Decrypting the Inner DNS Workings of EncryptHub

Table of Contents

Executive Report

Outpost24 recently discovered that rising cybercriminal entity EncryptHub inadvertently exposed elements of its malicious enterprise. The security investigation unveiled previously unknown aspects of the group's infrastructure, tools, and behavioral patterns.

The security researchers notably uncovered the group's directory listing, allowing them to take a peek into the threat actors' stealer logs, malware executables, PowerShell scripts, and Telegram bot configurations. These errors shed light on the group's operations, including their attack chain and methodologies.

Outpost24 reported its findings in "Unveiling EncryptHub: Analysis of a Multistage Malware Campaign," along with 20 indicators of compromise (IoCs) comprising 14 domains and six IP addresses, that WhoisXML API expanded through a DNS deep dive.

Our in-depth analysis of the EncryptHub IoCs led to the discovery of new connected artifacts comprising:

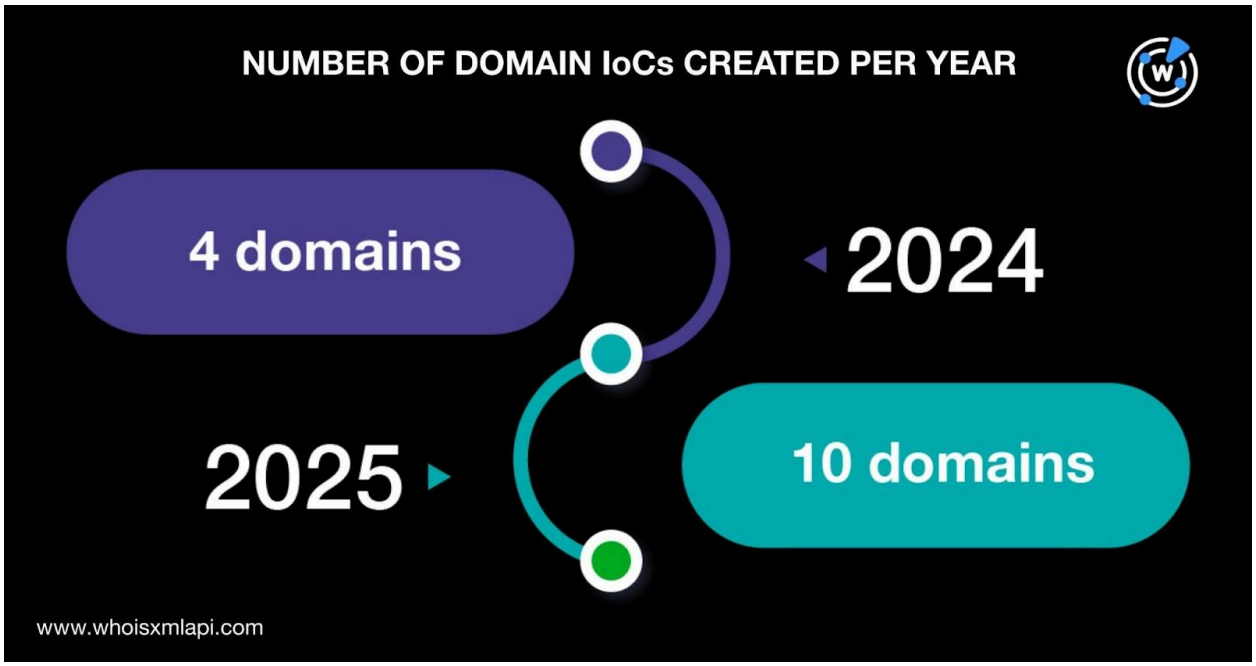
- 64 email-connected domains, one of which turned out to be malicious
- 10 additional IP addresses, seven of which have already been tagged as malicious
- 71 IP-connected domains, one of which has already been weaponized for attacks
- 419 string-connected domains, seven of which have already figured in malicious campaigns

