Baring the DNS Traces of the Slow Pisces Attack on Cryptocurrency Developers

Table of Contents

Executive Report

Palo Alto Unit 42 reported on the latest Slow Pisces attack that engaged with cryptocurrency developers on LinkedIn. The threat actors posed as potential employers and sent malware disguised as coding challenges. Developers who took on the challenge ended up running a compromised project, infecting their systems with RN Loader and RN Stealer.

The report identified 54 indicators of compromise (IoCs) comprising 27 domains and 27 IP addresses, which WhoisXML API expanded. Our analysis led to the discovery of other potentially connected artifacts, namely:

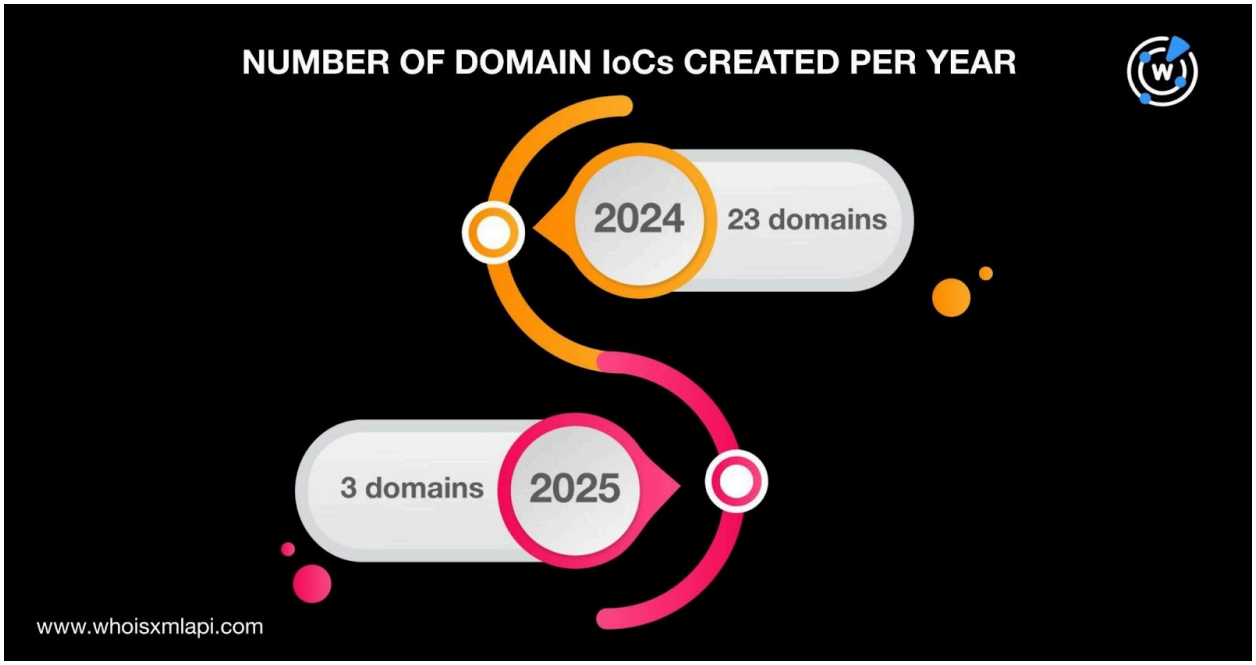
- 12 alleged victim IP records obtained from the Internet Abuse Signal Collective (IASC) tied to five Autonomous System numbers (ASNs)
- 551 email-connected domains
- One additional IP address that turned out to be malicious
- 179 IP-connected domains
- 389 string-connected domains, three of which turned out to be malicious

