Exploring Epsilon Stealer Traces Aided by DNS Intel

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts and IoCs

Executive Report

Computers that get infected with the Epsilon stealer could spell game over for serious gamers, but they are not the only ones at risk. The creators of games like EPSILON, Pokemon, and Roblox that the malware operators are mimicking stand to lose a lot as well. They may lose customers and damage their reputation in the process.

Epsilon steals not only user credentials but also personal data, in-game assets, and other sensitive information using Discord messages and fake game download sites. Sekoia.io security researchers published an in-depth analysis of the data stealer and named 133 domains and subdomains as indicators of compromise (IoCs). We extracted 76 domainsfrom their list for our ex.

The WhoisXML API research team expanded the IoC list to find unpublished connected threat artifacts using our massive DNS intelligence repositories and found:

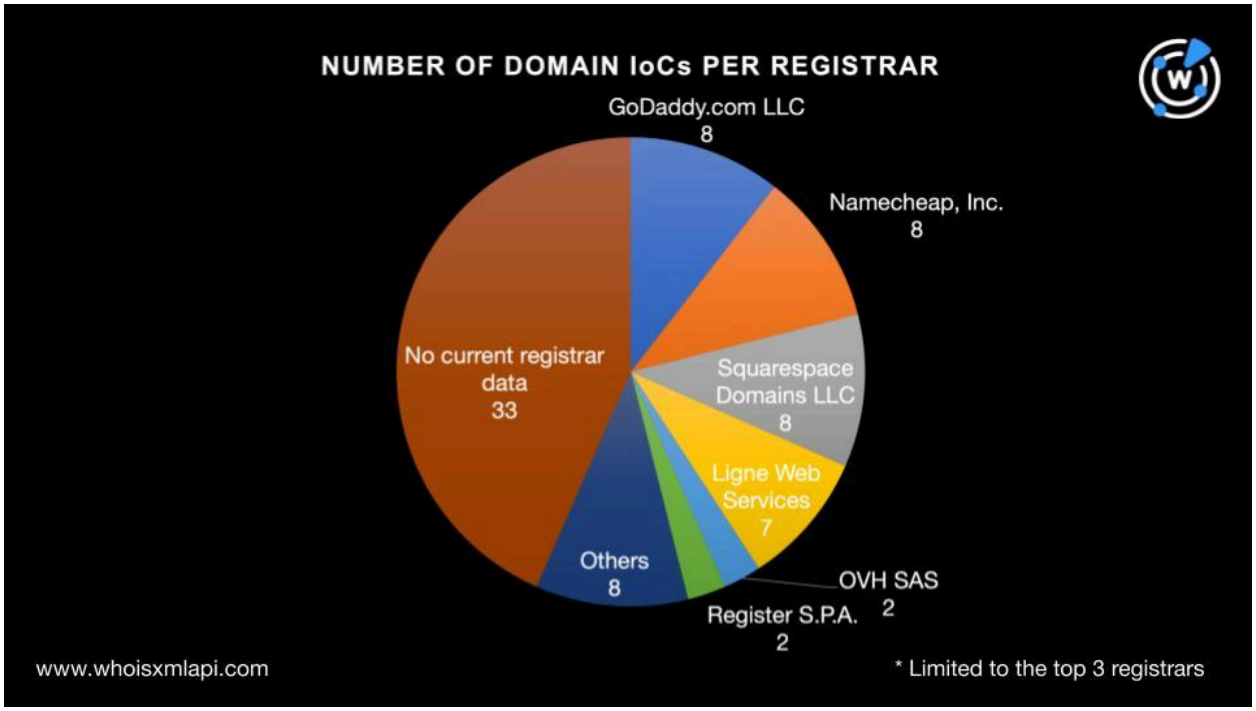
- 74 email-connected domains
- 33 IP addresses to which the domains identified as IoCs resolved, 28 of which turned out to be malicious
- 1,623 string-connected domains, two of which turned out to be malicious

