtered out.

As the last step in unearthing other REF7707-connected artifacts, we used Domains & Subdomains Discovery to look for other domains that started with the same text strings as the eight domains identified as IoCs. We found that the following strings also appeared in other domains:

- d-links.
- hobiter.
- vm-clouds.
- vmphere.

Specifically, the four text strings led to the discovery of 14 string-connected domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

While none of the connected domains we uncovered turned out to be malicious to date according to Threat Intelligence API, many of them contained strings that could be typosquatting variants of known security brands like d-links (i.e., possibly spoofing D-Link), vm-clouds (i.e., potentially spoofing VMware Cloud), and vmphere (i.e., possibly spoofing VMware's Vsphere).

That said, we scoured our current list of artifacts and collated 13 brand-containing connected artifacts. Bulk WHOIS API revealed that:

- While dlink[.]com—D-Link's legitimate domain—had a privacy-protected WHOIS record, none of the 11 d-links-containing domains shared any of the pertinent data points in dlink[.]com's WHOIS record. None of them had the same registrar or privacy protection service provider.
- None of the two VMware brand-containing domains were publicly attributable to the company as well.

—

Our DNS deep dive into the REF7707 campaign IoCs led to the discovery of 170 possibly connected artifacts comprising 155 email-connected domains, one IP-connected domain, and 14 string-connected domains. The list of artifacts we unearthed also included domains

containing potentially typosquatting variants of brand names belonging to two security companies like many of the original IoCs.

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

- a-m-s[.]org
- about-youtube[.]com
- beynalharameyn[.]com
- bistarri[.]org
- c0o1[.]com
- caf-corsair[.]com
- d-asso[.]com
- d-asso[.]net
- e-off[.]org
- earhairremoval[.]org
- fan-fan[.]org
- farmerbob[.]org
- ganpishi[.]org
- georgiescarlett[.]com
- habia-east[.]org
- hahei-iken[.]org
- idee-cadeau-deco[.]com
- imposture-lefilm[.]com
- jesusnetjapan[.]org
- joanmendez[.]com
- k-japan[.]org
- kanpeki[.]org
- lakegeorgeminnesota[.]com
- lakooltura[.]com
- mobilewhoa[.]com
- modelone[.]net
- n-kyotofuyaku[.]org
- naturalgasetflist[.]com
- odessachambersmedia[.]com
- oldstonechurch[.]info
- pachislo[.]org
- pascal-malaterre-photo[.]com
- qeustepolan[.]org
- r246[.]org
- remon[.]org
- sachan[.]org
- saikou[.]org
- tanigawa[.]org
- thenevinpolitology[.]com
- ushio-jp[.]org
- uso-pacific[.]org
- wco-jp[.]org
- wherecondom[.]com
- xmotorkari[.]org
- xn--cck0ctck1788djk1b9vc[.]net
- ykkap[.]org
- yoshizawahitomi[.]org

Sample String-Connected Domains

- d-links[.]co[.]jp
- d-links[.]co[.]uk
- d-links[.]com
- hobiter[.]ws
- vm-clouds[.]com
- vmphere[.]ws