WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

DNS Deep Dive: TA416 European Government Espionage Campaigns

Threat Report

Table of Contents

Executive Report

Proofpoint reported that TA416 resumed their European government espionage activities about a month ago. Their researchers analyzed the campaigns in great depth and published 96 network IoCs comprising subdomains, domains, and email addresses in their report.

We extracted unique domains from the subdomain IoCs and filtered out those that could belong to legitimate entities with the help of the WhoisXML API MCP Server. This step allowed us to collate 91 IoCs for our analysis comprising 11 subdomains, 73 domains, and seven email addresses.

Our DNS deep dive into the TA416 espionage campaigns led to these discoveries:

- 122 unique client IP addresses that communicated with five of the domain IoCs
- Three domain IoCs that were bulk-registered with 5–15 look-alikes each
- 45,197 email-connected domains, 15 of which were confirmed malicious
- 69 IP addresses, 60 of which were confirmed malicious
- 117 IP-connected domains
- 295 string-connected domains

TA416 Attack Subdomain IoC Study

To kick off our investigation, we studied the 11 subdomain IoCs further.

The findings from our WhoisXML API MCP Server queries confirmed that three fell under confirmed malicious hostnames. And while many were hosted on legitimate infrastructure, six of them were still considered suspicious. Take a look at more specific information on five examples below.

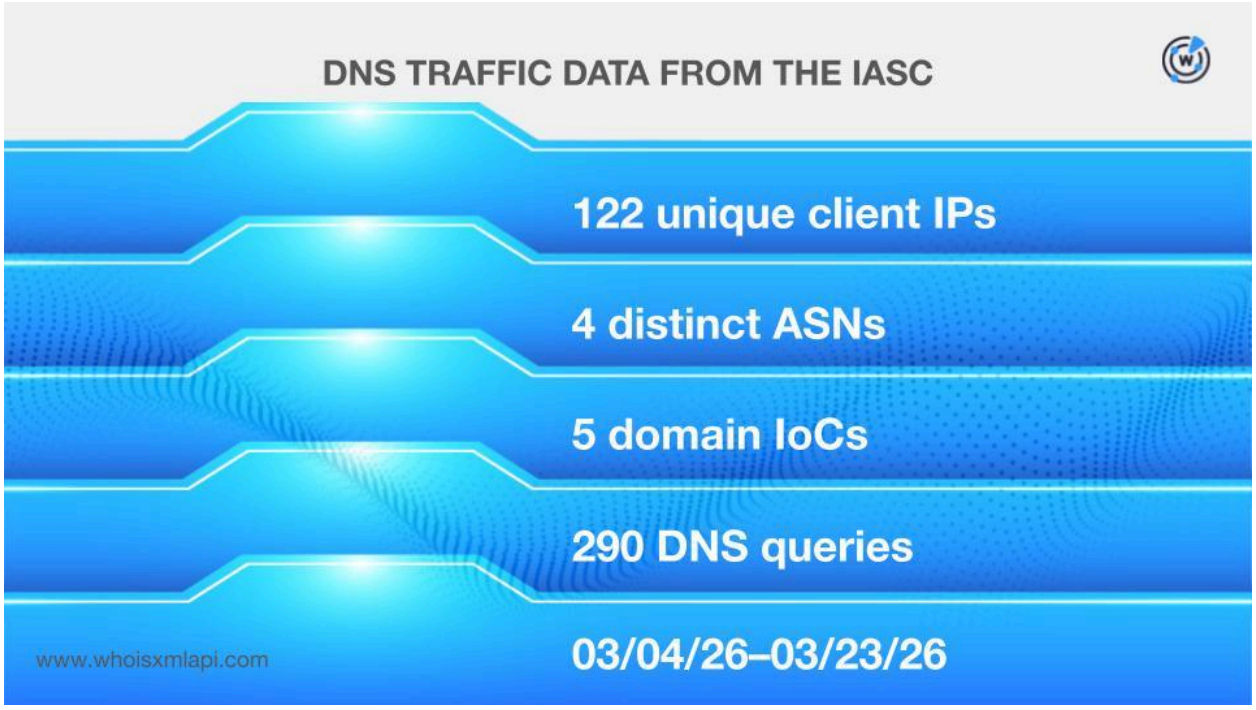
SUBDOMAIN IoC	WXA MCP SERVER FINDING
attd[.]z23[.]web[.]core[.]windows[.]net	While the apex domain is legitimate, the subdomain has been flagged for malware distribution
filestoretome[.]z23[.]web[.]core[.]windows[.]net	Since this sits in zone z23, which is a confirmed malware host, it may be worth blocking
gooledives[.]z48[.]web[.]core[.]windows[.]net	The most operationally active but has a very short TTL and possibly impersonates Google

