Mining for DNS Maxims: Top 10 Malware of Q3 2025

Table of Contents

Executive Report

The Center for Internet Security (CIS) just named the top 10 malware of Q3 2025 and identified 31 domains as IoCs for five of them. After weeding out legitimate domains from their list with the help of the WhoisXML API MCP Server, we were left with 26 domains for our study. Take a look at the breakdown below.

RANK	MALWARE	THREAT TYPE	NUMBER OF DOMAIN IoCs ORIGINALLY IDENTIFIED	NUMBER OF DOMAIN IoCs ANALYZED
1	SocGholish	Downloader	8	6
3	Agent Tesla	RAT	2	1
5	ZPHP	Downloader	9	7
7	Gh0st	RAT	4	4
9	Lumma Stealer	Infostealer	8	8
TOTAL			**31**	**26**

Note that three of the top 10 malware of Q2 2025—SocGholish, Agent Tesla, and ZPHP—remained part of this quarter's list. While SocGholish and Agent Tesla kept their top 1 and 3 rankings, respectively, ZPHP dropped from Q2's top 2 to this quarter's top 5.

Our in-depth analysis of five of the top malware for Q3 led to these discoveries:

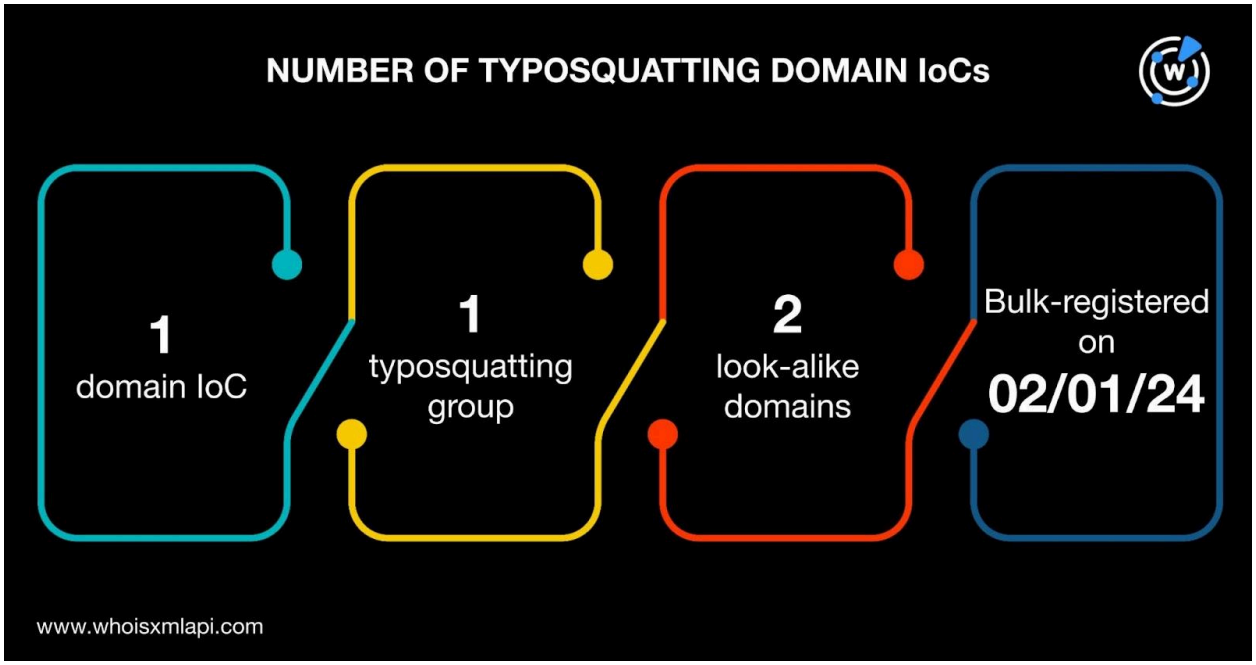
- Two domains identified as IoCs deemed likely to turn malicious 150–598 days prior to being dubbed as such
- One domain tagged as an IoC was bulk-registered with others and could be a typosquatter
- 5,266 email-connected domains, 56 were found malicious
- 11 IP addresses, seven were found malicious
- 104 IP-connected domains
- 606 string-connected domains, one was found malicious

Digging Up More Information on the IoCs

We began our in-depth investigation by checking if any of the 26 domains tagged as IoCs appeared on First Watch Malicious Domains Data Feed. We discovered that two of them were deemed likely to turn malicious as soon as they were registered, between 150 and 598 days before they were dubbed as IoCs on 14 November 2025. Here are more details.

