A Deep Dive into the GreedyBear Attack

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts

Executive Report

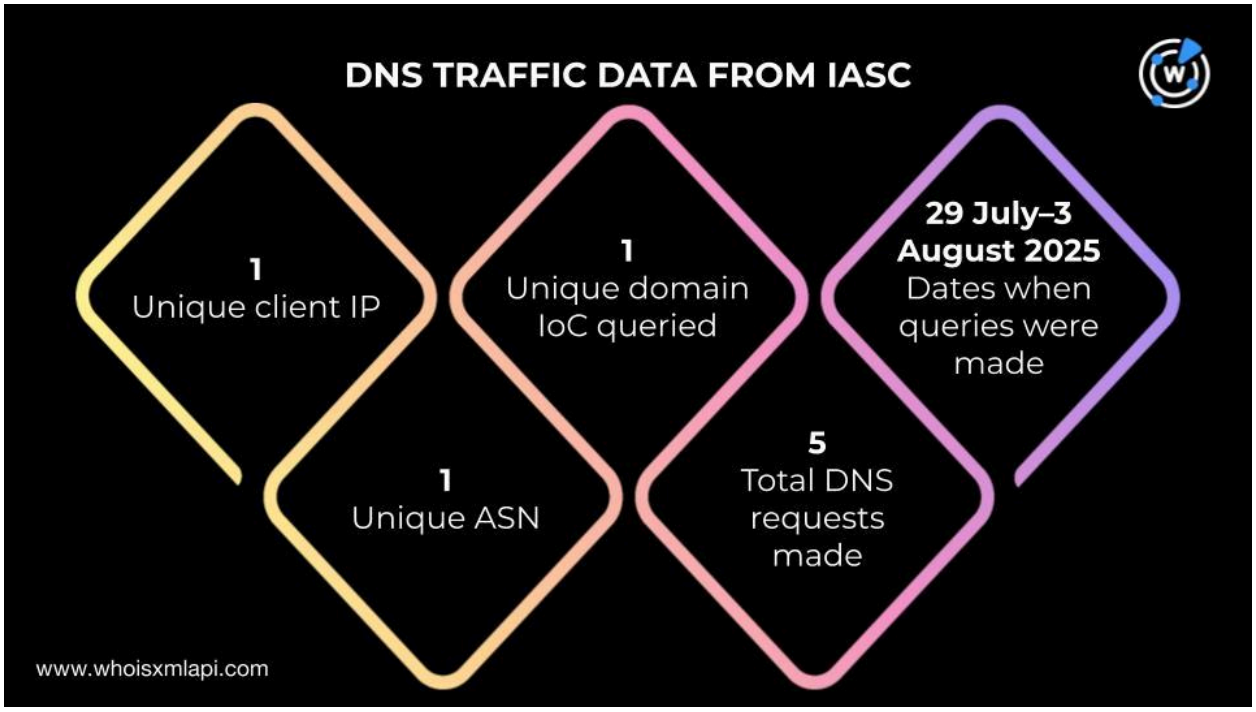
Koi Security recently dove into the widely executed and highly coordinated GreedyBear crypto theft attack that used 150 weaponized Firefox extensions. According to the company, it utilized close to 500 malicious executables and dozens of phishing sites. The result? The threat actors have amassed more than US$1 million to date.

The company identified 18 domains as indicators of compromise (IoCs) in "GreedyBear: 650 Attack Tools, One Coordinated Campaign." WhoisXML API dove deeper into the attack in a bid to uncover more information and new artifacts. Our in-depth analysis of the IoCs led to these discoveries:

- One unique client IP address communicated with one unique domain identified as an IoC based on sample DNS traffic data from the Internet Abuse Signal Collective (IASC)
- Five domain IoCs deemed likely to turn malicious 33–82 days before they were dubbed as such on 8 August 2025
- One email-connected domain
- Four IP addresses, three were malicious
- 11 IP-connected domains
- 607 string-connected domains, five were malicious

More on the GreedyBear IoCs

Sample DNS data obtained from IASC revealed that one unique client IP address under one unique Autonomous System number (ASN) communicated with one domain identified as an IoC via five DNS queries made between 29 July and 3 August 2025.