mydownfile[.]z11[.]web[.]core[.]windows[.]net	A confirmed malware host with nearly identical activity as attd[.]z23[.]web[.]core[.]windows[.]net
mydownload[.]z29[.]web[.]core[.]windows[.]net	A confirmed malware host

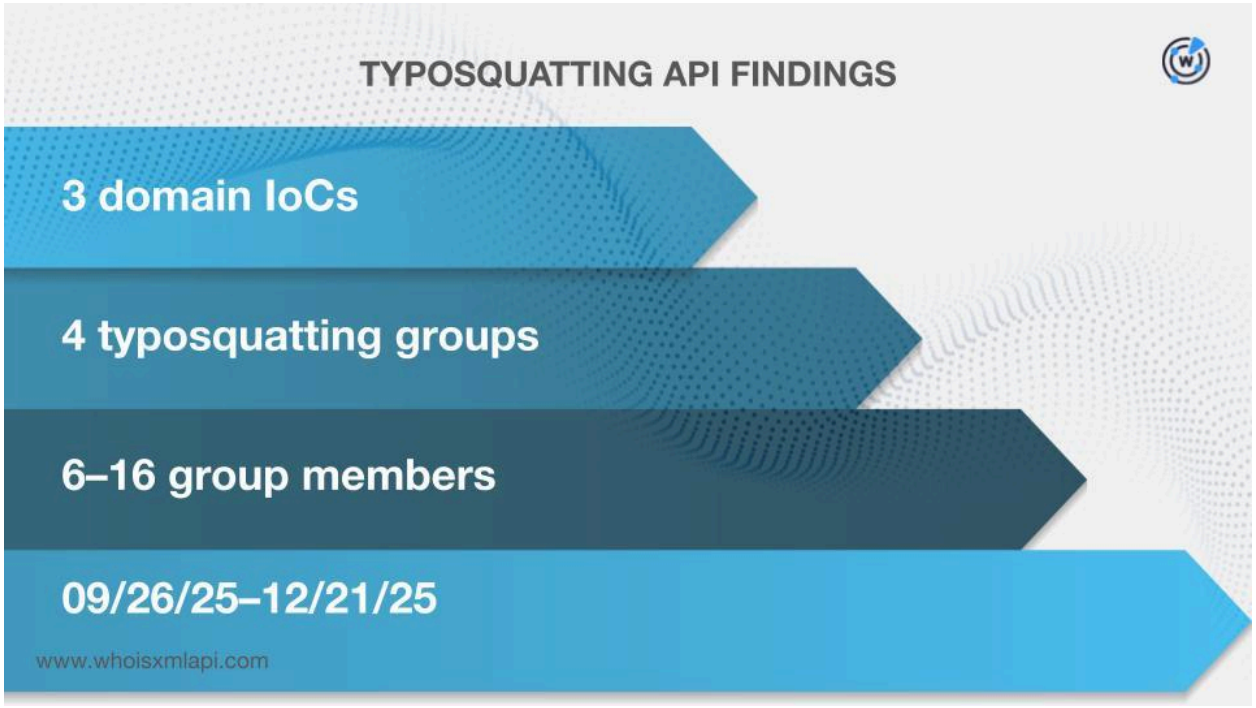
TA416 Attack Domain IoC Diagnosis

Next, we diagnosed the 73 domain IoCs some more.

First, sample network data from the IASC revealed that 122 unique client IP addresses under four distinct ASNs communicated with five of the domain IoCs via 290 DNS queries made between 4 and 23 March 2026.



Typosquatting API queries for the domain IoCs showed that three appeared in four typosquatting groups with 6–16 members each between 26 September and 21 December 2025.