A Closer Look at the Slow Pisces IoCs

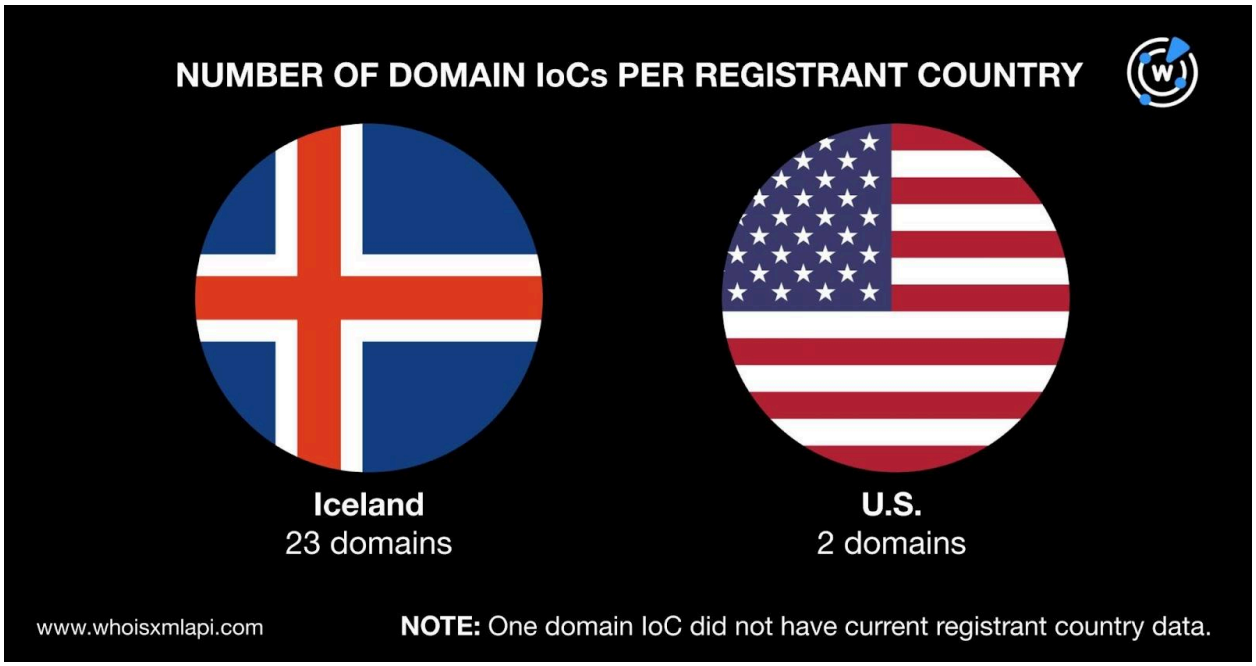
Our threat investigation began with a deep dive into the 54 IoCs Palo Alto Unit 42 identified.

We started by querying the 27 domains identified as IoCs on Bulk WHOIS API, which revealed that only 26 of them had current WHOIS records. We also found that:

- The 26 domains with current WHOIS records were created between 2024 and 2025. Specifically, 23 were created in 2024 while three were created in 2025.



- The 26 domains were all administered by Namecheap.
- While one of the 26 domains did not have a registrant country on record, the 25 remaining ones were split between two countries. Specifically, 23 domains were registered in Iceland while two were registered in the U.S.



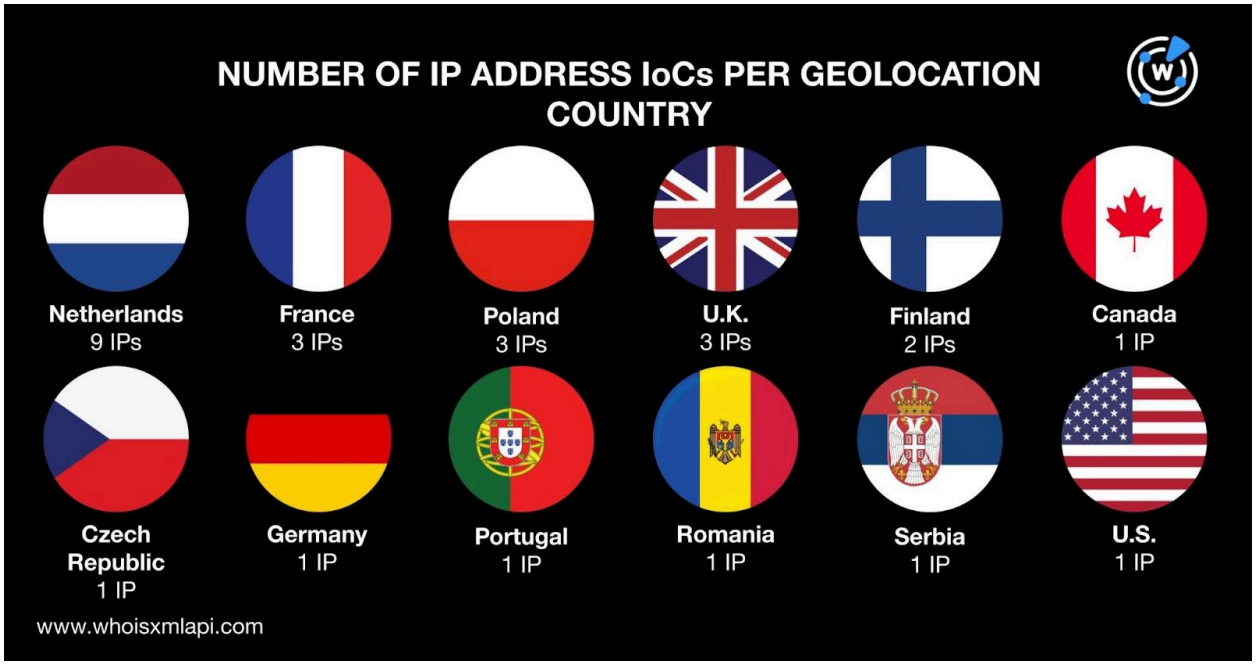
We then queried the 27 domains identified as IoCs on DNS Chronicle API and found that 24 of them had historical domain-to-IP address resolutions. The 24 domains had 239 IP resolutions over time. The domain leaguehub[.]net with 67 resolutions in all, in particular, recorded the oldest resolution date, that is, 6 February 2017. Take a look at more details for five other domains below.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST IP RESOLUTION DATE
bitzone[.]io	30	6 June 2020
coinhar[.]io	1	27 March 2025
getstockprice[.]info	1	8 January 2025
logoeye[.]net	1	9 October 2024
stocksindex[.]org	16	7 February 2017