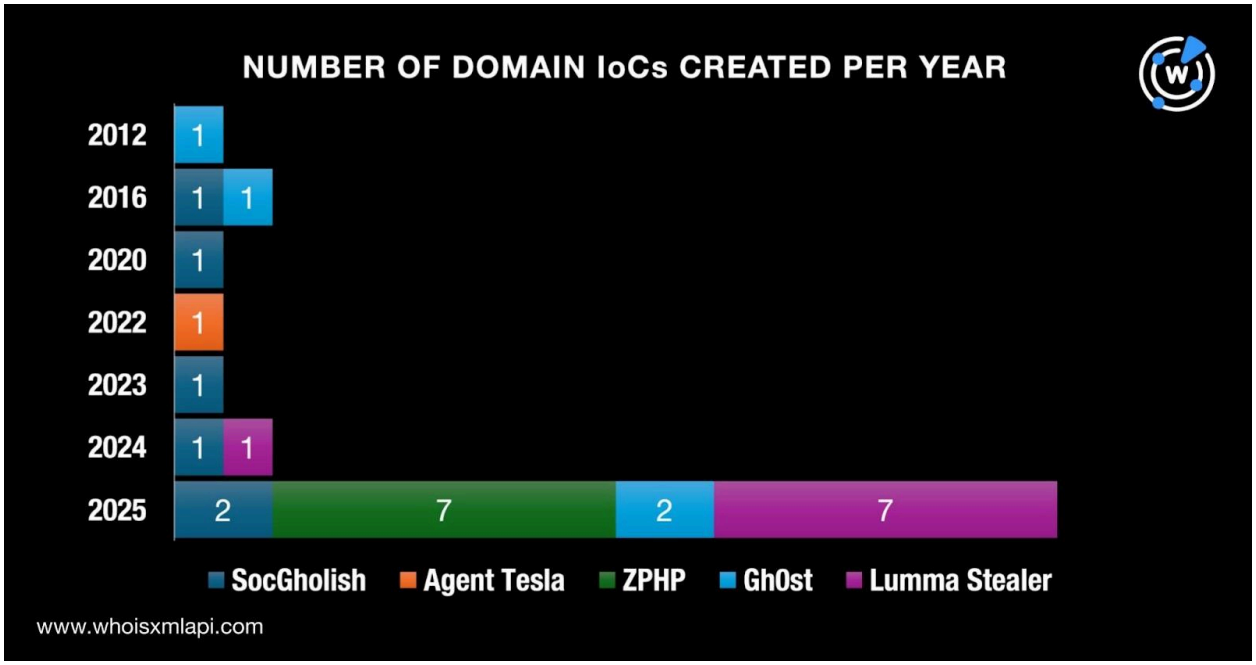
MALWARE	DOMAIN IoC	DATE SEEN ON FIRST WATCH	NUMBER OF DAYS BEFORE REPORT DATE
Gh0st	xmcxmr[.]com	26 March 2024	598
SocGholish	emeraldpinesolutions[.]com	17 June 2025	150

We also searched for the 26 domains identified as IoCs on Typosquatting Data Feed and discovered that one of them—trendings[.]top—was bulk-registered with two look-alikes—trendingg[.]shop and trendingon[.]store—on 1 February 2024.

