WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

ForceMemo in the DNS Spotlight

Threat Report

Table of Contents

Executive Report

StepSecurity recently uncovered and is continuously tracking the ForceMemo campaign targeting developers' GitHub accounts. The attackers reportedly injected the same malware into hundreds of Python repositories starting 8 March 2026.

The researchers identified several network IoCs related to the threat. We extracted domains from the subdomains tagged as IoCs and weeded out those that belonged to legitimate entities aided by the WhoisXML API MCP Server. In the end, we analyzed 20 IoCs comprising nine subdomains, five domains, and six IP addresses.

Our in-depth investigation of the IoCs led to these discoveries:

- One domain categorized as an IoC bulk-registered with 11 look-alike domains
- One domain named as an IoC was likely registered with malicious intent
- 86 email-connected domains found
- Nine additional IP addresses uncovered, four already classified as malicious
- 557 string-connected domains unearthed

Studying the DNS Footprint of the Subdomain IoCs

We kicked off our analysis by looking for more information about the nine subdomains dubbed as IoCs via the WhoisXML API MCP Server.

We discovered that they all belonged to code repositories, mostly open-source or free services. While none of the domains they fell under have been categorized as malicious, some of the code stored in them could have been injected with the malware as part of the ForceMemo campaign.

Take a look at specific findings for three examples below.

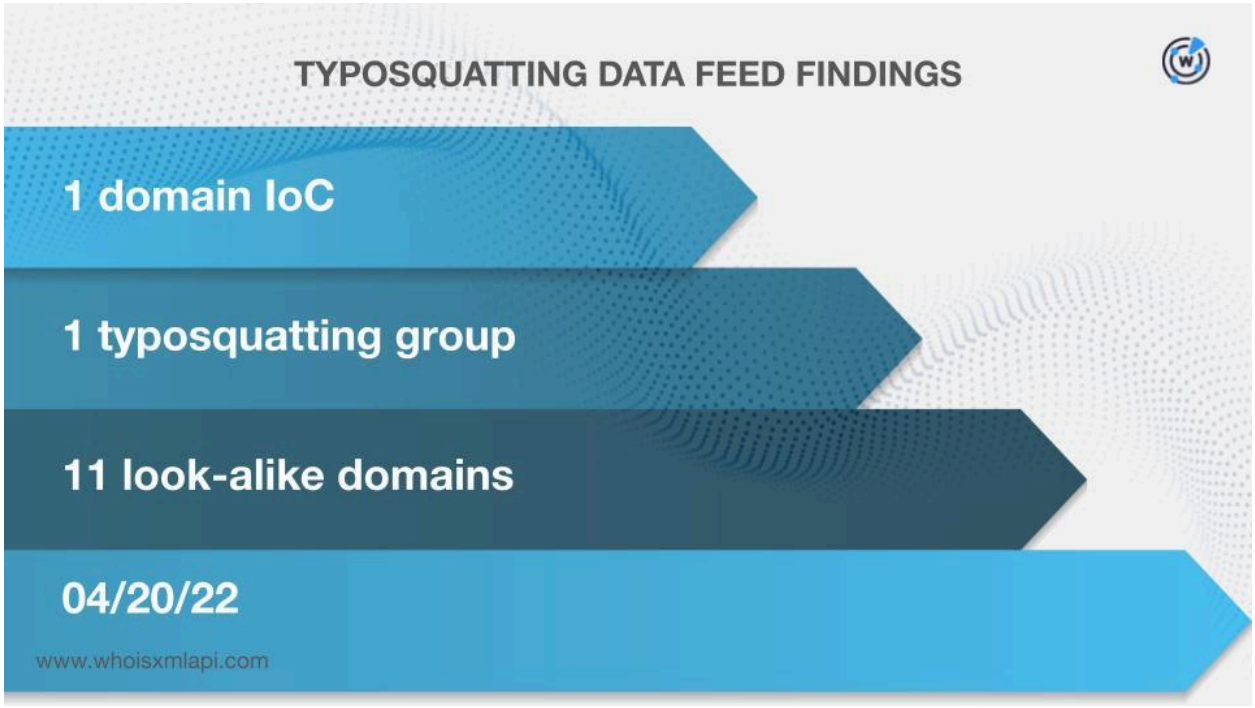
SUBDOMAIN IoC	WXA MCP SERVER FINDING
api[.]blockeden[.]xyz	Based on data up to August 2025, BlockEden[.]xyz is a blockchain infrastructure and API platform, primarily targeting Web3 developers. It provides RPC/API endpoints for multiple blockchains (Aptos, Sui, Ethereum, Solana, etc.), staking services, and analytics tools for on-chain data. This subdomain is their main developer API gateway.