More on the EncryptHub IoCs

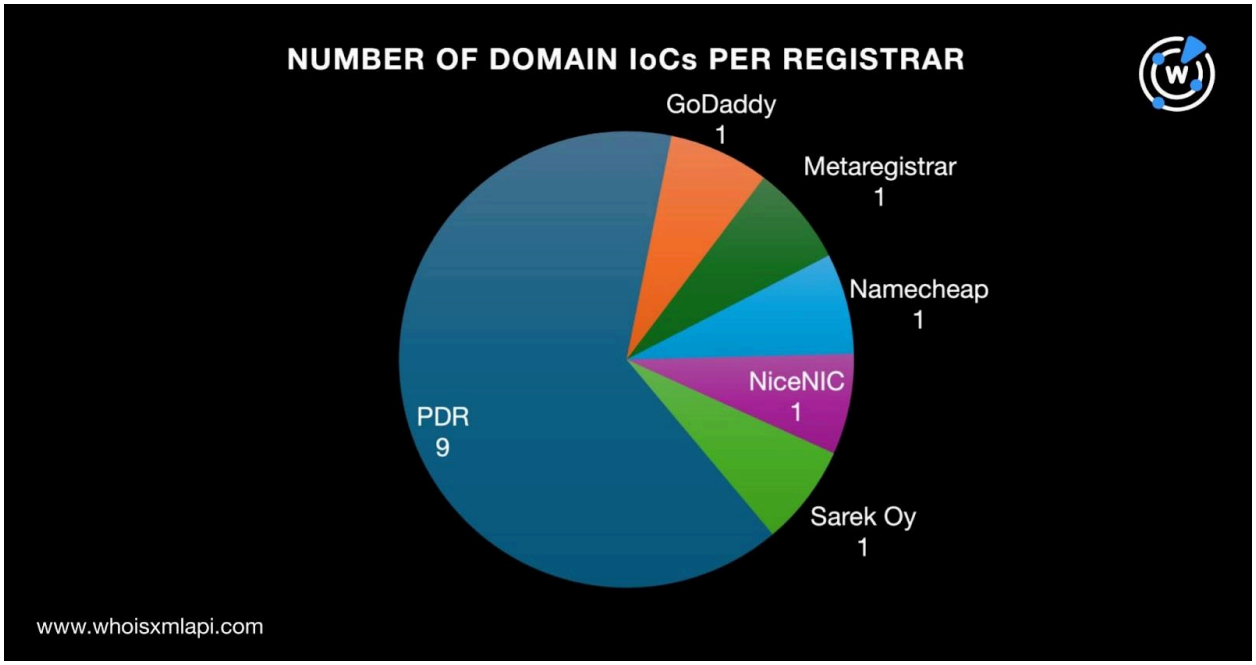
Before expanding the current list of EncryptHub IoCs, we sought to find more information on them first.

We began by querying the 14 domains identified as IoCs on Bulk WHOIS API. The results showed that:

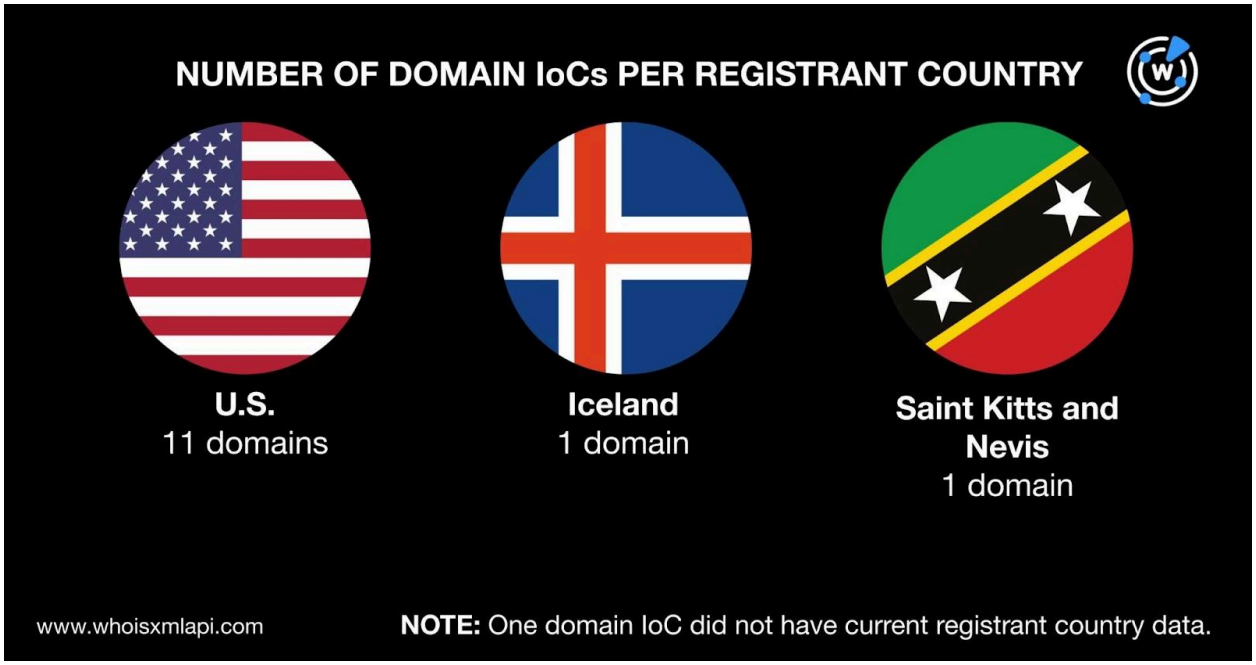
- They were all fairly newly registered, having been created between 2024 and 2025. Specifically, four were created in 2024 and 10 in 2025.



- They were administered by six registrars led by PDR, which accounted for nine domains. One domain each was administered by GoDaddy, Metaregistrar, Namecheap, NiceNIC, and Sarek Oy.



- Most of the domains, 11 to be exact, were registered in the U.S. One domain each was registered in Iceland and Saint Kitts and Nevis. Finally, one domain did not have a registrant country on record.



We then queried the 14 domains identified as IoCs on DNS Chronicle API and discovered that all of them had historical domain-to-IP resolutions. In fact, the 14 domains had 86 domain-to-IP

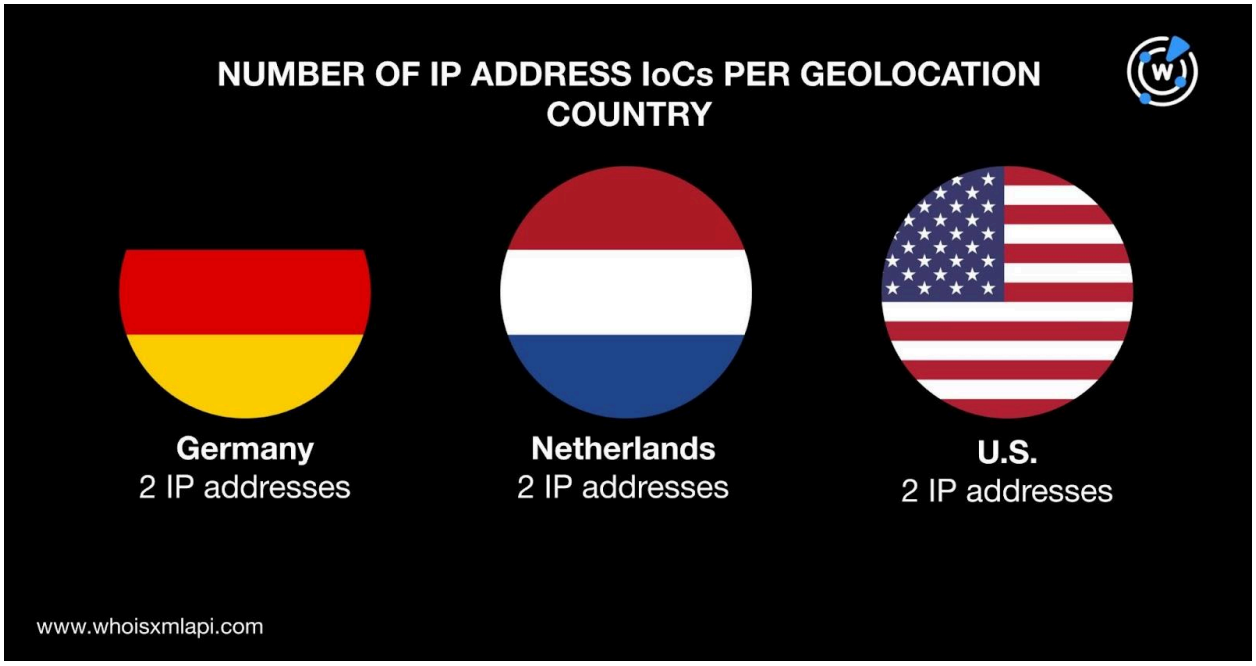
resolutions over time. The domain global-protect[.]net had the oldest IP resolution date—28 February 2020. Since its current creation date was 16 January 2025, it has probably been reregistered recently.