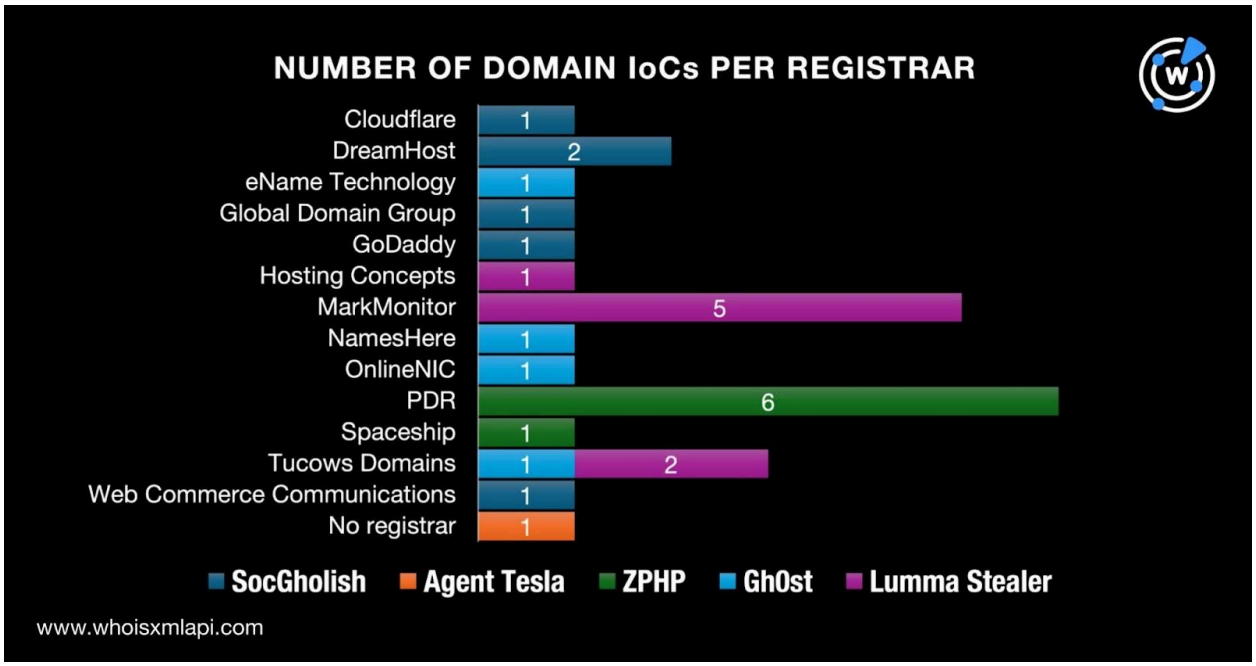


Next, we queried the 26 domains identified as IoCs on WHOIS API and filled out missing information aided by Domain Info API. We found out that:

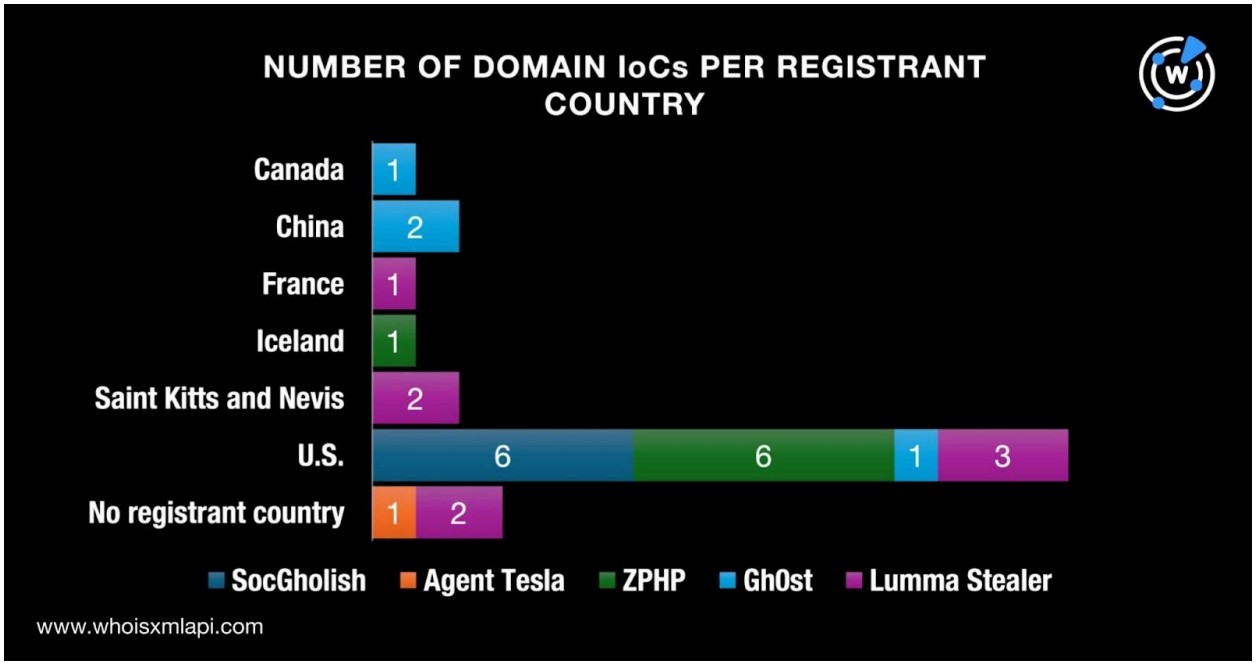
- They were created between 12 September 2012 (Gh0st's f3322[.]org) and 17 October 2025 (Lumma Stealer's lzh[.]fr). Specifically, 18 domains were created in 2025; two each in 2016 and 2024; and one each in 2012, 2020, 2022, and 2023.