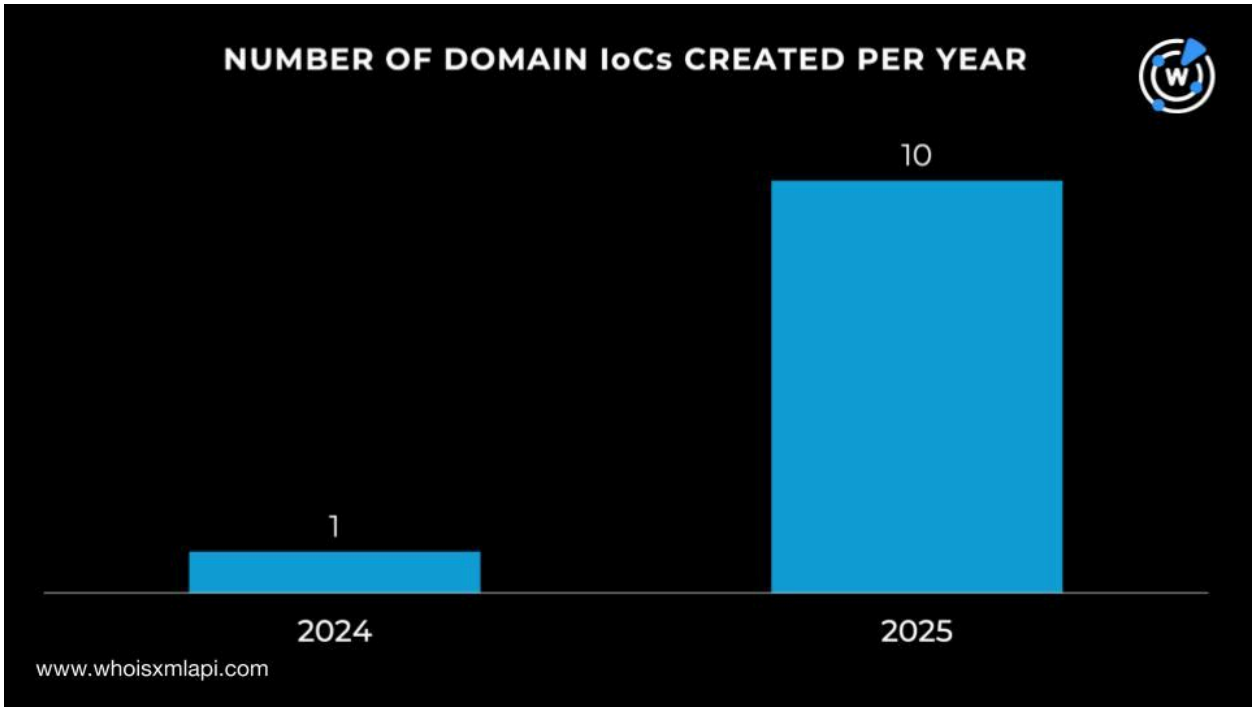


Meanwhile, First Watch Malicious Domains Data Feed files dated 18 May–6 July 2025 revealed that five domain IoCs were deemed likely to turn malicious 33–82 days before they were dubbed as IoCs on 8 August 2025. Take a look at more details below.