The table below shows the DNS histories of five other domains.

DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
353827-coinbase[.]com	1	27 January 2025
b8-crypt0x[.]com	1	22 February 2025
concur[.]net[.]co	3	22 January 2025
encrypthub[.]us	1	9 February 2025
healthy-cleanse-fit[.]com	23	27 September 2023

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

- They were geolocated in three countries. Two IP addresses each traced their origins to Germany, the Netherlands, and the U.S.



- None of the domains had ISPs on record.

Like the domains identified as IoCs, we also queried the IP addresses tagged as IoCs on DNS Chronicle API and discovered that only five had historical IP-to-domain resolutions. The five IP addresses had 123 IP-to-domain resolutions over time. The IP address 82[.]115[.]223[.]199 recorded the oldest domain resolution date—9 January 2021.

Here are details on three other IP addresses identified as IoCs.

IP ADDRESS IoC	NUMBER OF DOMAIN RESOLUTIONS	FIRST DOMAIN RESOLUTION DATE
193[.]149[.]176[.]228	19	7 June 2022
64[.]95[.]13[.]166	1	23 January 2025
85[.]209[.]128[.]128	7	17 December 2024

EncryptHub IoC List Expansion Findings

We started our search for connected web properties by querying the 14 domains identified as IoCs on WHOIS History API. We discovered that eight of them had eight email addresses in their historical WHOIS records after duplicates were filtered out. Four of the eight email addresses were public addresses.

We then queried the four public email addresses on Reverse WHOIS API and found that none of them appeared in the current WHOIS records of other domains. All of them, though, appeared in the historical WHOIS records of 64 domains after duplicates and those already identified as IoCs were filtered out.

A Threat Intelligence API query for the 64 email-connected domains showed that one—encrypthub[.]net—was already considered malicious.

Next, we queried the 14 domains identified as IoCs on DNS Lookup API. We discovered that 11 currently resolves to 10 IP addresses after duplicates and those already tagged as IoCs were filtered out.