- While one domain did not have registrar data in its current WHOIS record, the remaining 25 were distributed among 13 registrars. Six domains were administered by PDR; five by MarkMonitor; three by Tucows Domains; two by DreamHost; and one each by Cloudflare, eName Technology, the Global Domain Group, GoDaddy, Hosting Concepts, NamesHere, OnlineNIC, Spaceship, and Web Commerce Communications.



- While three domains did not have registrant country data on record, the remaining 23 were registered in six countries. A total of 16 domains were registered in the U.S.; two each in China and Saint Kitts and Nevis; and one each in Canada, France, and Iceland.



We also obtained additional information on the 26 domains tagged as IoCs from DNS Chronicle API. The results showed that 25 of them posted a total of 2,564 historical domain-to-IP resolutions over time. The SocGholish domain ebuilderssource[.]com recorded the oldest resolution on 5 February 2017. Take a look at more details below.

MALWARE	DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
SocGholish	ebuilderssource[.]com	192	02/05/17	11/04/17
Gh0st	vip5944[.]com	251	02/07/17	09/27/25
Gh0st	luyouxia[.]net	259	04/17/17	10/16/25
Gh0st	f3322[.]org	159	04/15/18	08/13/21
ZPHP	warpdrive[.]top	59	08/03/19	03/22/25

Prospecting for New Artifacts

We began our search for new artifacts by querying the 26 domains identified as IoCs on WHOIS History API. The results revealed that 16 of them had email addresses in their historical

WHOIS records. We collated 45 unique email addresses in all. Further scrutiny showed that 17 of them were public email addresses.

Next, we queried the 17 public email addresses on Reverse WHOIS API. While none of them appeared in current WHOIS records, 16 showed up on historical records. That led to the discovery of 5,266 email-connected domains after duplicates and those already tagged as IoCs were filtered out.

A Threat Intelligence API query for the 5,266 email-connected domains revealed that 56 of them have already been weaponized for nefarious activities. Here are five examples.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
dashboard-aave[.]us	Phishing Generic threat	04/20/25–10/19/25 04/21/25–09/20/25
help-opensea[.]us	Phishing Generic threat	03/25/25–09/25/25 03/27/25–09/20/25
id-verification-12912[.]us	Generic threat Phishing	09/10/25–10/13/25 09/09/25
information-id188322[.]com	Phishing Generic threat	07/18/25–11/20/25 07/19/25–09/20/25
progressdev[.]xyz	Malware distribution Generic threat	10/06/25–11/20/25 09/06/25

Afterward, we queried the 26 domains tagged as IoCs on DNS Lookup API. We discovered that 10 of them had active IP resolutions. They resolved to 11 unique IP addresses in all.