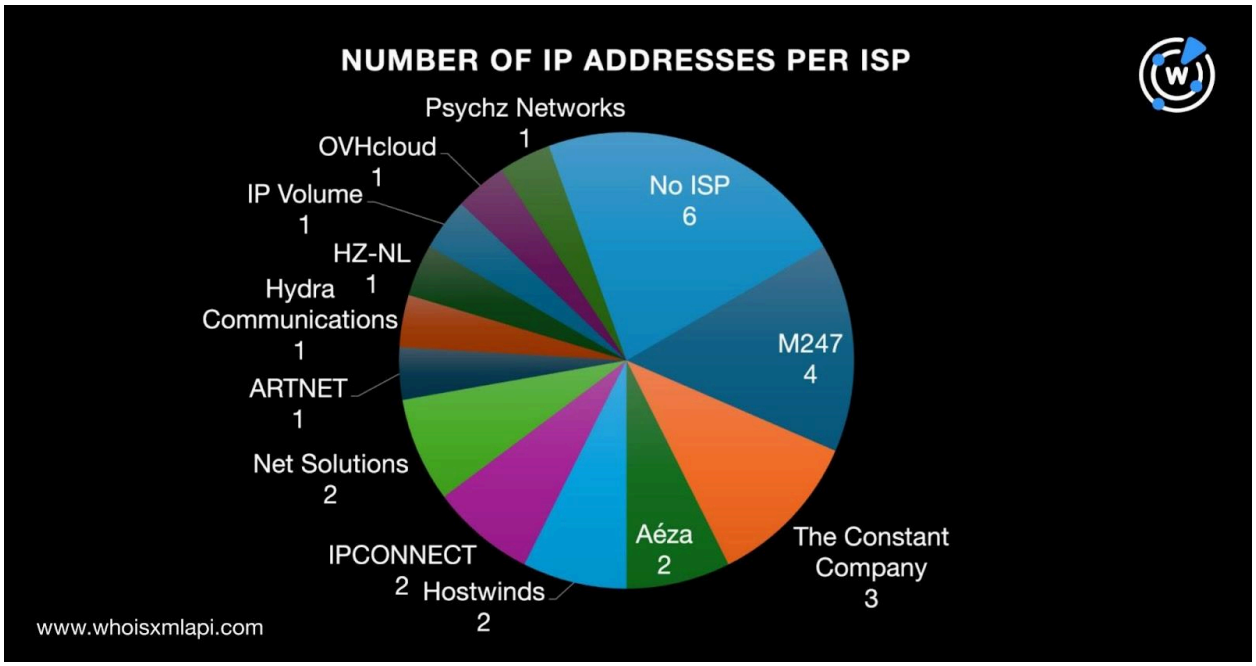
Considering that bitzone[.]io was created on 25 April 2024 but first resolved to an IP address on 6 June 2020, it may have been recently reregistered. The same is true for stocksindex[.]org, which was created on 11 September 2024 but first resolved to an IP address on 7 February 2017.

Next, we queried the 27 IP addresses identified as IoCs on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in 12 countries led by the Netherlands, which accounted for nine IP addresses. Three IP addresses each originated from France, Poland, and the U.K. Finland accounted for two IP addresses. Finally, one IP address each was geolocated in Canada, the Czech Republic, Germany, Portugal, Romania, Serbia, and the U.S.