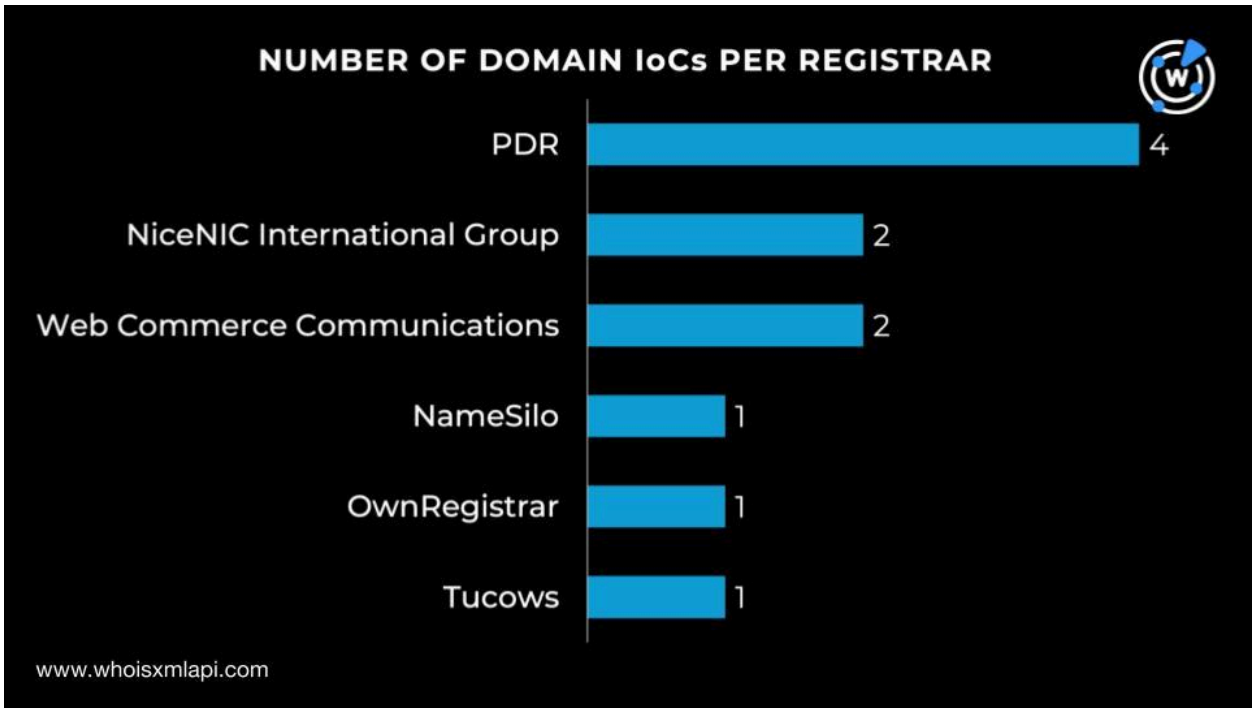
DOMAIN IoC	DATE ADDED TO FIRST WATCH	NUMBER OF DAYS PRIOR TO REPORTING DATE
extprojectdev[.]top	18 May 2025	82
suirokboys[.]digital	4 June 2025	65
metahoper[.]digital	11 June 2025	58

Now, on to a closer look at the WHOIS records of the 18 domains identified as IoCs. We queried them on Bulk WHOIS API and found out that:

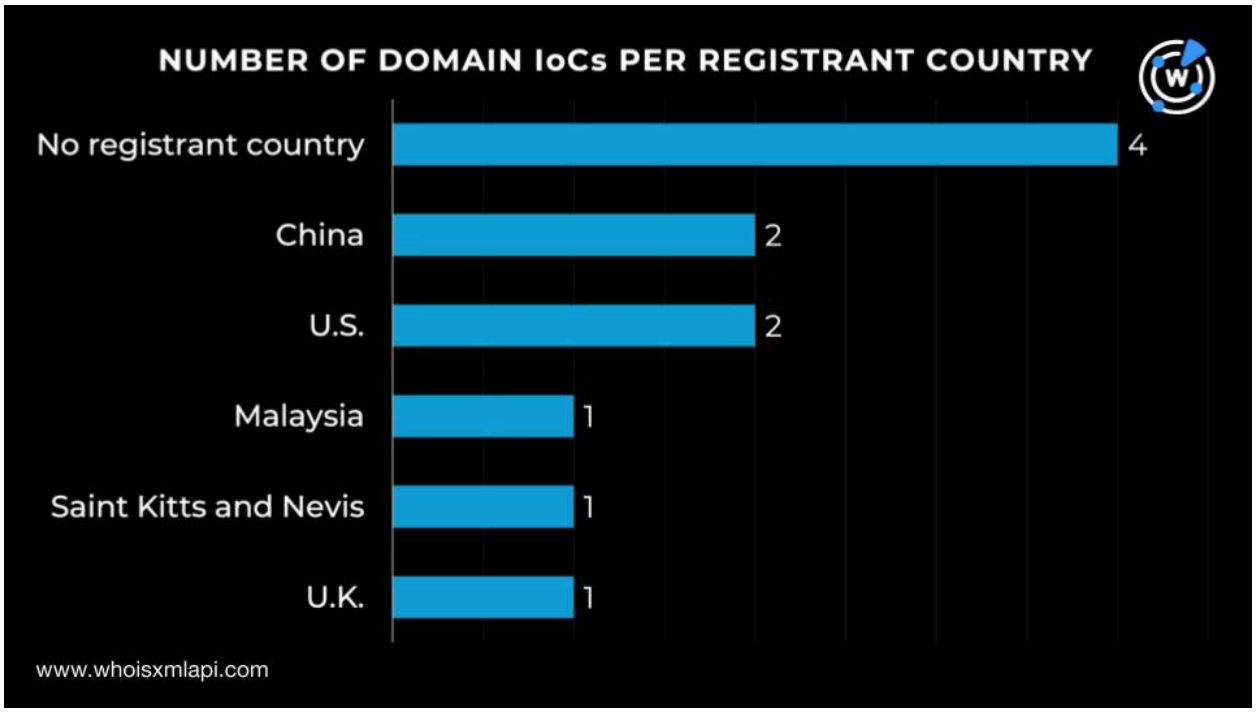
- Only 11 of the 18 domains had current WHOIS records.
- A majority of the 11 domains with current WHOIS records, 10 to be exact, were newly created, just this 2025. One domain, meanwhile, was created in 2024.