api[.]mainnet-beta[.]solana[.]com	This is the official public RPC endpoint for the Solana Mainnet Beta network operated by the Solana Foundation. Developers use it to interact with the Solana blockchain (submitting transactions, querying accounts, etc.). It is a heavily used but rate-limited endpoint. Production apps are generally encouraged to use dedicated RPC providers instead.
go[.]getblock[.]us	GetBlock (getblock[.]io) is a well-known blockchain node-as-a-service/RPC provider supporting 50+ blockchains including Solana, Ethereum, BNB Chain, Bitcoin, and many others. This subdomain appears to be their U.S.-facing API gateway with the dual-IP, ultra-low TTL setup designed to maximize availability and minimize latency for North American users.

Dissecting the DNS Underbelly of the Domain IoCs

We then went on to gather DNS data on the five domains categorized as IoCs.

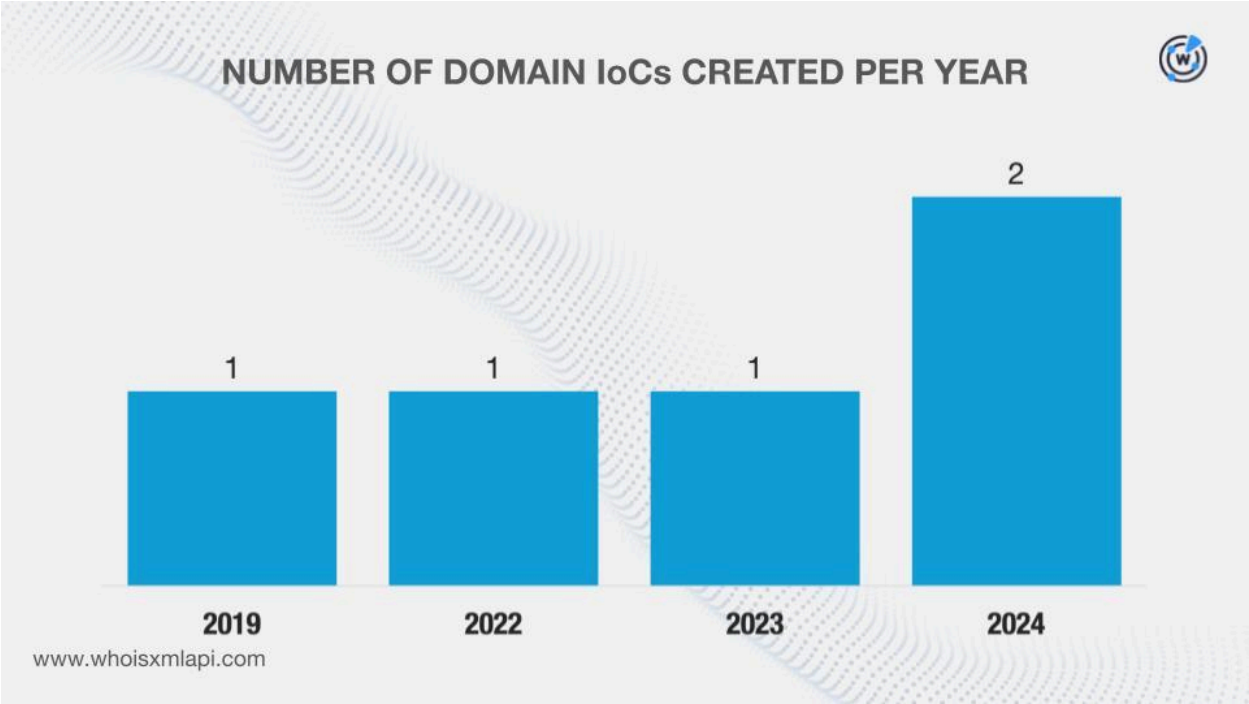
We scoured the Typosquatting Data Feed and found out that the domain pocket[.]network was bulk-registered with 11 look-alike domains on 20 April 2022.