- Only 21 of the 27 IP addresses had ISPs on record. Specifically, four IP addresses were administered by M247. The Constant Company administered three IP addresses while Aéza, Hostwinds, IPCONNECT, and Net Solutions administered two each. Finally, one IP address each was administered by ARTNET, Hydra Communications, HZ-NL, IP Volume, OVHcloud, and Psychz Networks.



A DNS Chronicle API query for the 27 IP addresses identified as IoCs revealed that 22 of them had historical IP address-to-domain resolutions. Specifically, the 22 IP addresses recorded 2,011 resolutions over time. The IP address 54[.]39[.]83[.]151 with 239 resolutions had the oldest resolution date, that is, 17 October 2019. Take a look at additional details for five other IP addresses below.

IP ADDRESS IoC	NUMBER OF RESOLUTIONS	FIRST DOMAIN RESOLUTION DATE
185[.]62[.]58[.]74	678	18 April 2020
195[.]133[.]26[.]32	14	19 November 2021
5[.]206[.]227[.]51	227	29 May 2020
91[.]193[.]18[.]201	28	28 January 2022
91[.]234[.]199[.]90	139	24 January 2023

In addition, using sample netflow data our researchers obtained from the IASC, we further analyzed three IP addresses. They served as command-and-control (C&C) IP addresses related to the threat. The sample data revealed 12 alleged victim IP records associated with four ISPs operating under five ASNs according to an additional Bulk IP Geolocation Lookup query.

The IP address IoC 91[.]103[.]140[.]191 proved most interesting in that it sent data to a potential victim IP 10 times and received data from that victim IP seven times for almost four weeks. The source IP 91[.]103[.]140[.]191 also most frequently communicated via port 443 (HTTPS) in our data sample.

Expanding the List of Slow Pisces IoCs

We began our IoC list expansion analysis by querying the 27 domains identified as IoCs on WHOIS History API. That enabled us to determine that 11 of them had 44 email addresses in their historical WHOIS records after duplicates were filtered out. Further scrutiny of the 44 email addresses revealed that seven were public email addresses.

Next, we queried the seven public email addresses on Reverse WHOIS API and found that while none of them appeared in any domain's current WHOIS record, six of them were present in the historical WHOIS records of several domains. Specifically, the six public email addresses led to the discovery of 551 email-connected domains after duplicates and those identified as IoCs were filtered out.

We then queried the 27 domains identified as IoCs on DNS Lookup API and found that eight of them actively resolved to IP addresses. A comparison of the results with the 27 IP addresses identified as IoCs and the removal of duplicates, however, left us with only one additional IP address—199[.]59[.]243[.]228.

A Threat Intelligence API query for the sole additional IP address revealed that it was associated with various threats, namely, attacks, C&C, generic threats, malware distribution, phishing, and suspicious activities.

An IP Geolocation API query for the additional IP address showed that it was geolocated in the U.S. and administered by Amazon.

We now had 28 IP addresses for further analysis. Querying them on Reverse IP API showed that 14 of them resolved to domains. A closer look at the results also revealed that 13 could be dedicated hosts. The 13 potentially dedicated IP addresses hosted 179 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

As a final step, we searched the DNS for other potentially connected domains. A closer look at the 27 domains identified as IoCs revealed 26 unique text strings. We used them as search terms on Domains & Subdomains Discovery and found that only 21 strings appeared at the beginning of other domains. These strings were:

- bitzone.
- blockprices.
- clubinfo.
- clublogos.
- coinhar.
- coinpricehub.
- ethzone.
- fivebit.
- indobit.
- jquerycloud.
- leaguehub.
- logoeye.
- logosports.
- skypredict.
- soccerlab.
- stockinfo.
- stocksindex.
- stockslab.
- thaibit.
- weatherdatahub.
- wfinance.

Our searches turned up 389 string-connected domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

A Threat Intelligence API query for the 389 string-connected domains showed that three of them were already associated with various threats. An example would be jquerycloud[.]com, which was associated with malware distribution.

—

Our IoC list expansion analysis for the Slow Pisces attack targeting cryptocurrency developers led to the discovery of 1,120 unreported connected artifacts. We specifically found 551 email-connected domains, one additional IP address, 179 IP-connected domains, and 389 string-connected domains. At present, only four of the connected artifacts we unearthed have already been weaponized for 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 Email-Connected Domains

