WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

# DNS Deep Diving into FakeWallet Crypto Stealer

Threat Report

## Table of Contents

## Executive Report

This March, researchers uncovered more than 20 phishing apps masquerading as popular crypto wallets. But when clicked, they redirected users to fake App Store pages where trojanized versions of the legitimate apps were hosted. If downloaded, the malicious apps dubbed "FakeWallet" hijacked affected users' recovery phrases and private keys. Worse, FakeWallet metadata suggests the campaign has been going on since at least fall 2025.

SecureList publicized 24 network IoCs comprising subdomains, domains, and an IP address in their FakeWallet analysis. We extracted unique domains from the subdomain IoCs they listed and determined if any of them belonged to legitimate organizations using the WhoisXML API MCP Server. We then filtered out legitimate and inactive domains from the final domain IoC list.

That said, we ended up with 28 network IoCs comprising 12 subdomains, 15 domains, and one IP address for our investigation. Aided by our extensive array of domain, DNS, and threat intelligence tools, our analysis led to these discoveries:

- One client IP address communicated with three domain IoCs
- One domain IoC was bulk-registered with two look-alikes
- Two domain IoCs were likely registered with malicious intent
- Nine potential victim IP addresses communicated with the sole IP IoC
- 10,812 email-connected domains, 11 were confirmed malicious
- 18 additional IP addresses, eight were confirmed malicious
- Eight IP-connected domains
- 17 string-connected domains

### FakeWallet Subdomain IoCs Under the Spotlight

We kicked off our investigation by looking more closely into the 12 subdomain IoCs via the WhoisXML API MCP Server. We summed up our findings for five examples below.

| SUBDOMAIN IoC | WXA MCP SERVER FINDING |
|---|---|
| 6688cf[.]jhxrpbgq[.]com | Flagged for malware distribution on 21–26 April 2026 |
| api[.]dc1637[.]xyz | Classified as suspicious due to lack of DNS data |
| api[.]npoint[.]io | While a legitimate service, it may have been used as an abuse vector |
| mgi1y[.]siyangoil[.]com | Flagged for malware distribution on 21–26 April 2026 |

| | |
|---|---|
| mti4ywy4[.]lahuafa[.]com | Flagged for malware distribution on 21–26 April 2026 |

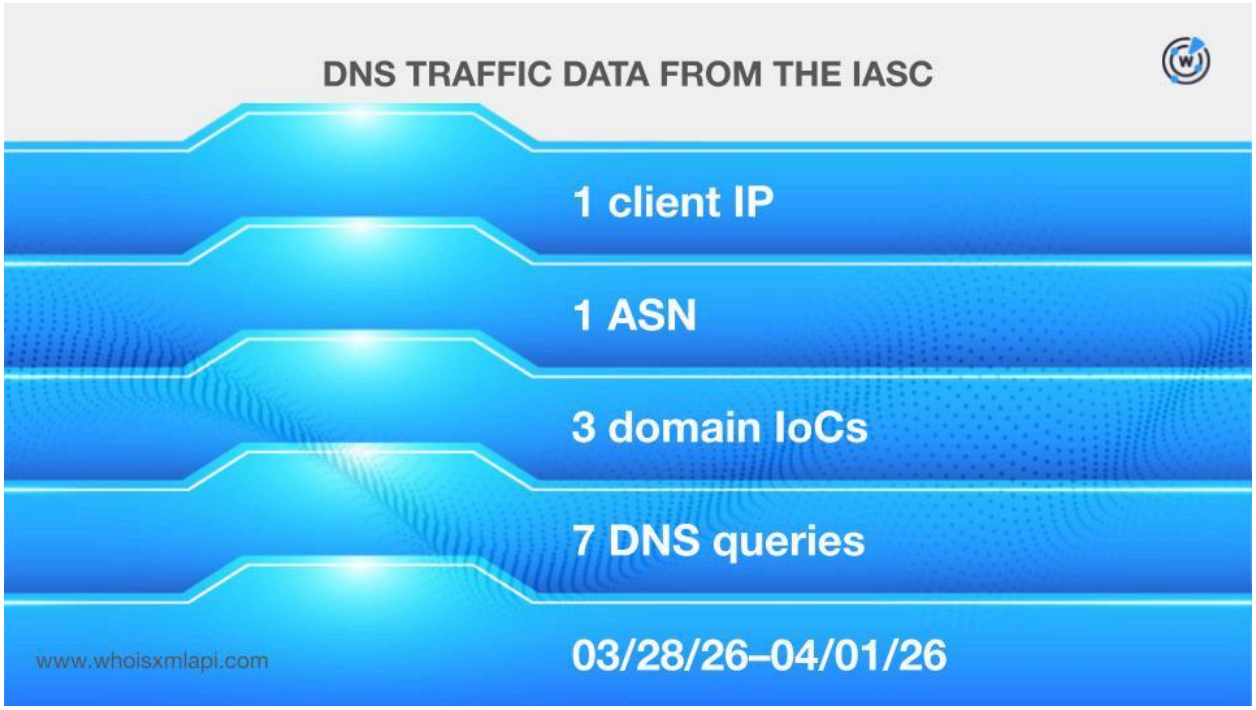
All in all, we determined that while one of the subdomain IoCs fell under a legitimate domain, it may have been specially crafted to host C&C configurations and payloads as JSON endpoints, since its Cloudflare IP addresses are hard to block without affecting legitimate traffic. Nine were confirmed malicious according to our tools, and two should be approached with caution.