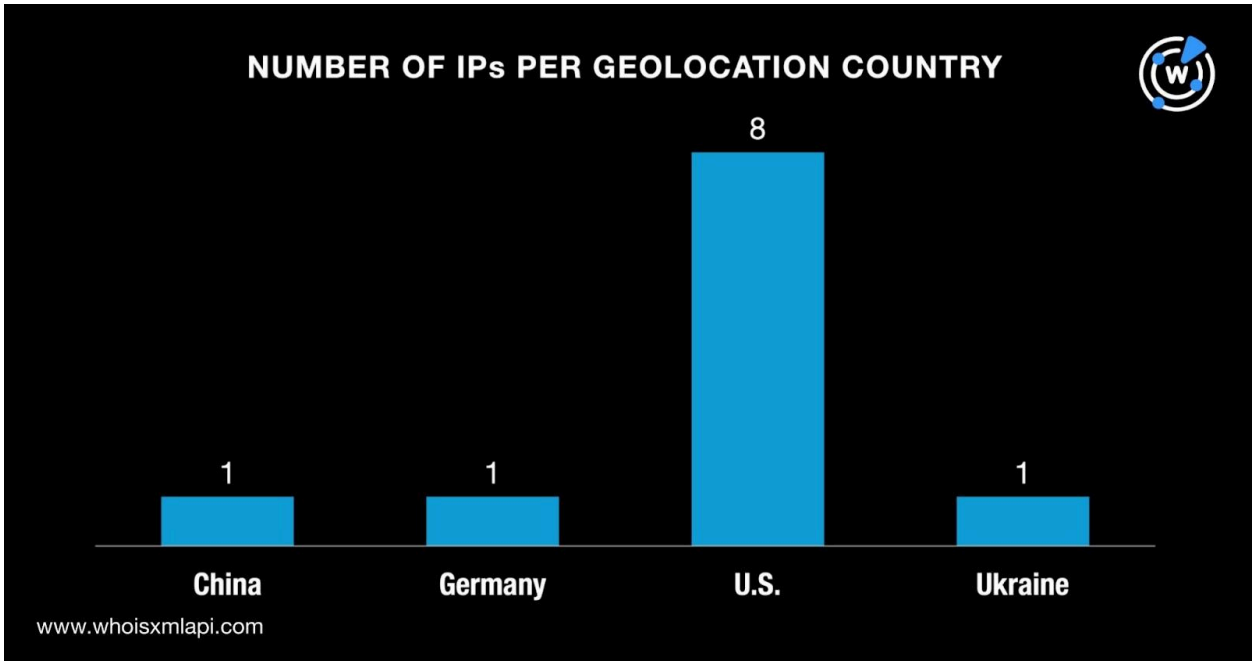
A Threat Intelligence API query for the 11 IP addresses showed that seven have already figured in malicious campaigns. Take a look at three examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
104[.]21[.]76[.]139	Phishing Malware distribution Generic threat	03/28/23–11/20/25 01/06/24–11/19/25 03/29/23–09/19/25
172[.]67[.]195[.]193	Phishing	03/28/23–11/20/25