- 0515dy[.]com
- 10i0[.]com
- 5jdm[.]com
- abam[.]science
- abam[.]webcam
- aboushokalawfirm[.]online
- babyuju[.]com
- bam114[.]com
- bammaster[.]com
- c163[.]net
- carsinsurers[.]com
- carsinsurers[.]net
- denverhighland[.]org
- dfckg[.]com
- dgbcapital[.]org
- eaahh[.]net
- earngb[.]com
- easybuy[.]london
- facekeek[.]com
- faceposts[.]net
- faceposts[.]org
- gayavatar[.]com
- glitted[.]com
- goddaz[.]com
- handleluxury[.]com
- haoxyw[.]net
- hatyaimte[.]com
- i-pu[.]net
- idoerr[.]com
- idoerr[.]net
- j6663[.]com
- jademother[.]com
- jaji[.]club
- kaalin[.]com
- kampkaos[.]com
- kazbau[.]com
- leafyzone[.]com
- liveboxes[.]com
- liveinrentals[.]com
- madamdent[.]com
- malim[.]net
- mcrqgs[.]com
- nakajam[.]com
- naverbam1[.]com
- naverbam18[.]com
- oacts[.]net
- oanma[.]com
- oladiy[.]com
- pickndrop[.]online
- pineprints[.]com
- plarket[.]com
- qatar2022news[.]org
- qatarfifa2022[.]org
- qiuf[.]net
- rayonbox[.]com
- rbbzz[.]net
- realanma[.]com
- sacsm[.]com
- samanafoods[.]com
- schedulefm[.]com
- tabbieshop[.]com
- teestyle[.]net
- teewish[.]com
- udaiso1[.]com
- udaiso33[.]com
- urxdeal[.]com
- vacationrentalz[.]net
- vacationrentalz[.]org
- vebila[.]com
- w-te[.]com
- web-33[.]com
- webdesignerskills[.]com

- xiebox[.]net
- xn--h43bo7b23h[.]net
- xzzh8[.]com
- yotoh[.]com
- yutam1[.]com
- yutam10[.]info
- zamsstar[.]com
- zepleen[.]com
- zevania[.]com

Sample IP-Connected Domains

- 0fob27ggjytxp4epa53n173jj4zeewpf5n07ny[.]genocide[.]xyz
- 315128182-878092767[.]netenyahu[.]org
- a90b5de2-e57f-42ba-a024-e7e41c655fcf[.]random[.]fetal-alcohol-syndrome[.]org
- aigoumall[.]shop
- b27aabff-4ecf-4d05-8fec-dac85a276d5b[.]random[.]genocide[.]xyz
- b7369857cf6a[.]random[.]thisisactivate[.]net
- cb9eeca1-e88c-4e7e-a134-38a4313a82e2[.]random[.]battyman[.]org
- clickuptools[.]com
- eliziba[.]shop
- f2770c15-768b-4513-80d7-a99ce88ee7d2[.]random[.]netenyahu[.]org
- f27aea85-cc67-42ce-a110-bcfd1ca4d425[.]random[.]thisisactivate[.]net
- globaldigital[.]trading
- goyim[.]net
- hoonhanggroup[.]pro
- howame[.]com
- imap[.]thisisactivate[.]net
- intercomcdn14[.]com
- l8kqx[.]genocide[.]xyz
- localhost[.]battyman[.]org
- m[.]clickuptools[.]com
- mail[.]battyman[.]org
- netenyahu[.]org
- niw2v[.]genocide[.]xyz
- owanso[.]xyz
- paco[.]clickuptools[.]com
- pop[.]battyman[.]org
- random[.]netenyahu[.]org
- random[.]thisisactivate[.]net
- simbabwe[.]shop
- sipexternal[.]thisisactivate[.]net
- thisisactivate[.]net
- truthwillsetyoufree[.]online
- vip-aigou[.]shop
- webdisk[.]battyman[.]org
- webdisk[.]clickuptools[.]com

Sample String-Connected Domains

- bitzone[.]app
- bitzone[.]asia
- blockprices[.]com
- clubinfo[.]app
- clubinfo[.]at
- clublogos[.]com
- clublogos[.]de
- coinhar[.]com
- coinpricehub[.]com
- ethzone[.]best
- ethzone[.]com
- fivebit[.]casa
- fivebit[.]cf
- indobit[.]academy
- indobit[.]club
- jquerycloud[.]com

- jquerycloud[.]host
- leaguehub[.]app
- leaguehub[.]co
- logoeye[.]cn
- logoeye[.]com
- logosports[.]biz
- logosports[.]ca
- skypredict[.]com
- skypredict[.]ph
- soccerlab[.]asia
- soccerlab[.]at
- stockinfo[.]ai
- stockinfo[.]app
- stocksindex[.]co[.]uk
- stocksindex[.]com
- stockslab[.]co
- stockslab[.]com
- thaibit[.]asia
- thaibit[.]biz
- weatherdatahub[.]com
- wfinance[.]adult
- wfinance[.]au