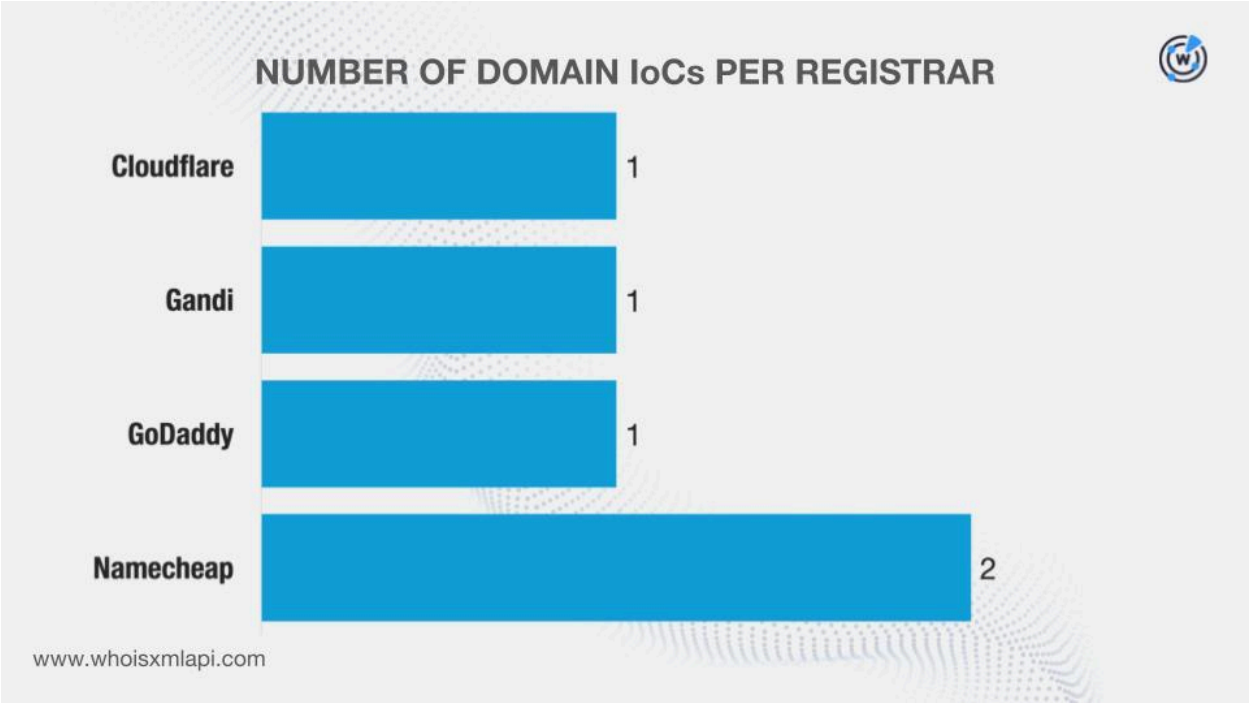
Our searches on the First Watch Malicious Domains Data Feed, meanwhile, revealed that the same domain—pocket[.]network—was deemed to have been registered with malicious intent on 23 February 2024, 750 days before being dubbed as an IoC on 14 March 2026.

We then queried the domains on WHOIS API and filled in gaps (i.e., missing details) specifically for blockeden[.]xyz using Domain Info API, which gave us the latest available information from its historical records. We discovered that:

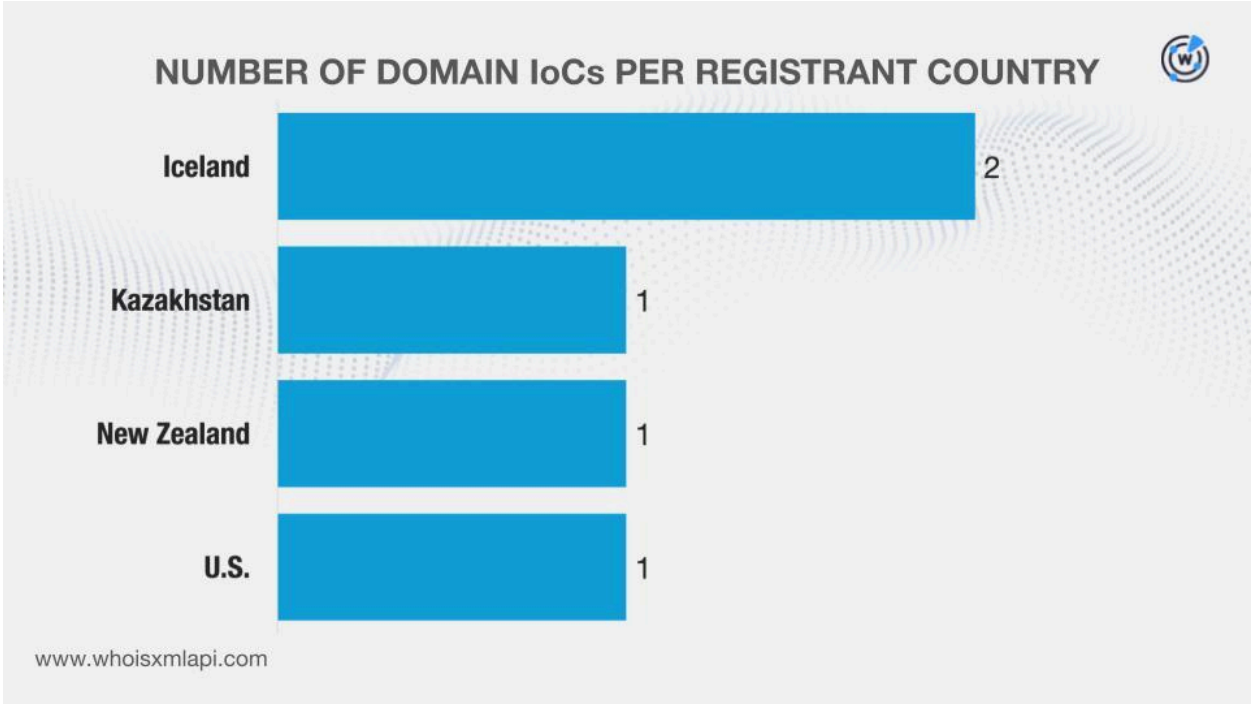
- They were created between 28 March 2019 and 26 September 2024, which could imply the attackers' preference for not using NRDs for this campaign.