It is also worth noting that the five parent domains of the nine subdomains were updated on 20 April 2026, the day before FakeWallet was first detected, which was consistent with precampaign infrastructure staging.

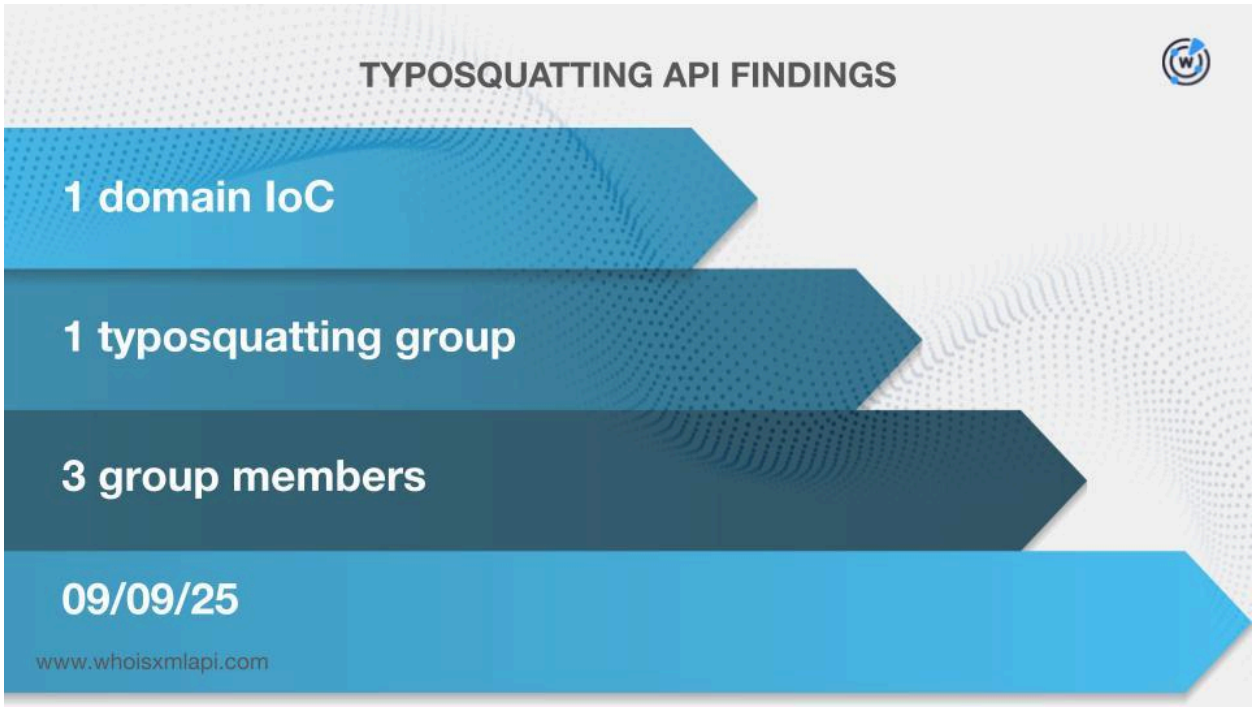
## FakeWallet Domain IoCs Deep Dive

Next, we analyzed the 15 domain IoCs in greater depth.

Sample network traffic data from the IASC revealed that one client IP address communicated with three domain IoCs via seven DNS queries between 28 March and 1 April 2026.