- The 11 active domains were administered by six different registrars led by PDR, which accounted for four IoCs. Two domains each, meanwhile, were registered with NiceNIC International Group and Web Commerce Communications. Finally, one domain each was handled by NameSilo, OwnRegistrar, and Tucows.



- While four of the 11 domains with current WHOIS records did not have registrant countries on record, the remaining seven were registered in five different countries. China and the U.S. led the pack of countries, accounting for two IoCs each. Finally, Malaysia, Saint Kitts and Nevis, and the U.K. accounted for one each.



After that, we took a closer look at the DNS histories of the 18 domains identified as IoCs. DNS Chronicle API showed that 13 had 255 domain-to-IP resolutions over time. The IoC snipersol[.]com recorded 178 resolutions from 29 April 2017 to date. Take a look at the DNS histories of five other domains below.

DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	FIRST DOMAIN-TO-IP RESOLUTION DATE
ventroxibnk[.]com	28	24 June 2025
trezor-wallet[.]io	19	1 December 2018
filecoinwallet[.]net	9	19 November 2021
avalancheproject[.]digital	5	10 April 2025
exodlinkbase[.]digital	4	12 June 2025

We further zoomed in on the domain trezor-wallet[.]io, which could be riding on the popularity of legitimate domain trezor[.]io via the WhoisXML API MCP Server. The prompt “find all assets connected to trezor-wallet[.]io” revealed these interesting nuggets:

- A warning saying the site is currently associated with malware distribution appeared as the initial finding. It currently resolves to the IP address 185[.]208[.]156[.]66.

⚠ SECURITY WARNING

trezor-wallet.io has been flagged as MALWARE by threat intelligence systems (first seen: 2025-08-09, last seen: 2025-09-03).

Domain Information

- **Created**: July 18, 2025 (recently registered - ~47 days old)
- **Registrar**: NICENIC INTERNATIONAL GROUP CO., LIMITED
- **Nameservers**: Cloudflare (ns1.cloudflare.com, ns2.cloudflare.com)
- **IP Address**: 185.208.156.66
- **Status**: Multiple protective holds (serverHold, clientDeleteProhibited, etc.)

- The site has 45 subdomains, many of which were crypto wallet-related. The subdomains were, however, suspicious in that they could be mimicking the names of other popular wallets.

Connected Subdomains (45 total)

The domain has extensive suspicious subdomain infrastructure including:

Wallet-related subdomains:

- keepkeys.co.trezor-wallet.io
- wallet-secure.io.trezor-wallet.io
- secure-wallets.co.com.trezor-wallet.io
- hardware-wallet.co.com.trezor-wallet.io

Suspicious patterns suggesting phishing/malware infrastructure:

- Multiple "co.com" and similar deceptive patterns
- Names mimicking legitimate services (jupiterwallet, securestorage, safelink)
- www variants of suspicious subdomains

The Search for GreedyBear-Connected Artifacts

We began our search for new artifacts by querying the 18 domains identified as IoCs on WHOIS History API. Three of them had email addresses in their historical WHOIS records. Specifically, three IoCs had nine unique email addresses, one of which was public.