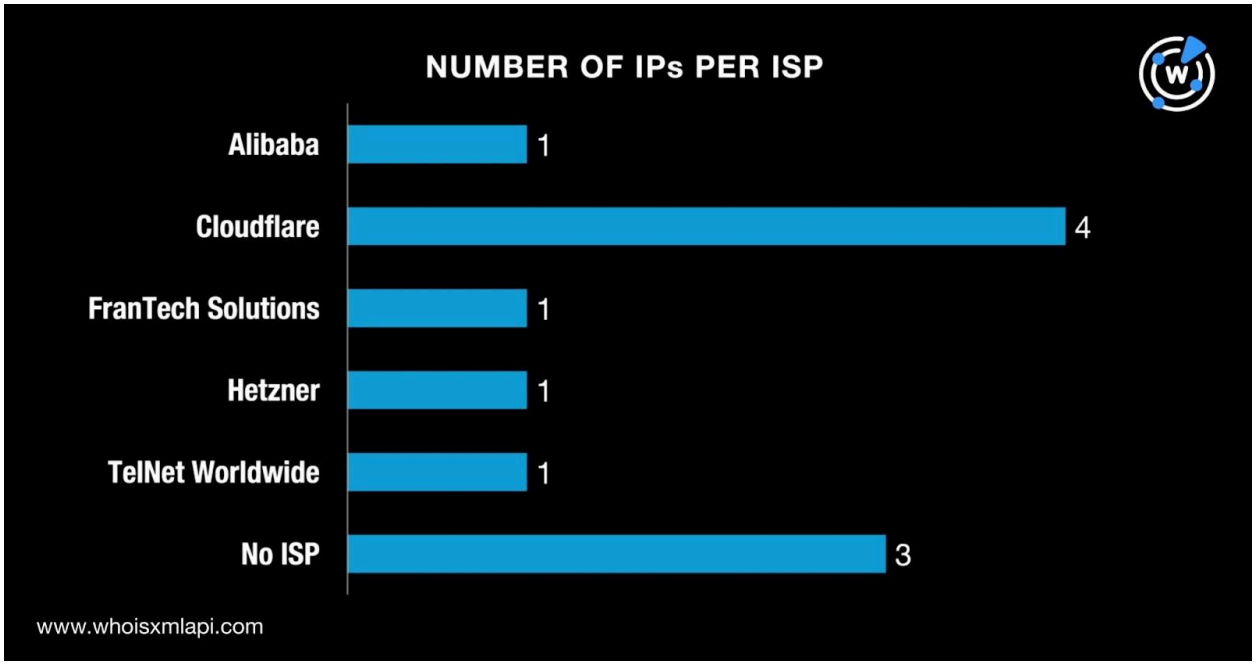
	Malware distribution Generic threat	01/06/24–11/19/25 03/29/23–09/19/25
104[.]21[.]88[.]252	Phishing Generic threat	04/14/23–11/20/25 04/15/23–11/19/25

We then gathered more information about the 11 IP addresses via Bulk IP Geolocation Lookup. The results showed that:

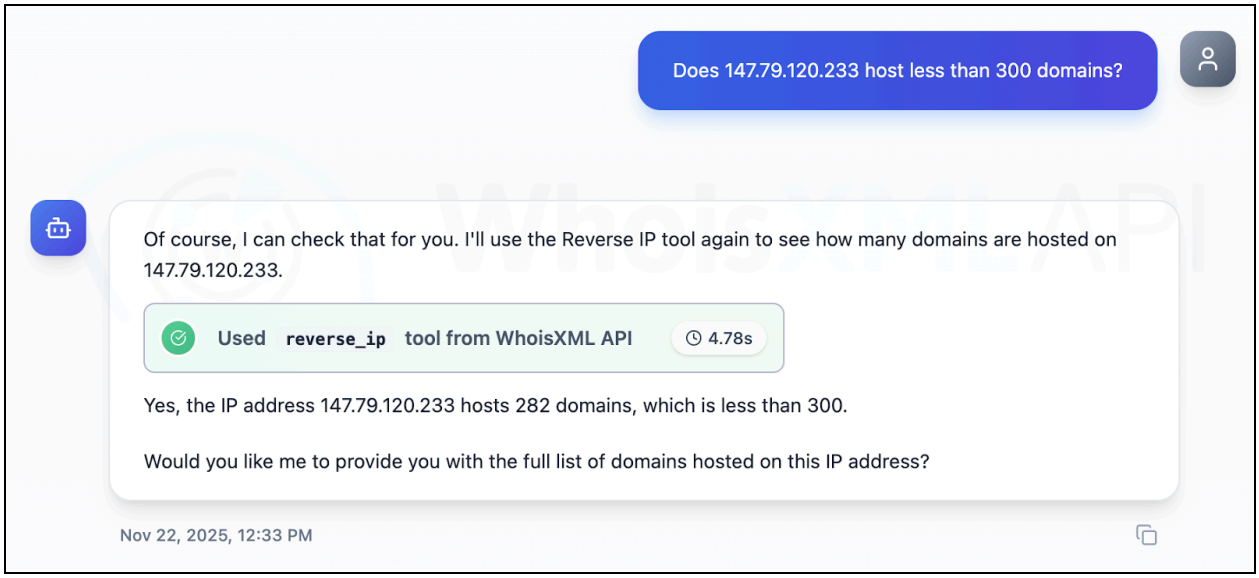
- They were geolocated in four countries. While eight IP addresses originated from the U.S., one each was geolocated in China, Germany, and Ukraine.