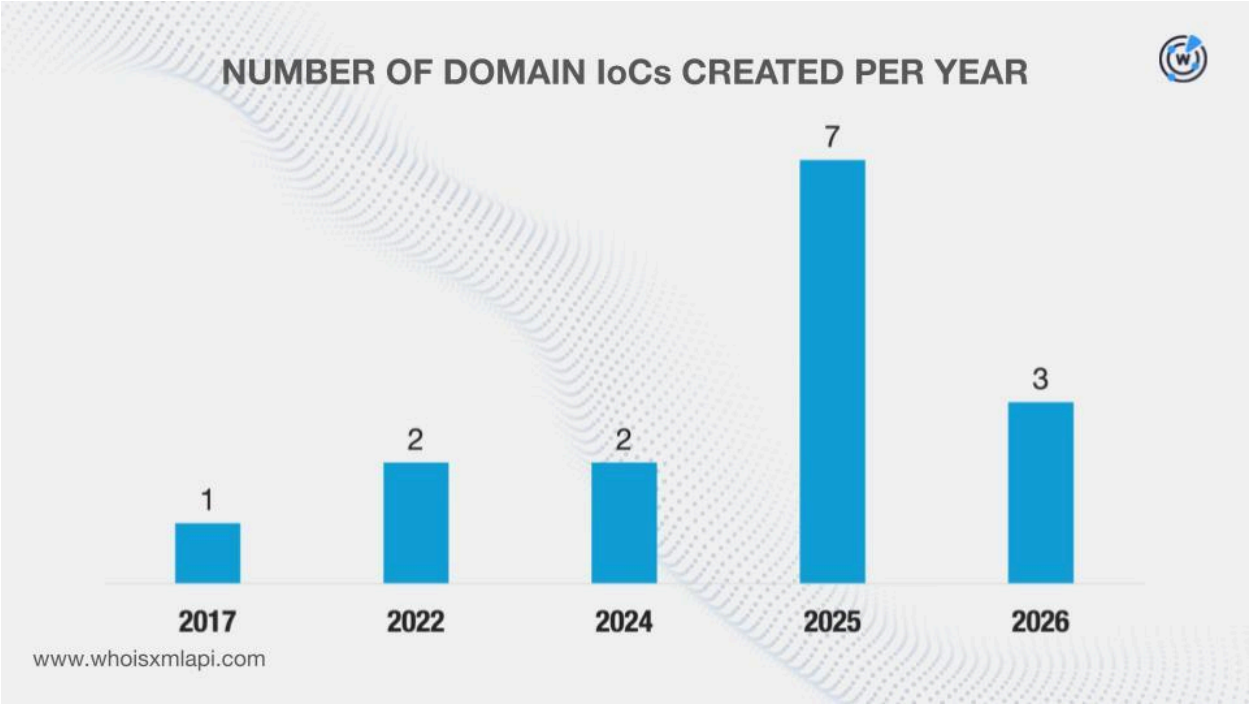

We then queried the domain IoCs on Typosquatting API and discovered that one—crypto-stroe[.]cc—was bulk-registered with two look-alikes—crypto-stroe[.]top and crypto-stroe[.]cn—on 9 September 2025.