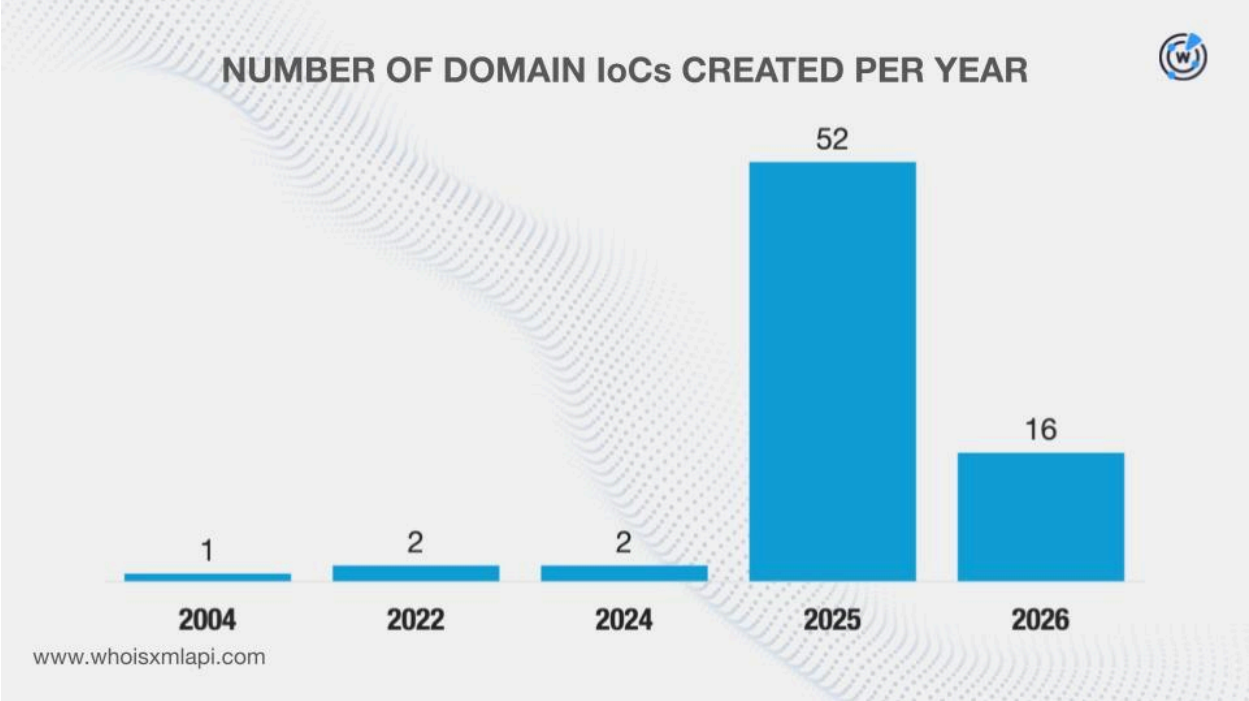
One of the domain IoCs—subusiness[.]org—appeared in two typosquatting groups. The first group had 12 members created between 15 and 16 December 2025. The second, meanwhile, had six members created between 15 and 21 December 2025. Here are more details about the two groups.

DOMAIN IoC	GROUP MEMBER NUMBER	LOOK-ALIKES	CREATION DATE
subusiness[.]org	12	jmbusiness[.]solutions zkbusiness[.]xyz nj-business[.]com jdbusiness[.]nl b3business[.]site allbusiness[.]onl albusiness[.]store aekbusiness[.]com dpbusiness[.]shop hybusiness[.]shop a2gbusiness[.]com	No date No date 12/16/25 12/16/25 No date 12/15/25 No date 12/16/25 12/16/25 12/16/25 12/16/25
subusiness[.]org	6	cnbusiness[.]net mybusiness[.]in[.]th 02business[.]co[.]uk combusiness[.]live	12/18/25 12/21/25 12/19/25 12/15/25