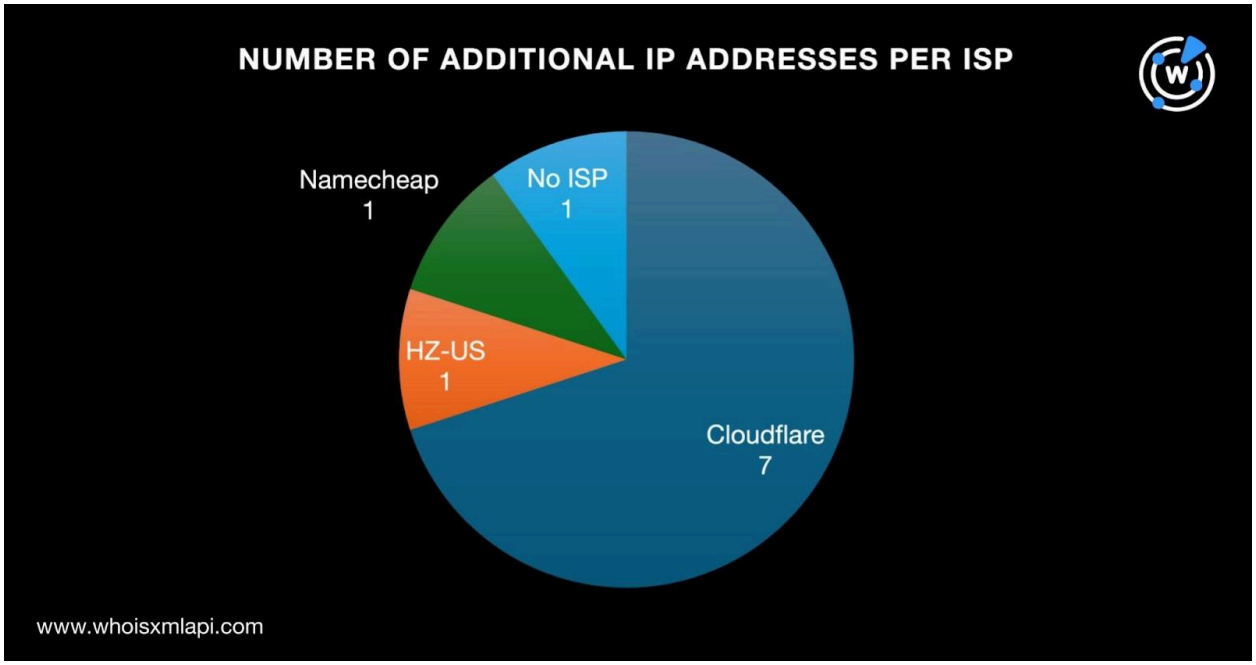
A Threat Intelligence API query for the 10 additional IP addresses revealed that seven have already been weaponized for attacks.

Here are details on three of the malicious additional IP addresses.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]16[.]1	Attack Command and control (C&C) Generic threat Malware distribution Phishing Spamming Suspicious activity
104[.]21[.]48[.]1	Attack C&C Generic threat Malware distribution Phishing Suspicious activity
104[.]21[.]80[.]1	Attack C&C Generic threat Malware distribution Phishing Suspicious activity

A Bulk IP Geolocation Lookup query for the 10 additional IP addresses showed that:

- Nine of them were geolocated in the U.S. One did not have a geolocation country on record.
- A majority of them, seven to be exact, were administered by Cloudflare. One IP address each was administered by HZ-US and Namecheap. Finally, one IP address did not have current ISP information.



So, given the six IP addresses identified as IoCs plus the 10 additional ones we uncovered, we now had 16 IP addresses on our expansion list. A Reverse IP API query for the 16 IP addresses revealed that 15 hosted other domains. Seven of them could be dedicated hosts. In fact, they hosted 71 domains after duplicates and those already identified as IoCs were filtered out.

A Threat Intelligence API query for the 71 IP-connected domains showed that one—lankantour[.]com—has already been utilized to distribute malware.

As our final step, we inspected the 14 domains identified as IoCs more closely and found that they started with 13 unique text strings. Domains & Subdomains Discovery searches for them revealed that eight strings appeared at the beginning of 419 domains after duplicates, those already tagged as IoCs, and the email- and IP-connected domains were filtered out. These eight text strings were:

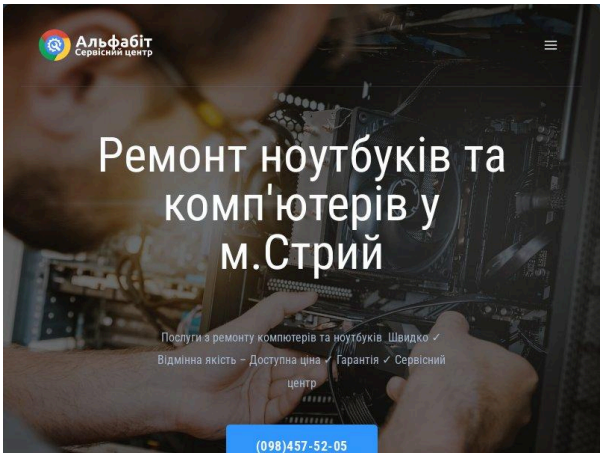
- alphabit.
- blackangel.
- concur.
- conferx.
- encrypthub.
- f*ckedserver.
- global-protect.
- malwarehunterteam.