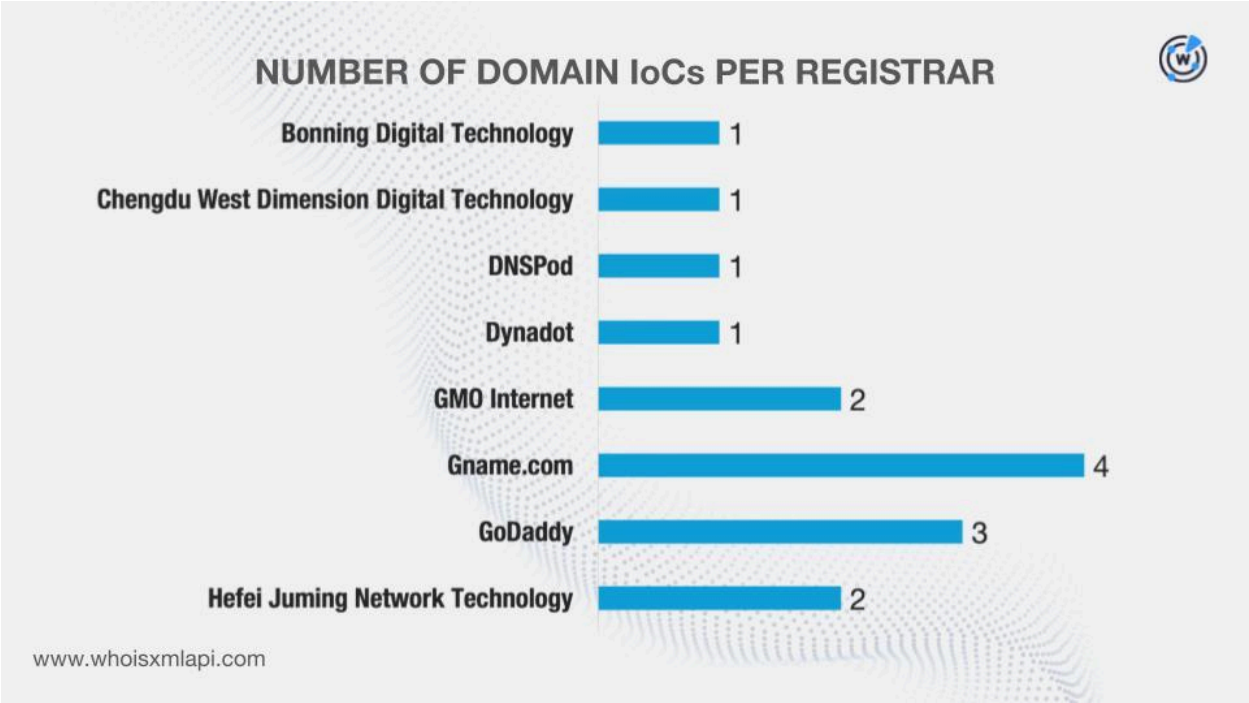

Next, we learned that two domain IoCs were likely registered with malicious intent. The domains gxzhrc[.]cn and jhxrpbgq[.]com were recorded on the First Watch Malicious Domains Data Feed 539 and 47 days, respectively, before they were dubbed as IoCs on 20 April 2026.

We then queried the domain IoCs on WHOIS API and filled in current WHOIS record detail gaps with the help of Domain Info API. We found out that:

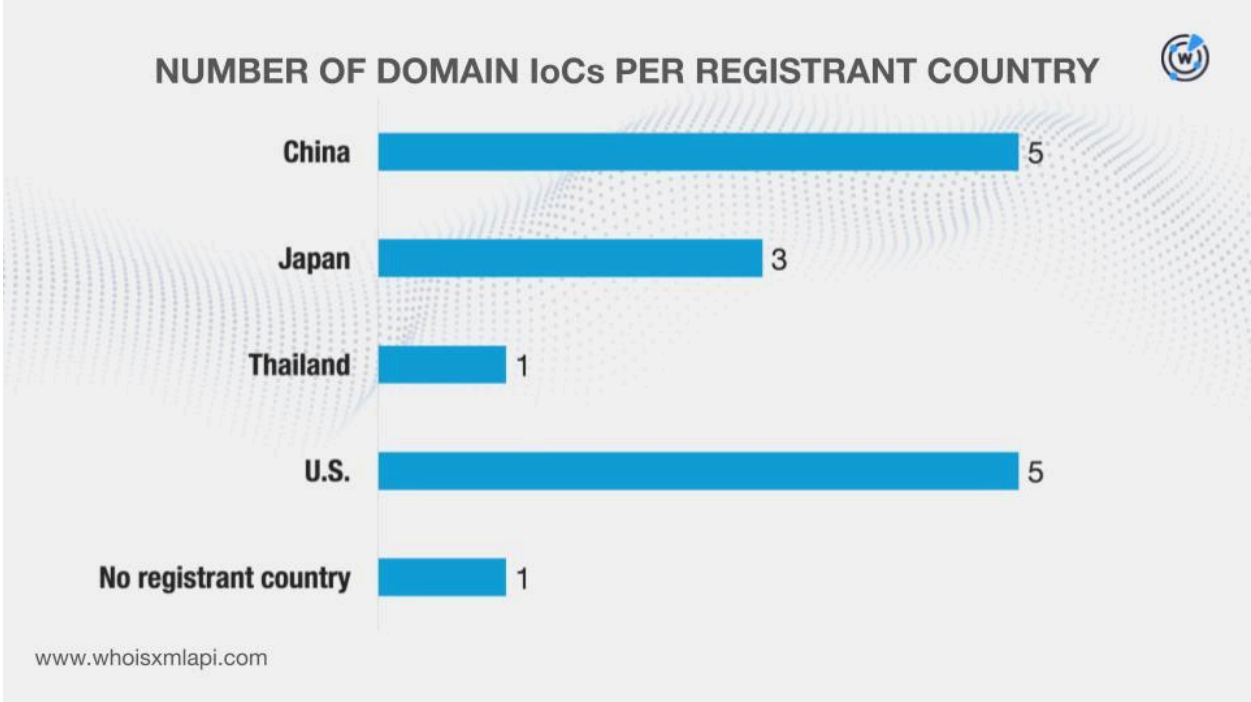
- They were created between 11 November 2017 and 23 March 2026.