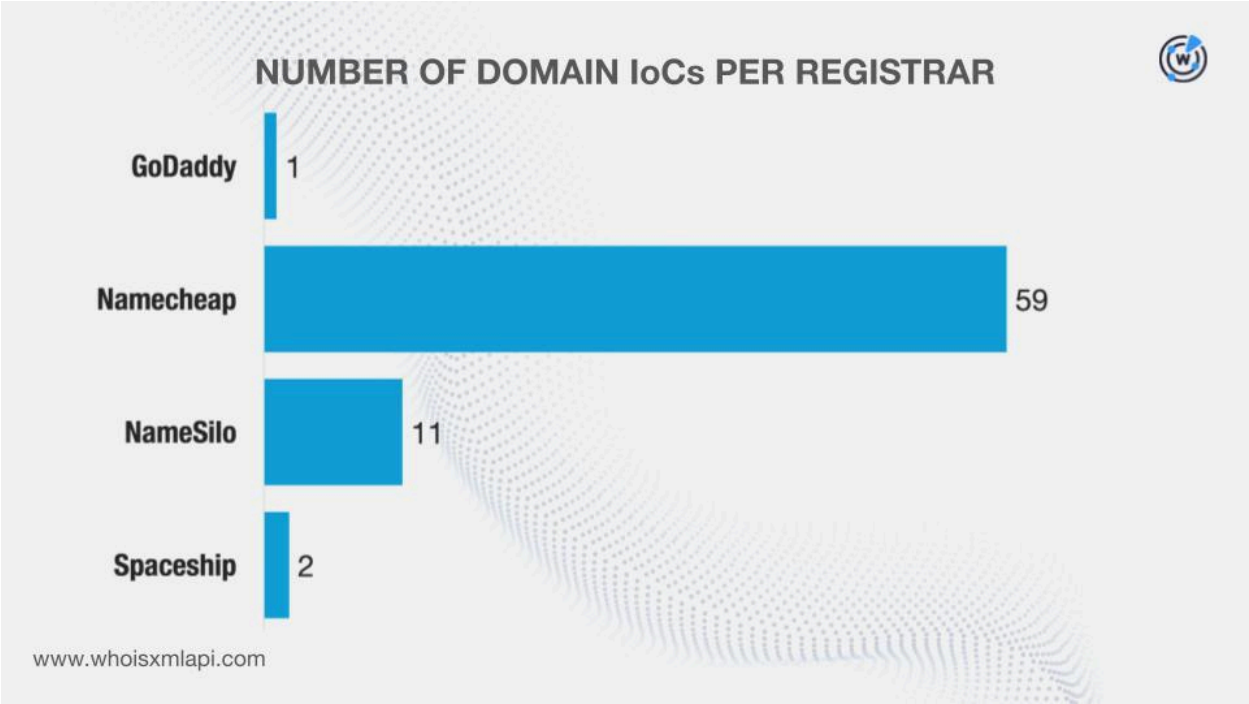
		carbusiness[.]biz	12/20/25

Next, we queried the domain IoCs on WHOIS API and discovered that:

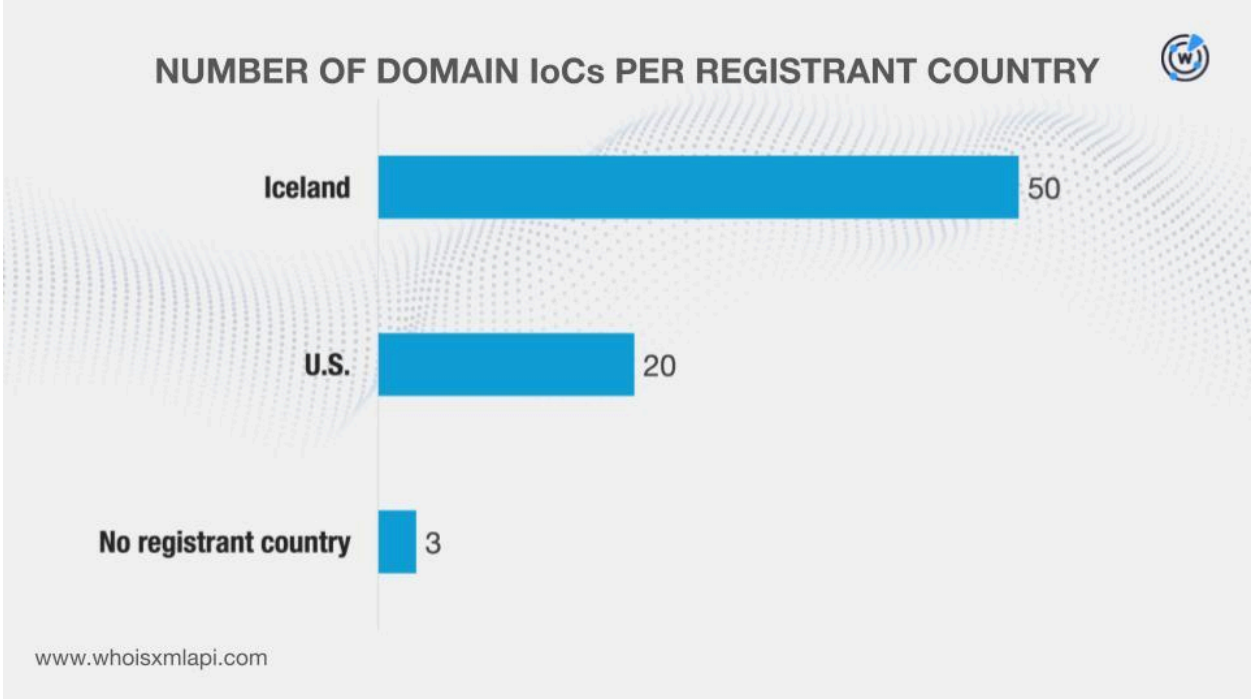
- They were created between 2 June 2004 and 19 March 2026, indicating that the threat actors used domains that were relatively new at the time the campaigns ensued.



- They were administered by four different registrars.



- While three did not have registrant countries on record, the remaining 70 were registered in two countries.



DNS Chronicle API queries for the domain IoCs revealed that all of them recorded 15,317 historical domain-to-IP resolutions over time. Take a look at more information for five examples below.

DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
aaitile[.]com	822	02/04/17–03/28/26
bobbush[.]org	553	02/05/17–01/06/26
stuypa[.]org	465	02/27/17–03/23/26
majicbus[.]org	430	02/06/17–12/23/25
ecolnomy[.]com	390	08/09/19–03/23/26

A total of 49 of the domain IoCs continued to post resolutions this year.

TA416 Attack Email IoC Examination

After that, we focused on the seven email IoCs.

We queried them on the WhoisXML API MCP Server and found out that:

- Only two remained active, meaning they passed SMTP verification. And both were Gmail addresses.
- None of them were used to register domains.

TA416 Attack New Artifact Hunting

After learning more about the IoCs, we then moved on to hunting for new artifacts.

We started by querying the 73 domain IoCs on WHOIS History API and discovered that 69 had 378 unique email addresses in their historical records. A closer look at them revealed that 88 were public email addresses.

Reverse WHOIS API queries for the public email addresses allowed us to discern that while three were not used as registrant email addresses, six could belong to domainers. The remaining 79 public email addresses, meanwhile, were used to register 45,197 unique email-connected domains after those already dubbed as IoCs were filtered out.

We then queried the email-connected domains on Threat Intelligence API and found out that 15 have already been weaponized for various attacks. Here are more details for five examples.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
chjq168[.]com	Phishing Generic threat	01/28/26–04/04/26 01/28/26–02/27/26
100viagra[.]com	Malware distribution	02/18/26–04/04/26
cisco-us[.]com	Malware distribution	05/06/25–04/04/26
downloadfreak[.]top	Malware distribution	06/11/25–04/03/26
e-brane[.]com	Phishing	03/06/26–04/04/26