- They were administered by four registrars.



- They were registered in four countries.



DNS Chronicle API queries for the domains showed that four recorded 1,368 historical domain-to-IP resolutions over time. Take a look at more information for two examples below.

DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
pocket[.]network	102	12/04/17–02/28/26
onfinality[.]io	1,000	04/24/20–02/17/26

Given the dates when the sample domains above last resolved to IP addresses, we can infer that they continue to be actively used for the campaign.

Investigating the DNS Traces of the IP IoCs

Next, we gathered more information on the six IP addresses identified as IoCs.

A Bulk IP Geolocation Lookup for the IP addresses revealed that:

- They were all geolocated in France.
- They were also administered by a single ISP, that is, The Constant Company.

Our DNS Chronicle API queries for the IP addresses showed that five recorded 251 historical IP-to-domain resolutions over time. Below are more details for two examples.

IP IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	DATES SEEN
45[.]32[.]151[.]157	58	02/11/17–06/07/21
217[.]69[.]11[.]57	61	04/18/20–05/04/25

Since the dates when the sample IP addresses above last resolved to domains do not extend to 2026, we can infer that the attackers may have opted to use new IPs for the campaign.

Hunting for New ForceMemo Artifacts

As the final step in our investigation, we sought to uncover artifacts that could be connected to the threat.

We began by querying the five domains tagged as IoCs on WHOIS History API. We found out that all of them had seven unique email addresses in their historical records. Further scrutiny revealed that three were public email addresses.

Reverse WHOIS API queries for the public email addresses led to the discovery of 86 unique email-connected domains after those already named as IoCs were filtered out.

We then queried the domains on DNS Lookup API and learned that four actively resolved to nine unique IP addresses that were not in the list of IoCs.

Threat Intelligence API queries for the additional IP addresses revealed that four have already been weaponized for various attacks. Take a look at more information for three examples below.