- While three IP addresses did not have ISPs on record, the remaining eight were administered by five ISPs. Four IP addresses were managed by Cloudflare while one each was administered by Alibaba, FranTech Solutions, Hetzner, and TelNet Worldwide.



Next, we queried the 11 IP addresses on Reverse IP API via Jake AI and discovered that three of them could be dedicated hosts. Altogether, the three possibly dedicated IP addresses hosted 104 IP-connected domains after filtering out duplicates, those already identified as IoCs, and the email-connected domains.



Sample Jake AI query result

To cap off our investigation, we scrutinized the 26 domains tagged as IoCs and extracted 26 unique text strings. Domains & Subdomains Discovery searches for them revealed that other domains started with these 15 strings:

- 365axissolution.
- ebuilderssource.
- emeraldpinesolutions.
- roofnrack.
- suziestuder.
- ply.
- buyedmeds.
- trendings.
- warpdrive.
- f3322.
- luyouxia.
- vip5944.
- digitbasket.
- lzh.
- marvelvod.

We uncovered 606 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 606 string-connected domains showed that one—warpdrive[.]store—has already been weaponized for phishing and generic threats on 27 March–27 September 2025 and 28 March–20 September 2025, respectively.

—

Our in-depth analysis of five of the top 10 malware of Q3 2025 revealed that two of the domains tagged as IoCs were deemed likely to turn malicious between 150 and 598 days before they were dubbed as such. In addition, one domain tagged as an IoC was bulk-registered with two look-alikes, making it a very likely typosquatter.

We also managed to dig up 5,987 new artifacts comprising 5,266 email-connected domains, 11 IP addresses, 104 IP-connected domains, and 606 string-connected domains. It is also worth noting that 64 of these newly discovered artifacts have already figured in malicious activity.

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

- 008680[.]com
- 016mu[.]com
- 01936[.]com
- a2glogistic[.]fr
- aa2017[.]com
- aaves-app[.]com
- b[.]coffee
- b71f4e05[.]sbs
- b7v7[.]com
- c0188[.]cn
- c0188[.]com
- c1c3[.]com
- d843[.]com
- dab123[.]com
- dadehua[.]com
- e130[.]com
- e90fd13bc2f3669fcccdbab0b561110c[.]in
- eajia[.]com
- f2i-cp33bis-ad[.]fr
- f3322[.]net
- f3800[.]com
- g51g[.]com
- g879[.]com
- gaimin[.]in
- h513[.]com
- haidao10[.]top
- haidaoxj[.]com
- i1118[.]com
- i183[.]cn
- i2346[.]com
- j3158[.]com
- j5566[.]com
- jacktix[.]com
- k0795[.]com
- k6266[.]com
- k6566[.]com
- l33l[.]com
- lab-outstanding-wind[.]com
- labobunerie[.]fr
- m-934betebet[.]com
- m-935betebet[.]com
- m-betcio59[.]com
- n8886[.]com
- n8sf[.]com
- nacreations[.]fr
- oakandsmokekw[.]com
- ocdmc[.]com
- octopink[.]fr
- p1681[.]com
- p1839[.]com
- p508[.]com
- q1861[.]com
- q1868[.]com
- q1918[.]com
- r1verside[.]us
- raagmemp3[.]com
- radical-lambda-uwu[.]com
- s4s6[.]com
- saafirbet[.]com
- saao49[.]fr
- t-me-idsid[.]us
- t1protocol[.]us
- t3m[.]us
- ua-zarahuvannja[.]com
- ue3hdn4-cdnsecurefile[.]com
- uetyszxedtsedzv[.]com
- v-betguncel[.]com
- v200[.]cn
- v5686[.]com
- w3gg[.]us
- w453[.]com

- w5688[.]com
- x-cas[.]com
- x-grok[.]us
- x-linkverification[.]com
- y1018[.]com
- y6555[.]com
- y9099[.]com
- z5z7[.]com
- z645[.]com
- z735[.]com