- They were administered by eight different registrars.




- While one domain did not have a registrant country on record, the remaining 14 were registered in four different countries.




Finally, we queried the domain IoCs on DNS Chronicle API and discovered that 12 posted 258 historical domain-to-IP resolutions over time. Take a look at specifics for five domains below.

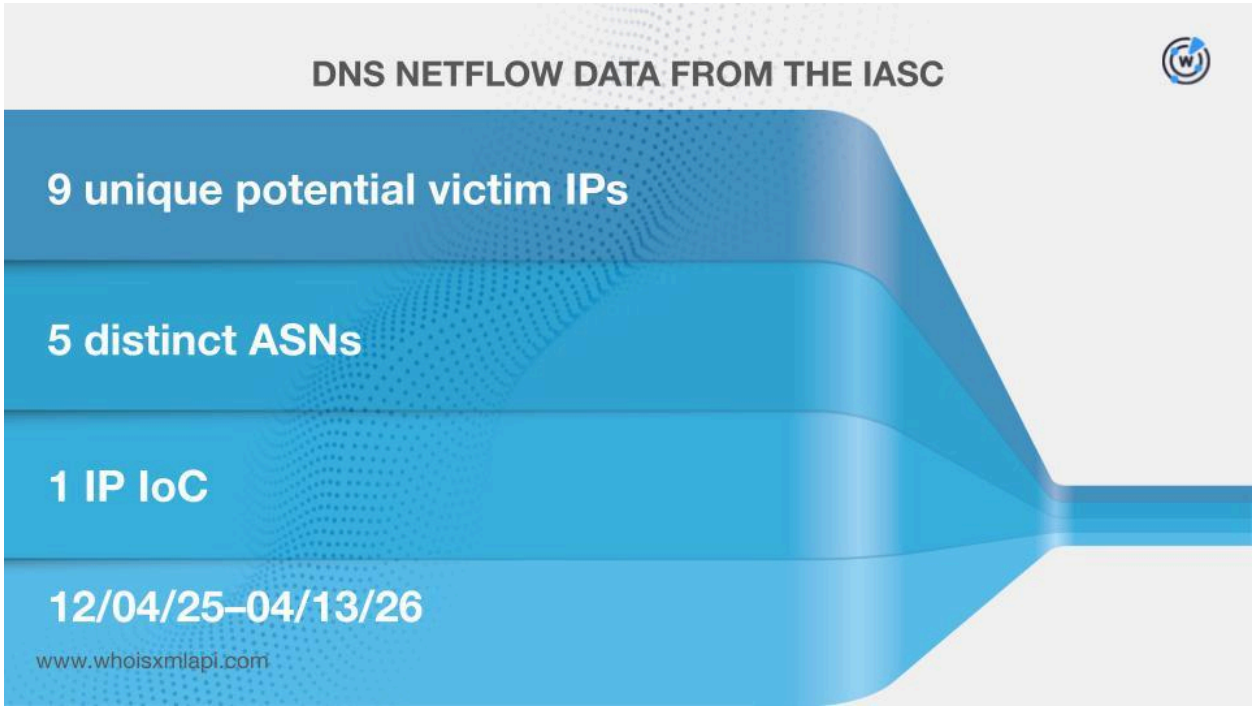
| DOMAIN IoC | NUMBER OF DOMAIN-TO-IP RESOLUTIONS | DATES SEEN |
|---|---|---|
| iosfc[.]com | 103 | 11/23/19–04/21/26 |
| siyangoil[.]com | 27 | 11/03/22–08/24/25 |
| kkkhhhnnn[.]com | 23 | 06/29/25–04/09/26 |
| sxsfcc[.]com | 22 | 11/15/19–04/12/25 |
| yjzhengruol[.]com | 19 | 01/28/25–06/17/25 |

Overall, the 12 domain IoCs with historical domain-to-IP resolutions posted the oldest resolution on 15 November 2019.