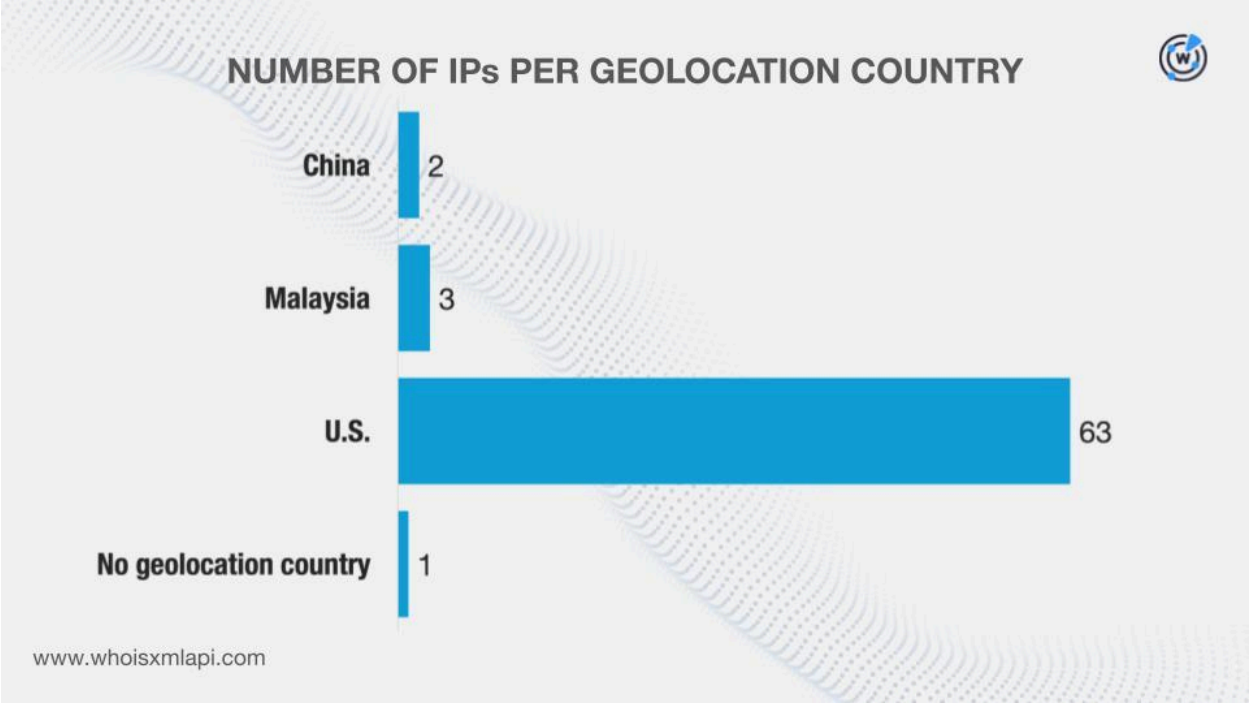
After that, we queried the domain IoCs on DNS Lookup API and discovered that 61 actively resolved to 69 unique IP addresses.

Threat Intelligence API queries for the IP addresses revealed that 60 have already figured in various malicious campaigns. Take a look at more information for five examples below.