Epsilon Stealer IoC Facts

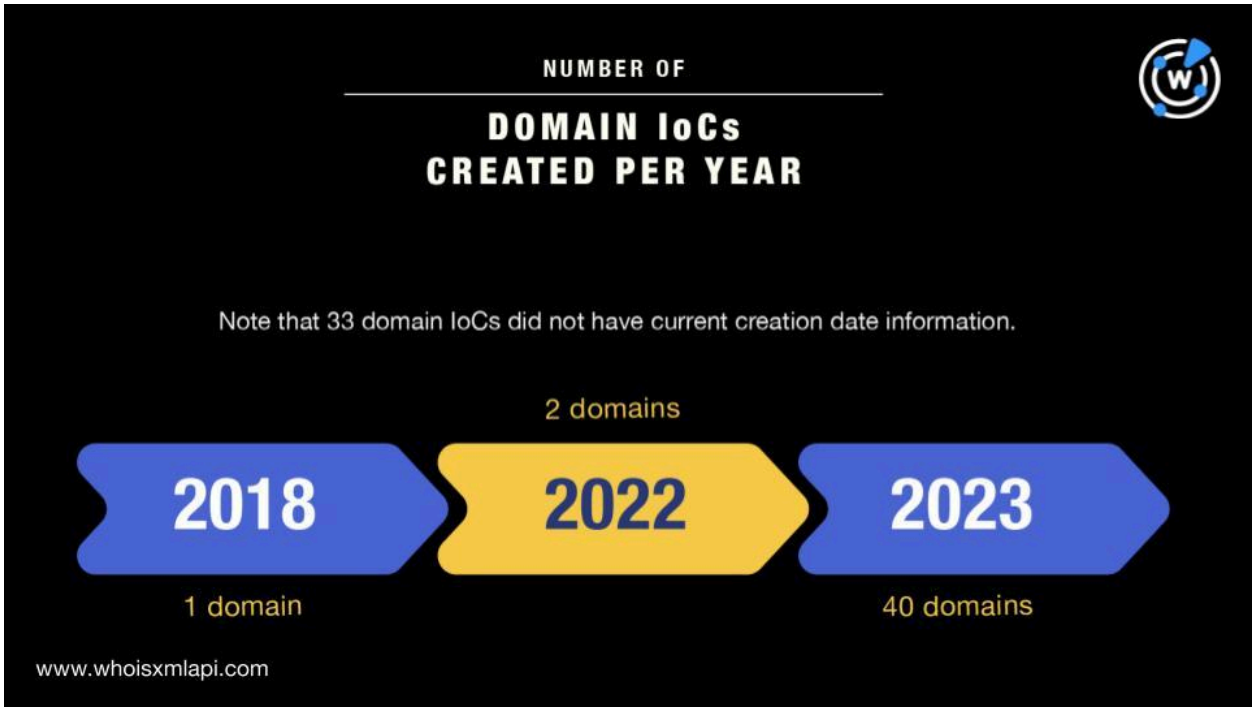
To begin our analysis, we sought to find as much information as possible on the 76 domains tagged as IoCs starting with a bulk WHOIS lookup, which revealed that:

- They were distributed among 14 registrars led by GoDaddy.com LLC, Namecheap, Inc., and Squarespace Domains LLC with eight domains each. Ligne Web Services took the second spot with seven domains. OVH SAS and Register S.P.A. took third place with