## FakeWallet IP IoCs Investigated

After that, we investigated the sole IP IoC further.

First, sample network traffic data from the IASC showed that nine unique IP addresses owned by potential victims under five distinct ASNs communicated with the IP address between 4 December 2025 and 13 April 2026.




We then queried the sole IP IoC on IP Geolocation API and learned that it was geolocated in Singapore under the purview of The Constant Company.

A DNS Chronicle API query for the IP IoC, meanwhile, revealed that it has recorded 114 historical IP-to-domain resolutions between 8 October 2019 and 22 March 2026.

## Fresh FakeWallet Artifacts Found

After learning more about the IoCs identified so far, we then hunted for new artifacts.

We began by querying the 15 domain IoCs on WHOIS History API. We uncovered 19 unique email addresses from their historical WHOIS records. Upon further scrutiny, we learned that nine were public email addresses.

Reverse WHOIS API queries for the public email addresses revealed that two could belong to domainers hence their exclusion from the next part of our analysis. The remaining seven public email addresses were used to register 10,812 unique email-connected domains after those already tagged as IoCs were filtered out.

According to the results of our Threat Intelligence API queries for the email-connected domains, 11 have already been weaponized for various malicious campaigns. Here are more details on five of them.

| MALICIOUS EMAIL-CONNECTED DOMAIN | ASSOCIATED THREAT | DATES SEEN |
|---|---|---|
| bitpiecn[.]com[.]cn | Malware distribution | 03/09/23–04/25/26 |
| ld018[.]com | Malware distribution | 02/25/25–04/27/26 |
| meta-mask[.]org[.]cn | Malware distribution | 03/09/23–04/27/26 |
| one-key[.]org[.]cn | Malware distribution | 03/09/23–04/27/26 |
| t0kenpocket[.]cn | Malware distribution | 03/09/23–04/27/26 |

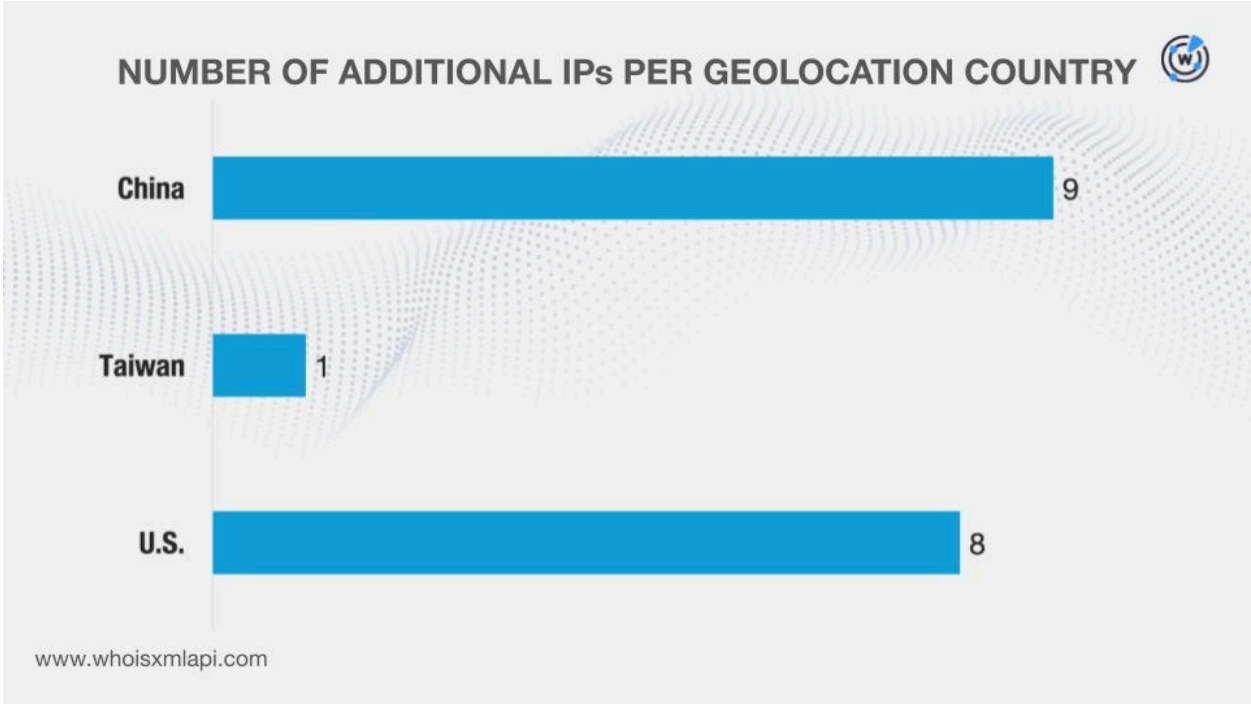
Next, we queried the domain IoCs on DNS Lookup API and discovered 18 additional IP addresses after the sole IP IoC was filtered out.