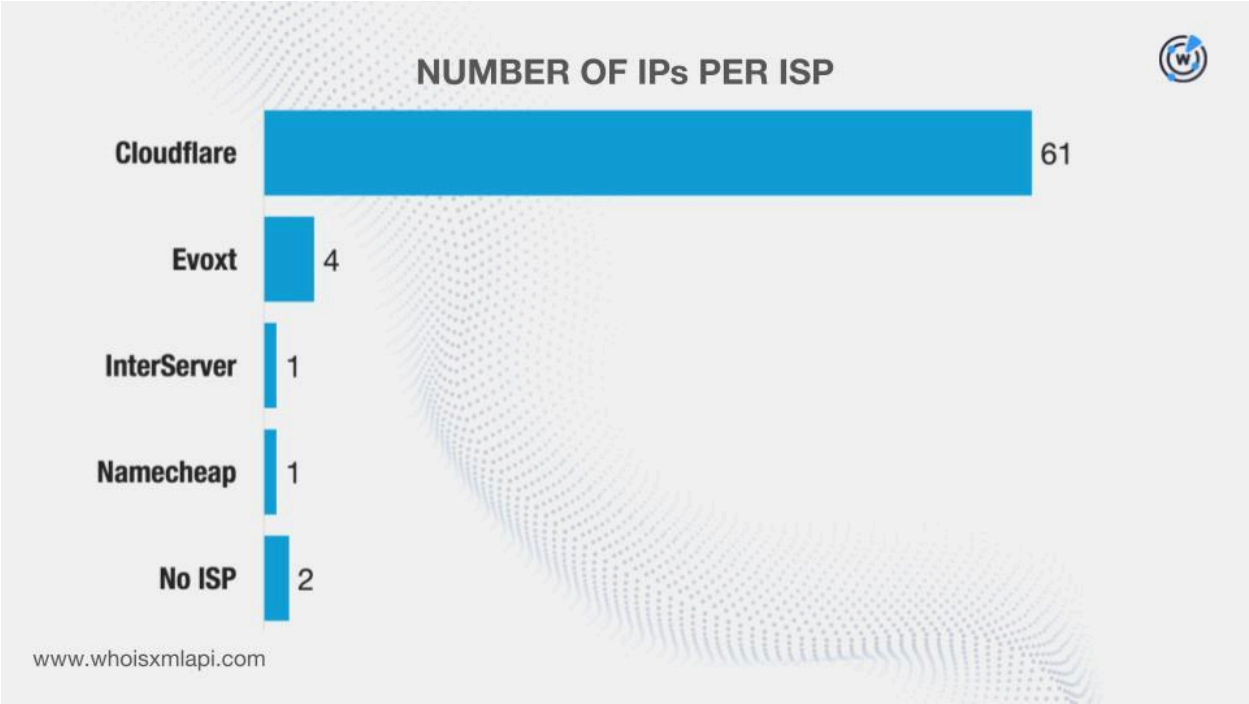
MALICIOUS IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
198[.]54[.]117[.]242	Malware distribution Generic threat Phishing C&C	03/09/23–04/05/26 03/28/23–04/05/26 03/28/23–04/05/26 04/22/23–02/08/26
104[.]21[.]20[.]57	Malware distribution Phishing Generic threat	07/27/23–04/05/26 05/30/23–04/04/26 08/29/23–03/03/26
104[.]21[.]30[.]7	Malware distribution Phishing	02/04/25–04/05/26 03/09/23–04/05/26
104[.]21[.]20[.]125	Malware distribution	10/29/24–04/04/26
104[.]21[.]37[.]73	Malware distribution Phishing	10/17/24–04/05/26 05/21/23–03/22/26

We then queried the IP addresses on Bulk IP Geolocation Lookup and learned that:

- While one did not have a geolocation country on record, the remaining 68 were geolocated in three different countries, one of which—the U.S.—was also a registrant country.



- While two did not have ISPs on record, the remaining 67 were administered by four different ISPs.



Reverse IP API queries for the IP addresses enabled us to determine that 69 were currently active. Further scrutiny revealed that five could be dedicated hosts. This step led to the discovery of 117 unique IP-connected domains after those already identified as IoCs and the email-connected domains were filtered out.

Next, we extracted 73 unique text strings from the domain IoCs. Aided by Domains & Subdomains Discovery, we searched for domains other than those already tagged as IoCs that started with the strings we identified. We found connections for 44 strings including but not limited to the following:

- aaitile.
- basecampbox.
- carhirechicago.
- dalerocks.
- ecoafrique.
- famisu.
- gesecole.
- harrietmwelch.
- majicbus.
- napasbdc.
- ombut.
- paquimetro.
- racineupci.
- shalomrav.
- thecamco.
- welnetsanda.
- ytsonline.

This step led to the discovery of 295 unique string-connected domains after those already named as IoCs and the email- and IP-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.

The Final Word

Our DNS deep dive into the TA416 attack led to some interesting facts about the IoCs. First, 122 unique client IP addresses communicated with five of the domain IoCs. We also learned that three of the domain IoCs were bulk-registered with 5–15 look-alikes each.

Our hunt for new artifacts, meanwhile, turned up 45,678 unique possibly connected web properties comprising 45,197 email-connected domains, 69 IP addresses, 117 IP-connected domains, and 295 string-connected domains. It is also worth noting that 75 of them have already been confirmed malicious.