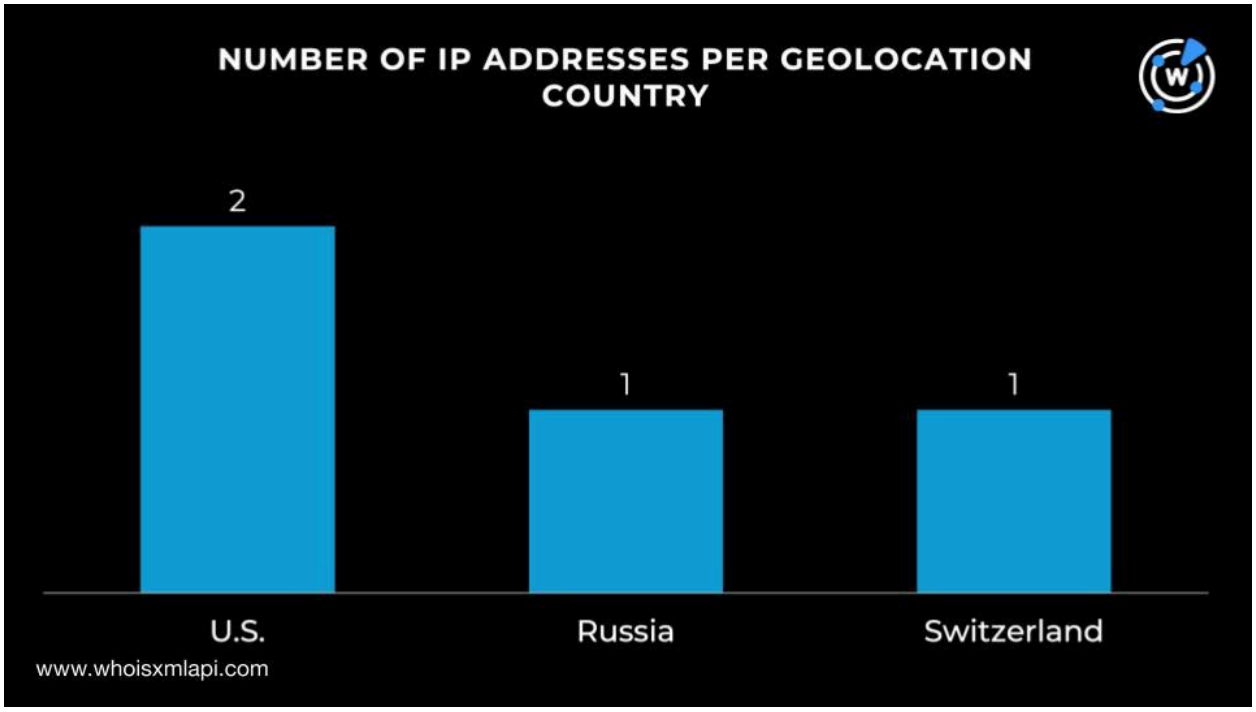
A Reverse WHOIS API query for the public email address enabled us to uncover one email-connected domain—bonkpunk[.]com—after duplicates and those already identified as IoCs were filtered out.

Next, we queried the 18 domains identified as IoCs on DNS Lookup API and discovered that 10 actively resolved to four unique IP addresses.

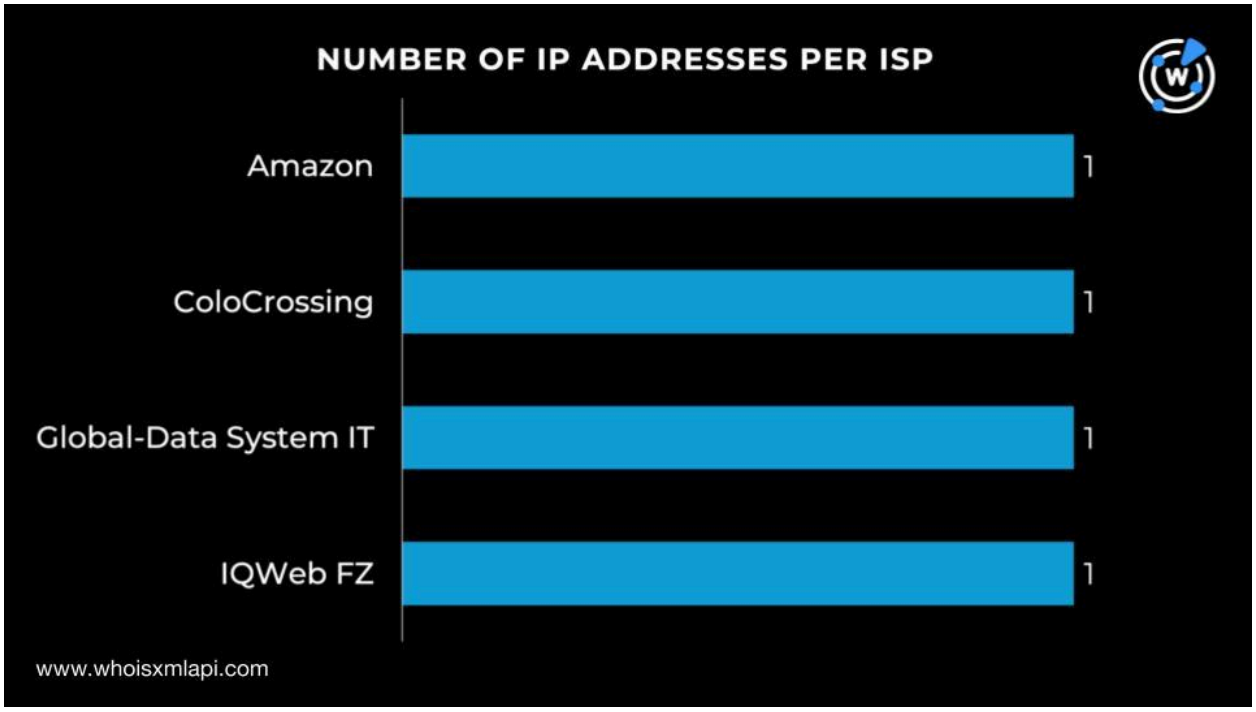
A Threat Intelligence API query for the four IP addresses showed that three have already been weaponized for various attacks. An example would be 76[.]76[.]21[.]21, which was associated with phishing, generic threats, malware distribution, suspicious activity, command and control (C&C), and attacks.