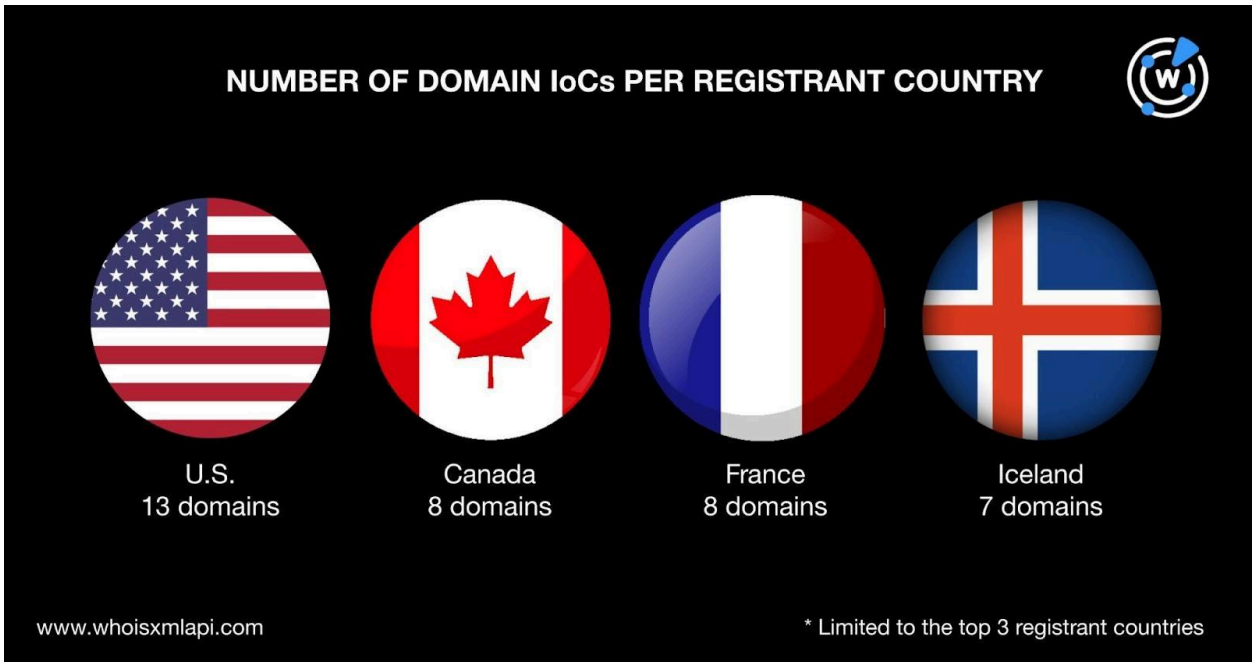
two domains each. One domain each was administered by eight other registrars while the remaining 33 did not have current registrar data.



- Forty-three of them were created between 2018 and 2023 while the remaining 33 did not have creation date information in their current WHOIS records.



- The top 3 registrant countries were the U.S., which accounted for 13 domains; Canada and France with eight domains each; and Iceland with seven domains. One domain each was created in Cyprus, the Netherlands, Romania, and Turkey while 37 did not have current registrant country data.



- It is also worth noting that one of them—plaguehunter[.]com—had a publicly viewable registrant name.

Epsilon Stealer IoC List Expansion Findings

To expand the current list of Epsilon stealer IoCs, we began by looking into their historical WHOIS records.

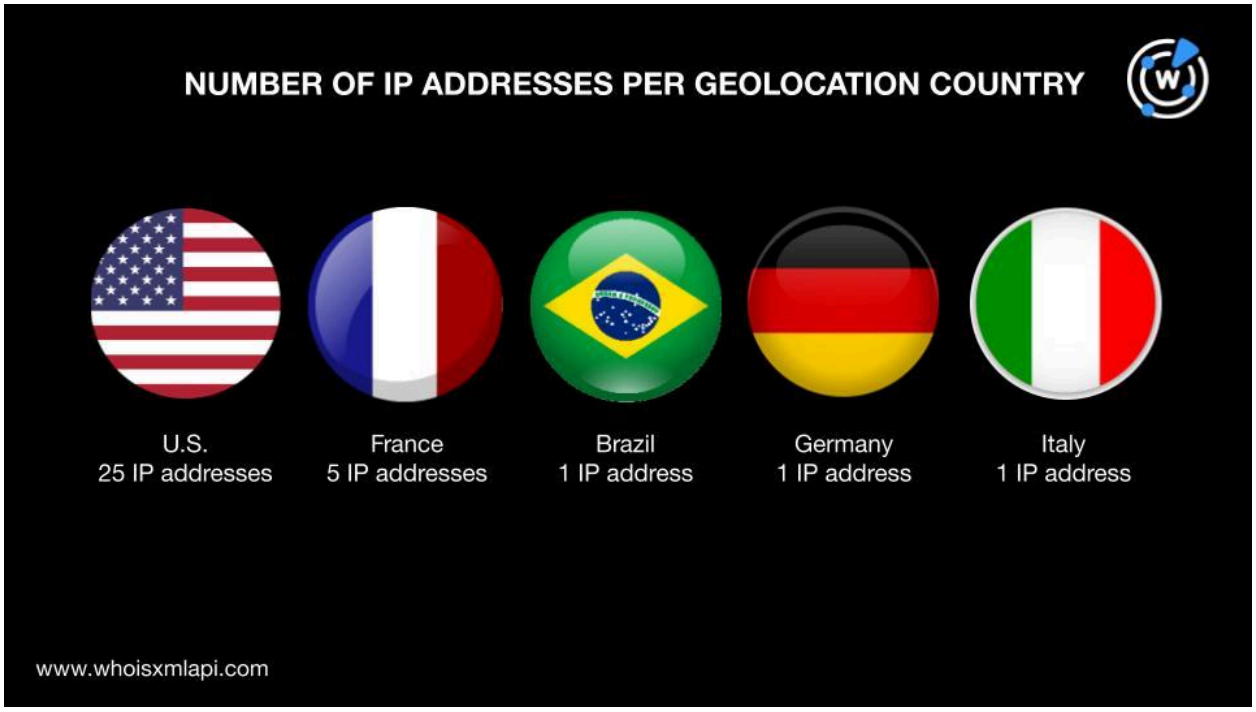
WHOIS History API revealed that 31 of the 76 domains classified as IoCs had 32 email addresses in their historical WHOIS records. Nine of them were public email addresses.