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

- 0-60served[.]com
- 000[.]world
- 0000798[.]com
- a-1cellphones[.]com
- a-1contracting2125[.]com
- a-automotive[.]com
- b-b[.]xyz
- b-bonus[.]com
- b-it[.]xyz
- c-and-a[.]xyz
- c-doll[.]com
- c-hunter[.]com
- d-dubpress[.]com
- d-grafix[.]com
- d-link[.]xyz
- e-2-door[.]com
- e-anjie[.]com
- e-bay[.]xyz
- f-b[.]xyz
- f-designer[.]com
- f-fiber[.]com
- g-covers[.]com
- g-gold[.]com
- g20apps[.]com
- h-alali[.]cc
- h-c-c[.]com
- h-e-s[.]com
- i-am[.]xyz
- i-banq[.]com
- i-butler[.]xyz
- j-angda[.]com
- j-k[.]info
- j-k[.]xyz
- k-e-pix[.]com
- k-hitotuma[.]info
- k-m[.]online
- l-168[.]com
- l-immobilier-nantes[.]com
- l-l[.]xyz
- m-d[.]xyz
- m-e[.]xyz
- m-finfo[.]com
- n-aman[.]com
- n-iroha[.]com
- n-joy[.]xyz
- o-beiral[.]com
- o-kampus[.]com
- o-orz[.]com
- p-c[.]xyz
- p-f-h[.]org
- p1europe[.]com
- q-bao[.]com
- q-cells[.]xyz
- q-tech[.]xyz
- r-a[.]xyz
- r-autolease[.]com
- r-buraydah[.]com
- s-ax[.]com
- s-front[.]org
- s-gz[.]com
- t-cong[.]com
- t-labo-space[.]com
- t-nk33[.]com
- u-easypost[.]com
- u-meplace[.]com
- u-proirity[.]com
- v-fit[.]us
- v-tac[.]xyz
- v-you-media[.]com
- w-jsy[.]net
- w-srv[.]com
- w-theory[.]net
- x-media[.]xyz
- x-pole[.]xyz

- x1177[.]com
- y0ung[.]com
- y13[.]org
- y2k[.]xyz
- z-linefilter[.]com
- z-solution[.]com
- z0se[.]com

Sample IP Addresses

- 104[.]26[.]0[.]214
- 127[.]0[.]0[.]1
- 172[.]67[.]71[.]108
- 173[.]225[.]103[.]232
- 198[.]54[.]117[.]242
- 205[.]186[.]64[.]141
- 23[.]27[.]28[.]130

Sample IP-Connected Domains

- 1[.]theprmummy[.]com
- a[.]theprmummy[.]com
- backend[.]theprmummy[.]com
- cdn[.]theprmummy[.]com
- dan[.]theprmummy[.]com
- ftp[.]theprmummy[.]com
- game[.]theprmummy[.]com
- health[.]theprmummy[.]com
- ifloy[.]top
- kcnledger[.]com
- log[.]theprmummy[.]com
- magento[.]theprmummy[.]com
- new[.]theprmummy[.]com
- old[.]theprmummy[.]com
- panel[.]theprmummy[.]com
- qa[.]theprmummy[.]com
- recruit[.]theprmummy[.]com
- s[.]theprmummy[.]com
- t-mobile[.]theprmummy[.]com
- ups[.]theprmummy[.]com
- verizon[.]theprmummy[.]com
- wccheck-566ebed7-a[.]theprmummy[.]com

Sample String-Connected Domains

- aaitile[.]ws
- adimagemarketing[.]ph
- alpinemfg[.]ca
- amblecote[.]co
- basecampbox[.]de
- bobbush[.]co
- buscacnpj[.]com
- bushidomma[.]ca
- busopps[.]biz
- buzzurro[.]biz
- creatday[.]net
- cseconline[.]com
- dalerocks[.]us
- decoraat[.]com
- devredin[.]com[.]tr
- doorforum[.]ru
- ecoafrique[.]blog
- ecomputers[.]ae
- famisu[.]cn
- fuyuju[.]cn
- gesecole[.]com
- gestationsdiabetes[.]at
- ghonline[.]aquila[.]it
- gynecocuk[.]cd
- harrietmwelch[.]cf
- majicbus[.]biz
- mettayoga[.]ca
- mongolianews[.]com

- ombut[.]eu
- paquimetro[.]com
- phbusiness[.]biz
- phpthemes[.]com
- premegalithic[.]com[.]ws
- racineupci[.]com
- rhonline[.]app
- ronnybush[.]org
- shalomrav[.]co[.]uk
- stuypa[.]com
- subusiness[.]ch
- thecamco[.]co[.]uk
- winesnmore[.]co[.]ke
- ytsonline[.]co