A Threat Intelligence API query for the 419 string-connected domains showed that seven have already been weaponized for attacks.

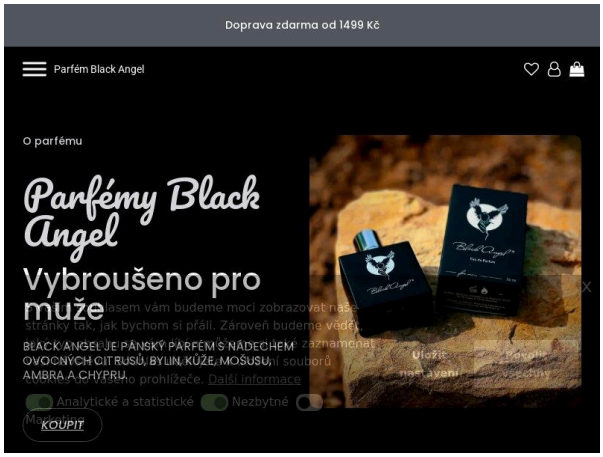
Here are details on three malicious string-connected domains.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREATS
concur[.]bond	Malware distribution
concur[.]life	Malware distribution
concur[.]re	Malware distribution

A Screenshot API query for the 419 string-connected domains also revealed that 225 remained accessible to date.



alphabit[.]com[.]ua



blackangel[.]cz

—

All in all, our search for EncryptHub connections led to the discovery of 564 web properties comprising 64 email-connected domains, 10 additional IP addresses, 71 IP-connected domains, and 419 string-connected domains. A total of 16 of these connected properties (i.e., seven IP addresses and nine domains) have already figured in 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

- appreciatethehelp[.]com
- barracudaenergizeupdate[.]com
- barracudaenergizeupdates[.]com
- barracudaevaluations[.]com
- ciscopeeps[.]com
- cudawebfilters[.]com
- darkfibers[.]net
- databasepeeps[.]com
- economicsqna[.]com
- encrypthub[.]net
- energizeupdate[.]com
- fuckbeans[.]net
- fuckedserver[.]org
- historyoverflow[.]com
- historyqna[.]com
- historyslayer[.]com
- icalevent[.]com
- livesecurityrenewals[.]com
- madmandy[.]com
- movieqna[.]com
- nannygrades[.]com
- networkingpeeps[.]com
- oraclepeeps[.]com
- paloaltofirewall[.]com
- paloaltofirewalls[.]com
- paloaltonettworks[.]com
- scienceqna[.]com
- securitycombat[.]com
- securitycrunch[.]com
- technicalpeeps[.]com
- techvade[.]com
- techvader[.]com
- xemployed[.]com

Sample Additional IP Addresses

- 104[.]21[.]112[.]1
- 104[.]21[.]16[.]1
- 104[.]21[.]32[.]1
- 104[.]21[.]64[.]1

Sample IP-Connected Domains

- copygit[.]com
- lankantour[.]com
- www[.]b8-crypt0x[.]com

Sample String-Connected Domains

- alphabit[.]ai
- alphabit[.]app
- alphabit[.]asia
- blackangel[.]africa
- blackangel[.]ai
- blackangel[.]at
- concur[.]ad
- concur[.]ae
- concur[.]africa
- conferx[.]com
- conferx[.]xyz
- encrypthub[.]com

- encrypthub[.]io
- encrypthub[.]org
- fuckedserver[.]com
- global-protect[.]ch
- global-protect[.]co[.]uk
- global-protect[.]com
- malwarehunterteam[.]com