Subjecting the nine public email addresses to Reverse WHOIS API queries allowed us to determine they were present in the current WHOIS records of 74 other domains (email-connected) after duplicates and those already part of the current IoC list were filtered out.

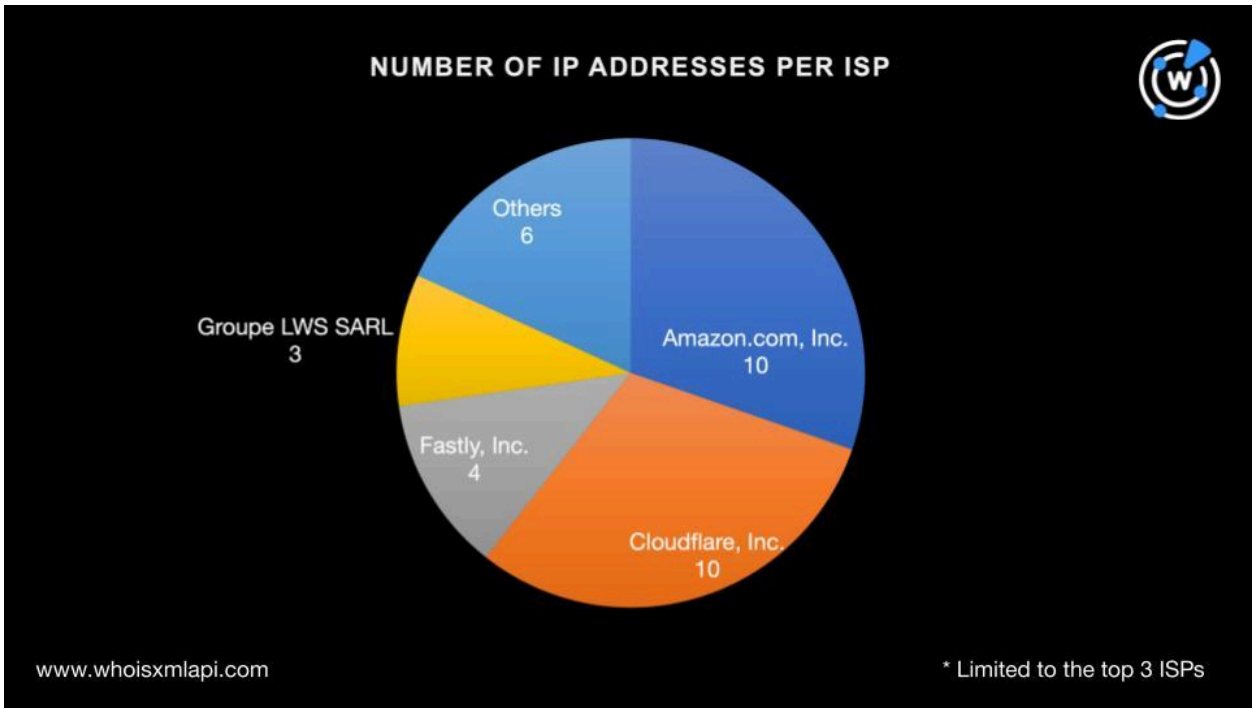
DNS lookups for the 76 domains tagged as IoCs revealed that 22 of them had active IP resolutions. They resolved to 33 IP addresses after duplicates were removed.