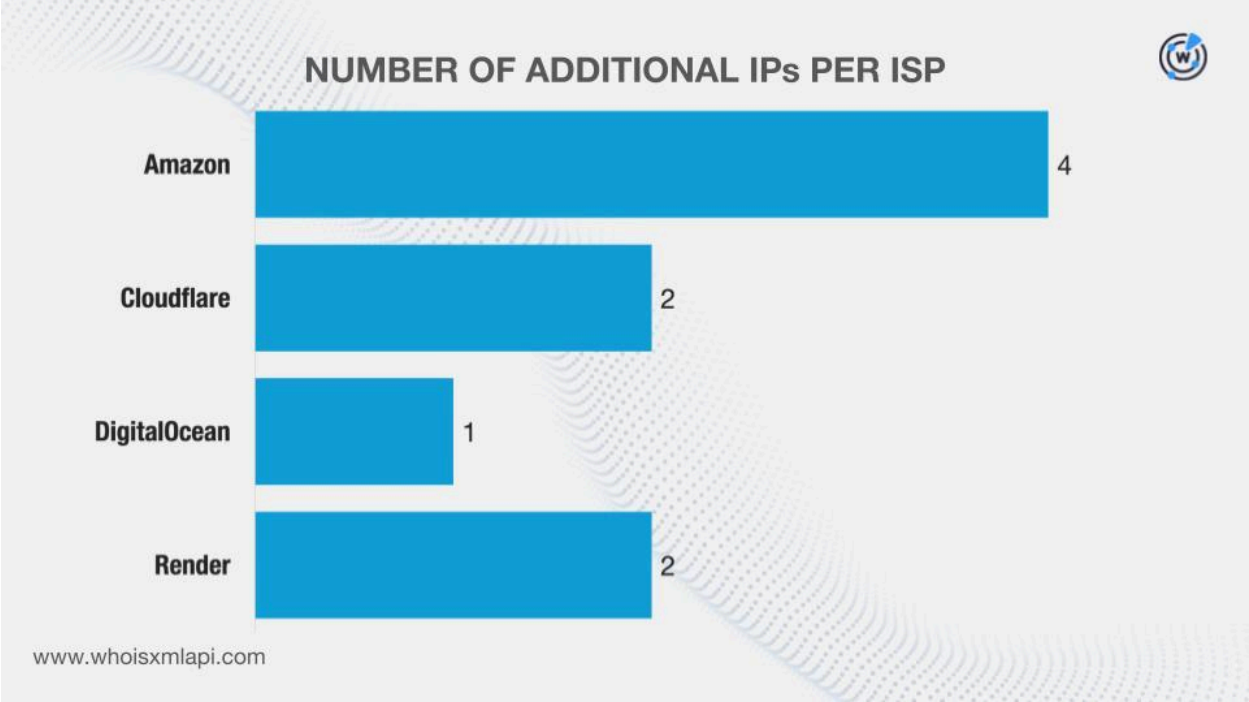
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
104[.]21[.]81[.]16	Malware distribution Phishing Generic threat	07/17/23–03/16/26 09/09/23–03/15/26 04/28/25–12/22/25
172[.]67[.]137[.]124	Malware distribution Phishing	07/17/23–03/16/26 09/09/23–03/15/26

	Generic threat	04/28/25–12/22/25
216[.]24[.]57[.]251	Phishing Malware distribution	07/31/25–03/17/26 07/23/25–03/16/26

Given the more recent dates when the sample IP addresses were last seen, we can infer that they have taken the place of the IPs classified as IoCs in the campaign, which seem to be no longer in use.

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

- They were all geolocated in the U.S., a far cry from those dubbed as IoCs, which all originated in France.
- They are administered by four ISPs, also all different from the sole ISP of those categorized as IoCs.



At this point, we now had 15 IP addresses. Reverse IP API queries for them showed that while one was a dedicated host, the sole IP-connected domain it resolved, pocket[.]network, was already cited as an IoC.

We then extracted five unique text strings from the domains identified as IoCs and searched for others that started with them on Domains & Subdomains Discovery. We

unearthed 557 unique string-connected domains after those already tagged as IoCs and the email-connected domains were filtered out.

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.

Summing Up Our ForceMemo Findings

Our DNS deep dive into the ForceMemo network IoCs revealed that one domain dubbed as an IoC was likely registered with malicious intent from the get-go. We also uncovered 652 new artifacts that could be connected to the campaign. These comprised 86 email-connected domains, nine additional IP addresses, and 557 string-connected domains. It is also worth noting that four of these artifacts have already figured in 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

- 212[.]film
- 213[.]film
- 310[.]film
- actors[.]film
- actress[.]film
- asia[.]film
- beijing[.]film
- beverlyhills[.]film
- careers[.]film
- castaicstudios[.]film
- dtla[.]film
- dtla[.]live
- dtla[.]social
- els[.]house
- estates[.]wedding
- events[.]film
- filmanywhere[.]com
- freelance[.]film
- gig[.]film
- gigg[.]film
- giggs[.]film
- hankachu[.]us
- homes[.]film
- houses[.]film
- imagelocation[.]film
- imagelocations[.]film
- independent[.]film
- job[.]film
- jobs[.]film
- location[.]film
- location[.]pics
- locationdepartment[.]com
- malibu[.]film
- mansions[.]film
- nyc[.]film
- nyu[.]film
- paulkim[.]com
- paulkim[.]film
- pls[.]house
- reel[.]jobs
- rodeo[.]studio
- rodeolocation[.]com
- scout[.]film
- scouting[.]film
- scouts[.]film
- talent[.]film
- usc[.]film
- weddingestates[.]photo
- weddingestates[.]pics
- weddinglocations[.]photo

Sample Additional IP Addresses

- 104[.]21[.]81[.]16
- 172[.]67[.]137[.]124
- 216[.]24[.]57[.]251
- 216[.]24[.]57[.]7

Sample String-Connected Domains

- blockeden[.]cn
- blockeden[.]com
- getblock[.]ai
- getblock[.]app
- getblock[.]asia
- leorpc[.]xyz
- onfinality[.]cloud
- onfinality[.]com
- onfinality[.]foundation
- pocket[.]5g[.]in