Next, we queried the four IP addresses on Bulk IP Geolocation Lookup and found out that:

- They were geolocated in three different countries led by the U.S., which accounted for two IP addresses. One IP address each, meanwhile, was geolocated in Russia and Switzerland.



- The four IP addresses were administered by four different ISPs. One IP address each was handled by Amazon, ColoCrossing, Global-Data System IT, and IQWeb FZ.



A Reverse IP API query for the four IP addresses revealed that only one could be a dedicated host. Specifically, the dedicated IP address 190[.]115[.]30[.]145 hosted 11 domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

Next, we further scrutinized the 18 domains identified as IoCs and discovered that they started with 18 unique text strings. Domains & Subdomains Discovery searches showed that only 10 of the strings listed below, however, appeared in 607 other domains after duplicates, those already tagged as IoCs, and the email- and IP-connected domains were filtered out.

- avalancheproject.
- connects.
- filecoinwallet.
- jub.
- secure-wallets.
- snipersol.
- suinetwork.
- teaser.
- trezor-wallet.
- tweser.

Finally, a Threat Intelligence API query for the 607 string-connected domains enabled us to discern that five have already been weaponized for various attacks. Here are three examples.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREATS
jub[.]cc	Malware distribution
teaser[.]dating	Suspicious activity
trezor-wallet[.]co	Phishing

—

Our deep dive into the GreedyBear attack enabled us to determine that one unique client IP address under one unique ASN queried one unique domain identified as an IoC via five DNS queries made between 29 July and 3 August 2025. First Watch also showed that five domains identified as IoCs were deemed likely to turn malicious 33–82 days before they were dubbed as such on 8 August 2025.

In addition, our expansion analysis of the 18 domains identified as IoCs unearthed 623 new artifacts comprising one email-connected domain, four IP addresses, 11 IP-connected domains, and 607 string-connected domains. We also found out that eight of the newly discovered artifacts have already figured in 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 IP Addresses

- 107[.]172[.]61[.]186
- 185[.]208[.]156[.]66
- 190[.]115[.]30[.]145

Sample IP-Connected Domains

- cpanel[.]proexchangeltd[.]com
- ftp[.]proexchangeltd[.]com
- localhost[.]proexchangeltd[.]com
- mail[.]proexchangeltd[.]com
- pop[.]proexchangeltd[.]com

Sample String-Connected Domains

- avalancheproject[.]com
- avalancheproject[.]eu
- avalancheproject[.]net
- connects[.]ae
- connects[.]aero
- connects[.]africa
- filecoinwallet[.]app
- filecoinwallet[.]cn
- filecoinwallet[.]com
- jub[.]aero
- jub[.]ag
- jub[.]ai
- secure-wallets[.]co
- secure-wallets[.]co[.]uk
- secure-wallets[.]com
- snipersol[.]app
- snipersol[.]dev
- snipersol[.]life
- suinetwork[.]app
- suinetwork[.]cc
- suinetwork[.]cn
- teaser[.]agency
- teaser[.]ai
- teaser[.]amsterdam
- trezor-wallet[.]app
- trezor-wallet[.]at
- trezor-wallet[.]biz
- tweser[.]com