Performing IP geolocation lookups for the 33 IP addresses led to these interesting findings:

- A majority of them, 25 to be exact, pointed to the U.S. as their origin. Five were geolocated in France. One IP address each originated from Brazil, Germany, and Italy.



- They were spread across 10 Internet service providers (ISPs) led by Amazon.com, Inc. and Cloudflare, Inc. with 10 IP addresses each. Fastly, Inc. took the second spot with four IP addresses. Groupe LWS SARL took third place with three IP addresses. Six other ISPs accounted for one IP address each.



- Twenty-eight of them were flagged as malicious by the built-in Threat Intelligence API engine. Take a look at the tool's detailed findings for five of the IP addresses below.

IP ADDRESS	ASSOCIATED THREAT TYPE	DATE FIRST SEEN
104[.]21[.]0[.]216	Generic Malware Phishing	29 March 2023
104[.]21[.]61[.]207	Malware Suspicious	5 April 2023
104[.]21[.]63[.]236	Generic Malware Phishing	21 May 2023
13[.]248[.]169[.]48	C2 Generic Malware Phishing Suspicious	28 March 2023
13[.]248[.]213[.]45	C2 Generic Malware Phishing Suspicious	7 December 2023

Finally, to cover all our bases, we used Domains & Subdomains Discovery to look for domains containing 48 text strings that appeared in the IoCs, namely:

- **abyssgame**
- **aqua-phobia**
- **aquafridge**
- **articpunk**
- **conditus**
- **conquistadorio**
- **creseller**
- **deadlegacy**
- **deadsould**
- **dualcorps**
- **epsilon1337**
- **fightordie**
- **flstudiocrack**
- **grimwalker**
- **hentaimaster**
- **homurahime**
- **inovaperf**
- **legacysurvival**
- **movesoul**
- **mythicguardian**

- **nobodysleft**
- **plaguehunter**
- **pokemonadventure**
- **pokemonaventure**
- **rolaslegacy**
- **ronawind**
- **samuraihime**
- **shirokim**
- **shirone**
- **siltgame**
- **siltproject**
- **slayercat**
- **snotragame**
- **spacewars-beta**
- **spiralcircusgame**
- **strangerlegends**
- **survival-machine**
- **theblacktail**
- **timberstory**
- **trailofnanook**
- **ultra-flighter**
- **unturned**
- **vaniapunk**
- **voidofspace**
- **voidvanguard**
- **wdb.**
- **weavergames**
- **worldofsymphony**

We uncovered 1,623 string-connected domains, two of which were flagged as malicious by Threat Intelligence API. See the details in the table below.

STRING-CONNECTED DOMAIN	ASSOCIATED THREAT TYPE	DATE FIRST SEEN
dualcorps[.]site	Generic	2 November 2023
unturnedplayable[.]com	Phishing	9 March 2023

—

Our deep dive into Epsilon Stealer led to the discovery of 1,730 potentially connected threat artifacts, including 28 malicious IP addresses and two malware-laden string-connected domains.