Sample IP Addresses

- 104[.]21[.]76[.]139
- 172[.]67[.]155[.]49
- 198[.]251[.]84[.]7
- 203[.]107[.]60[.]192
- 216[.]144[.]210[.]189
- 5[.]181[.]161[.]82
- 69[.]9[.]177[.]255
- 79[.]141[.]172[.]204

Sample IP-Connected Domains

- 0139eefd-52c4-42fa-b424-279b604c9084[.]random[.]buyanemostatonline[.]com
- 018aebaf-ce3c-4035-9eec-acf6acb1160b[.]random[.]buydoorlitesandlouvers[.]com
- 038d159d-b3bc-44dd-a0c4-bec68c0c4123[.]random[.]ebuilderssource[.]com
- admin[.]buydoorlitesandlouvers[.]com
- admin[.]buywashroomequipment[.]com
- api[.]buywashroomequipment[.]com
- bbs[.]buyelectricstrikesonline[.]com
- blog[.]buydoorlitesandlouvers[.]com
- blog[.]buymaglocksonline[.]com
- c02e0923-76e8-4f42-86d4-9f1152d2c841[.]random[.]buywashroomequipment[.]com
- c2b5b6ff-82b0-4bdd-a66e-4075b5167256[.]random[.]buyanemostatonline[.]com
- c5065b2b-16a3-4b4f-a8da-21ecedd8e267[.]random[.]buyintercomsonline[.]com
- d166ab3b-91ab-410f-a50d-c702fa55858d[.]random[.]buyanemostatonline[.]com
- d166ab3b-91ab-410f-a50d-c702fa55858d[.]random[.]buyintercomsonline[.]com
- d3f08448-5364-4150-a42f-44a88c1aafc6[.]random[.]buywashroomequipment[.]com
- e58318ec-a8b5-4a34-85e6-ba67642d089f[.]random[.]buyexitdevicesonline[.]com
- e9ee228b-57e8-4349-a41e-71a7b6d67aa2[.]random[.]buytvsecurityonline[.]com
- extranet[.]admin[.]buyelectricstrikesonline[.]com
- f27aea85-cc67-42ce-a110-bcfd1ca4d425[.]random[.]ebuildingsource[.]net
- faq[.]admin[.]buyexitdevicesonline[.]com
- financeiro7[.]fabricadesp[.]com
- links[.]admin[.]buydoorlitesandlouvers[.]com

- localhost[.]buywashroomequipment[.]com
- m[.]buywashroomequipment[.]com
- mail[.]buywashroomequipment[.]com
- mail[.]financeiro7[.]fabricadesp[.]com
- ns8[.]ebuilderssource[.]com
- pay[.]buywashroomequipment[.]com
- play[.]admin[.]buyexitdevicesonline[.]com
- pop[.]buyintercomsonline[.]com
- random[.]buywashroomequipment[.]com
- rd-9[.]ebuilderssource[.]com
- remote19[.]ebuilderssource[.]com
- securemail[.]ebuilderssource[.]com
- smtp[.]buyintercomsonline[.]com
- smtp[.]buywashroomequipment[.]com
- webdisk[.]buywashroomequipment[.]com
- webmail[.]buyintercomsonline[.]com
- webmail[.]buywashroomequipment[.]com

Sample String-Connected Domains

- 365axissolution[.]ws
- buyedmeds[.]com
- buyedmeds[.]shop
- digitbasket[.]net
- digitbasket[.]org
- ebuilderssource[.]net
- emeraldpinesolutions[.]ph
- emeraldpinesolutions[.]ws
- f3322[.]bid
- f3322[.]cf
- f3322[.]club
- luyouxia[.]cc
- luyouxia[.]club
- luyouxia[.]co
- lzh[.]ac[.]cn
- lzh[.]aero
- lzh[.]ah[.]cn
- marvelvod[.]xyz
- ply[.]ae
- ply[.]aero
- ply[.]ag
- roofnrack[.]com
- roofnrack[.]ph
- roofnrack[.]ws
- suziestuder[.]ws
- trendings[.]ai
- trendings[.]app
- trendings[.]art
- vip5944[.]cn
- vip5944[.]net
- vip5944[.]tk
- warpdrive[.]ae
- warpdrive[.]ai
- warpdrive[.]app