Threat Intelligence API queries for the additional IP addresses showed that eight have already figured in various attacks. Here are five examples.

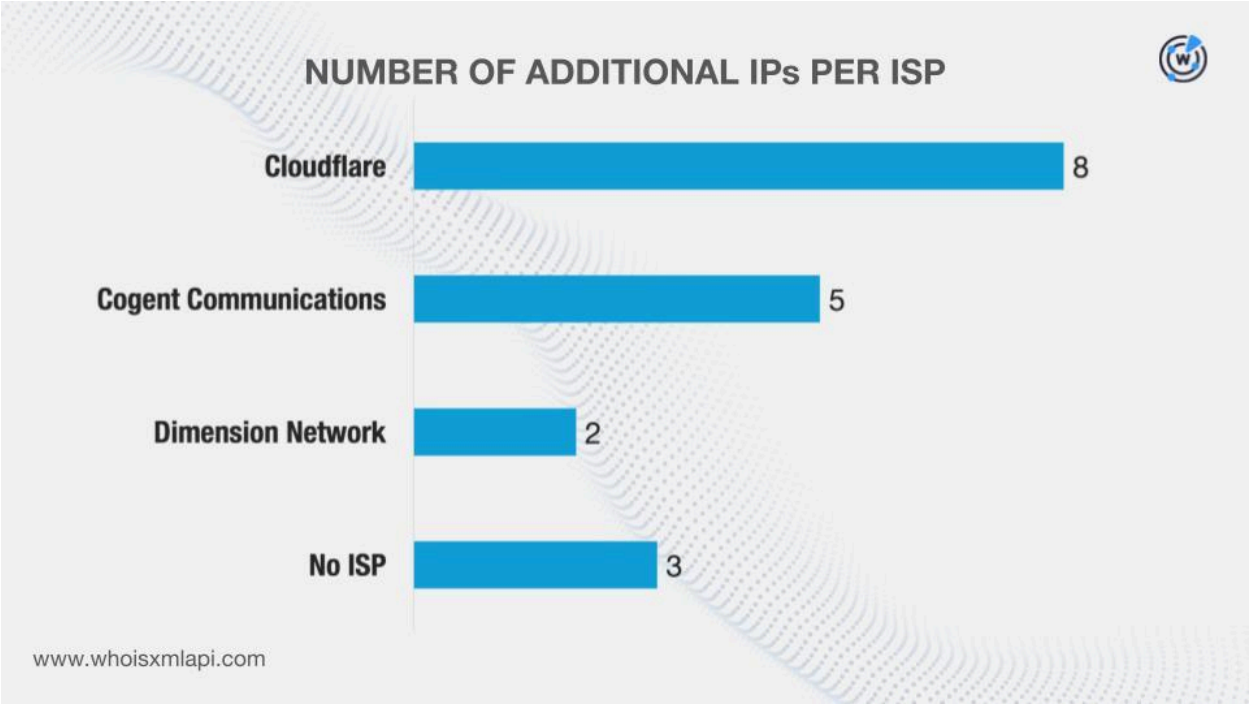
| MALICIOUS ADDITIONAL IP ADDRESS | ASSOCIATED THREAT | DATES SEEN |
|---|---|---|
| 104[.]21[.]42[.]187 | Malware distribution<br>Phishing | 03/30/23–04/27/26<br>05/21/23–04/12/26 |
| 172[.]67[.]208[.]92 | Malware distribution<br>Phishing | 03/30/23–04/27/26<br>05/21/23–04/12/26 |
| 104[.]26[.]4[.]170 | Malware distribution | 04/23/26–04/26/26 |
| 104[.]26[.]5[.]170 | Malware distribution | 04/23/26–04/26/26 |
| 104[.]26[.]8[.]38 | Malware distribution | 04/23/26–04/26/26 |

After that, we sought additional information about the additional IP addresses using Bulk IP Geolocation Lookup and found out that:

- They were geolocated in three different countries, none of which was the same as that of the sole IP IoC.




- While three did not have ISPs on record, the remaining 15 were administered by three different ISPs, again none of which were the sole IP IoC's ISP.