If you wish to perform a similar investigation or 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

- 4006118263[.]xyz
- 4805058877[.]xyz
- adslw[.]xyz
- aisoge[.]xyz
- aisouge[.]xyz
- azcy[.]xyz
- azfc[.]xyz
- azgw[.]xyz
- azjr[.]xyz
- azlc[.]xyz
- azlx[.]xyz
- azly[.]xyz
- ben-simmons[.]xyz
- breakthroughenergycoalition[.]xyz
- cangbi[.]xyz
- demonoton[.]com
- detedium[.]com
- dianguan[.]xyz
- emoticombat[.]com
- haodaizhi[.]xyz

Sample IP Addresses

- 104[.]21[.]0[.]216
- 104[.]21[.]48[.]205
- 104[.]21[.]51[.]98
- 104[.]21[.]61[.]207
- 104[.]21[.]63[.]236
- 13[.]248[.]169[.]48
- 13[.]248[.]213[.]45
- 15[.]197[.]142[.]173
- 172[.]67[.]128[.]80
- 172[.]67[.]156[.]47
- 172[.]67[.]173[.]25
- 172[.]67[.]178[.]135
- 172[.]67[.]214[.]140
- 18[.]213[.]222[.]111
- 185[.]135[.]132[.]50
- 185[.]199[.]108[.]153
- 185[.]199[.]109[.]153
- 185[.]199[.]110[.]153
- 185[.]199[.]111[.]153
- 185[.]98[.]131[.]192

Sample String-Connected Domains

- abyssgame[.]club
- abyssgame[.]com
- abyssgame[.]ws
- abyssgamecenter[.]com
- abyssgamecenter[.]ph
- abyssgamer[.]com
- abyssgamers[.]com
- abyssgamers[.]com[.]br
- abyssgamers[.]team
- abyssgamerx[.]com
- abyssgames[.]ca
- abyssgames[.]com
- abyssgames[.]de
- abyssgames[.]io
- abyssgames[.]net
- abyssgames[.]tk
- abyssgamestore[.]com
- abyssgameworks[.]com
- aqua-phobia1st[.]co[.]uk
- aqua-phobia1st[.]com
- aquafridge[.]com
- aquafridge[.]info

- aquafridge[.]net
- aquafridge[.]org
- articpunk[.]games
- articpunk[.]xyz
- conditus[.]at
- conditus[.]be
- conditus[.]co[.]uk
- conditus[.]com
- conditus[.]com[.]au
- conditus[.]com[.]mx
- conditus[.]group
- conditus[.]info
- conditus[.]it
- conditus[.]lt
- conditus[.]net
- conditus[.]nl
- conditus[.]org
- conditus[.]se
- conditus[.]si
- conditus[.]tech
- conditus[.]vg
- condituscapital[.]com
- condituscatering[.]co[.]uk
- condituscoulis[.]com
- conditusfitness[.]com
- conditusspices[.]com
- conquistadorio[.]info
- conquistadorio[.]xyz
- creseller[.]com
- creseller[.]xyz
- cresellerhosting[.]com
- cresellers[.]com
- cresellersresource[.]com
- deadlegacy[.]cn
- deadlegacy[.]co
- deadlegacy[.]co[.]uk
- deadlegacy[.]com
- deadlegacy[.]net
- deadlegacy[.]online
- deadlegacy[.]ru
- deadlegacy[.]se
- deadlegacy[.]site
- deadlegacy[.]store
- deadlegacye-sports[.]com
- deadlegacymx[.]com
- deadlegacyreviews[.]com
- deadlegacyusa[.]com
- deadsouldesigns[.]com
- dualcorps[.]com
- dualcorps[.]online
- dualcorps[.]site
- dualcorps[.]xyz
- dualcorpsactivities[.]com
- epsilon1337[.]xyz
- fightordie[.]cf
- fightordie[.]club
- fightordie[.]co
- fightordie[.]co[.]uk
- fightordie[.]com
- fightordie[.]com[.]au
- fightordie[.]com[.]br
- fightordie[.]de
- fightordie[.]eu
- fightordie[.]ga
- fightordie[.]info
- fightordie[.]it
- fightordie[.]ml
- fightordie[.]net
- fightordie[.]org
- fightordie[.]pl
- fightordie[.]ru
- fightordie[.]tk
- fightordie[.]us
- fightordieapparel[.]com
- fightordieclothing[.]com
- fightordiee[.]us
- fightordiemovie[.]com