We then continued with our hunt for new artifacts with 19 IP addresses on hand—one IP IoC and 18 additional ones.

Reverse IP API queries for the IP addresses revealed that seven could be dedicated hosts. Together, they hosted eight unique IP-connected domains after those already named as IoCs and the email-connected domains were filtered out.

Next, we extracted unique text strings from the domain IoCs. We queried them on Domains & Subdomains Discovery and learned that these nine were seen at the start of other domains:

- ahroar.
- appstoreios.
- crypto-stroe.
- dc1637.
- gxzhrc.
- iosfc.
- kkkhhhnnn.
- lahuafa.
- ulbcl.

In sum, we unearthed 17 unique string-connected domains.

Note that the string-connected domains only serve to reflect the overall popularity of the strings extracted from the IoCs. As such, determining their legitimacy may require further investigation.

## The Final Word on FakeWallet

Our analysis of the FakeWallet campaign revealed that one client IP address communicated with three of the domain IoCs. One domain IoC was bulk-registered with two look-alikes while two domain IoCs were likely registered with malicious intent. In addition, nine potential victim IP addresses communicated with the sole IP IoC.

We also uncovered 10,855 new artifacts that could be tied to the threat. This number comprised 10,812 email-connected domains, 18 additional IP addresses, eight IP-connected domains, and 17 string-connected domains. Of these, 19 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

- 000lj[.]com
- 000zw[.]com
- 001cdn[.]com
- a-hong[.]com
- a-vip[.]cn
- a1a5[.]cn
- b0mr[.]cn
- b1sx[.]cn
- b2bfabu[.]com
- c-bago[.]com
- c11media[.]com
- c25kt[.]cn
- d-ones[.]com
- d46×25[.]com
- d68618[.]com
- e-colab[.]com
- e-driving[.]com[.]cn
- e-j-p[.]com
- f0530[.]com
- f0539[.]com
- f0633[.]com
- g3d-app[.]com[.]cn
- g516r[.]com
- g5way[.]com
- h3d97[.]cn
- h4nkn[.]cn
- h530y[.]cn
- i-azure[.]com
- i-cec[.]com[.]cn
- i-jj[.]cn
- j-yif[.]com
- j2t9[.]cn
- j6zp[.]cn
- k1home[.]com
- k400y[.]cn
- k4rh[.]cn
- l-sung[.]com
- l0622[.]com
- l3kj[.]cn
- m08888[.]com
- m1820[.]com
- m22275[.]cn
- n-i-a[.]com
- n-i-z[.]com
- n-v-n[.]com
- o-roman[.]com
- o4506[.]com
- o4an[.]cn
- p1wu[.]cn
- p21247[.]cn
- p2k870[.]cn
- q07gs[.]com
- q235dxgg[.]com
- q7789[.]com
- r15y[.]cn
- ra207[.]com
- raazweb23[.]com
- s-ajand[.]com
- s-touroku[.]com
- s0l4re[.]com
- t-jia[.]com
- t-mag[.]cn
- t03gx9[.]com
- u-ad-me[.]com
- u11fl[.]com
- u7b6[.]cn
- v-v-t[.]com
- v0728[.]cn
- v0a9[.]cn
- w-links[.]com
- w12sq[.]cn
- w2vo[.]cn
- x-dosug[.]com
- x-jia[.]cn

- x-jiang[.]com
- y06yb[.]cn
- y13qam[.]com
- y2ezslb[.]cn
- z-argus[.]cn
- z24r[.]cn
- z27399z[.]com

## Sample Additional IP Addresses

- 104[.]21[.]42[.]187
- 154[.]38[.]242[.]10
- 172[.]67[.]208[.]92
- 206[.]119[.]188[.]101
- 223[.]26[.]11[.]141
- 43[.]169[.]13[.]10

## Sample IP-Connected Domains

- 4g-app[.]com
- fewzg6dx[.]n[.]xmocloud01[.]com
- gc50-site-02[.]gocname[.]com
- hengshenzhenquan[.]online
- tm[.]vip[.]fastestgmt[.]com
- wqtab3sx[.]n[.]xmocloud01[.]com

## Sample String-Connected Domains

- ahroar[.]cn
- appstoreios[.]tk
- crypto-stroe[.]cn
- dc1637[.]com
- gxzhrc[.]com
- iosfc[.]cn
- kkkhhhnnn[.]shop
- lahuafa[.]cn
- ulbcl[.]cn