WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A Look Back at 11 of the Red Report 2026 Featured Threats

Threat Report

Table of Contents

Executive Report

Picus Security, in Red Report 2026, identified the top 10 MITRE ATT&CK techniques in 2025 and named some of the groups that employed them. We zoomed in on 11 attacks featured in their report for six of the 10 ATT&CK techniques with their corresponding subtechniques where applicable in hopes of gathering more insights and collating additional artifacts.

MITRE ATT&CK TECHNIQUE/ SUBTECHNIQUE ABUSED	THREAT/ACTOR	THREAT/GROUP
T1036 Masquerading T1036.008 Masquerade File Type	UNC6384 abused file type masquerading to deliver STATICPLUGIN to diplomatic targets' systems	STATICPLUGIN
T1055 Process Injection T1055.004 Asynchronous Procedure Call	SadBridge Loader used APC injection as a key technique to execute malicious code within a legitimate process	SadBridge Loader
T1055 Process Injection T1055.004 Asynchronous Procedure Call	XLoader 6 and 7 used APC injection to execute their payloads within legitimate processes	XLoader 6 and 7
T1055 Process Injection T1055.003 Thread Execution Hijacking	NoisyBear used execution hijacking in Operation BarrelFire to run its payload under trusted processes	Operation BarrelFire
T1055 Process Injection T1055.002 Portable Executable Injection	ClickFix used PE injection to execute its final payload entirely in memory	ClickFix
T1059 Command and Scripting Interpreter T1059.006 Python	APT36 or Transparent Tribe demonstrated a significant evolution in their capabilities with the Python-based ELF malware	APT36 Python-Based ELF Malware
T1059 Command and Scripting Interpreter T1059.001 PowerShell	Chihuahua Stealer launched a compact PowerShell command that decoded a Base64 payload,	Chihuahua Stealer

	executing it in memory	
T1555 Credentials from Password Stores T1555.004 Windows Credential Manager	Earth Ammit enumerated credentials saved on compromised systems	Earth Ammit
T1562 Impair Defenses T1562.004 Disable or Modify System Firewall	Cryptojacking campaign leveraged Docker Swarm and Kubernetes for attack	Docker Swarm and Kubernetes Attack
T1562 Impair Defenses T1562.004 Disable or Modify System Firewall	PlushDaemon used the Ruler system to dynamically modify iptables firewall rules to intercept and manipulate network traffic on compromised systems	PlushDaemon
T1486 Data Encrypted for Impact	Earth Alux queried the MachineGUID value from the Windows Registry to serve as a persistent, unique identifier for each target host	Earth Alux

We obtained a total of 147 network IoCs from the abovementioned 11 analyses referenced in the report.

THREAT/GROUP	IoCs ANALYZED
STATICPLUGIN	Domain: 1 IPs: 2
SadBridge Loader	Subdomains: 5 Domains: 5
XLoader 6 and 7	Domains: 67
Operation BarrelFire	Domain: 1 IPs: 2
ClickFix	Subdomains: 7 Domains: 16 IPs: 3
APT36 Python-Based ELF Malware	Domain: 1

	IP: 1
Chihuahua Stealer	Subdomains: 2 Domains: 2
Earth Ammit	Subdomains: 7 Domains: 7 IPs: 3
Docker Swarm and Kubernetes Attack	Subdomain: 1 Domain: 1 IPs: 3
PlushDaemon	Subdomains: 2 Domain: 1 IPs: 2
Earth Alux	Subdomains: 2 Domains: 2 IP: 1

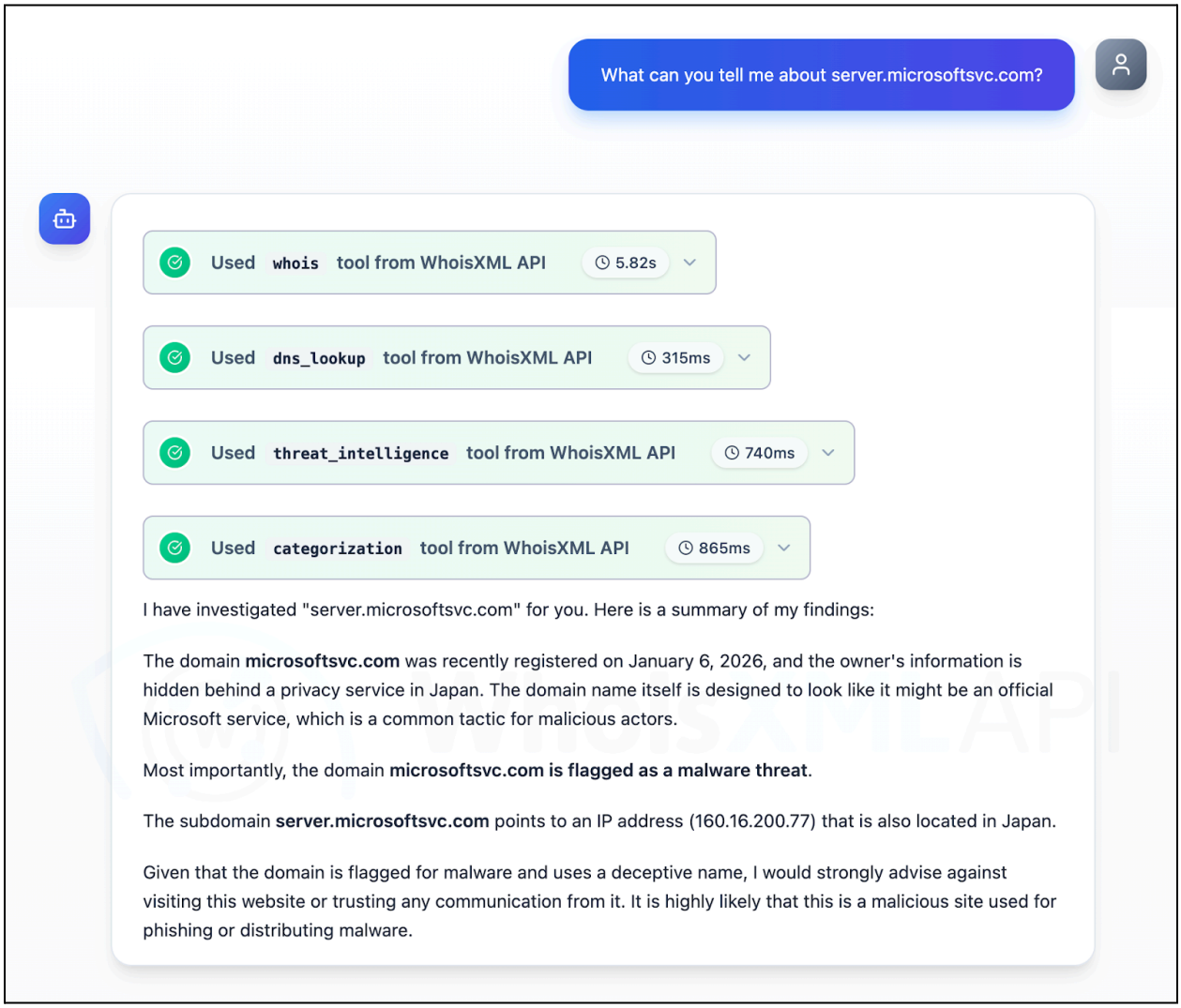
We analyzed the IoCs further, which led to these discoveries:

- 616 unique client IP addresses communicated with five domains identified as IoCs
- 23 domains classified as IoCs were bulk-registered with 2–936 look-alike domains each
- 28 domains tagged as IoCs deemed likely to turn malicious 46–516 days before they were reported as such
- Three unique potential victim IP addresses communicated with two IP addresses named as IoCs
- 7,770 email-connected domains, 25 were confirmed malicious
- 56 additional IP addresses, 46 were confirmed malicious
- 186 IP-connected domains, 143 were confirmed malicious
- 2,106 string-connected domains, two were confirmed malicious

More DNS Insights on the Subdomain IoCs

We began our analysis by looking for more information about the 26 subdomains identified as IoCs for seven of the 11 attacks via the WhoisXML API MCP Server.

We determined that while many of them were considered either benign or inactive, five have been confirmed as malicious—four related to Earth Ammit and one to Earth Alux.

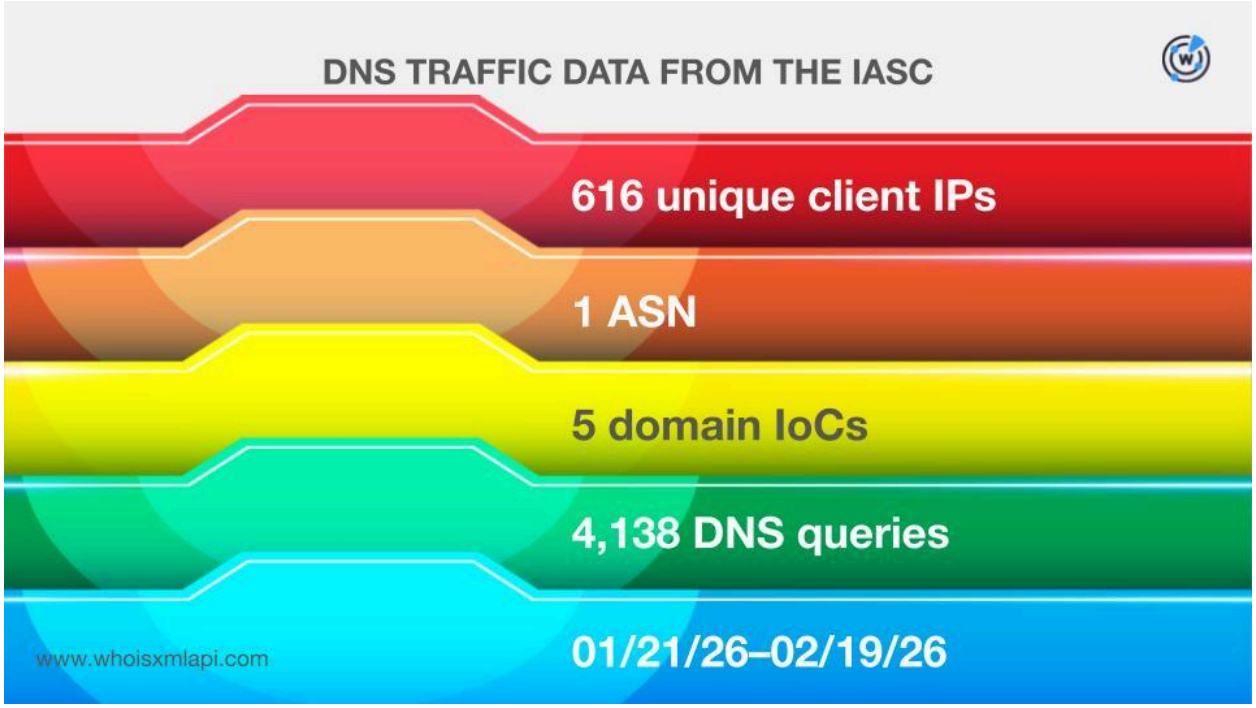


Jake AI result for the subdomain server[.]microsoftsvc[.]com that figured in the Earth Ammit attack

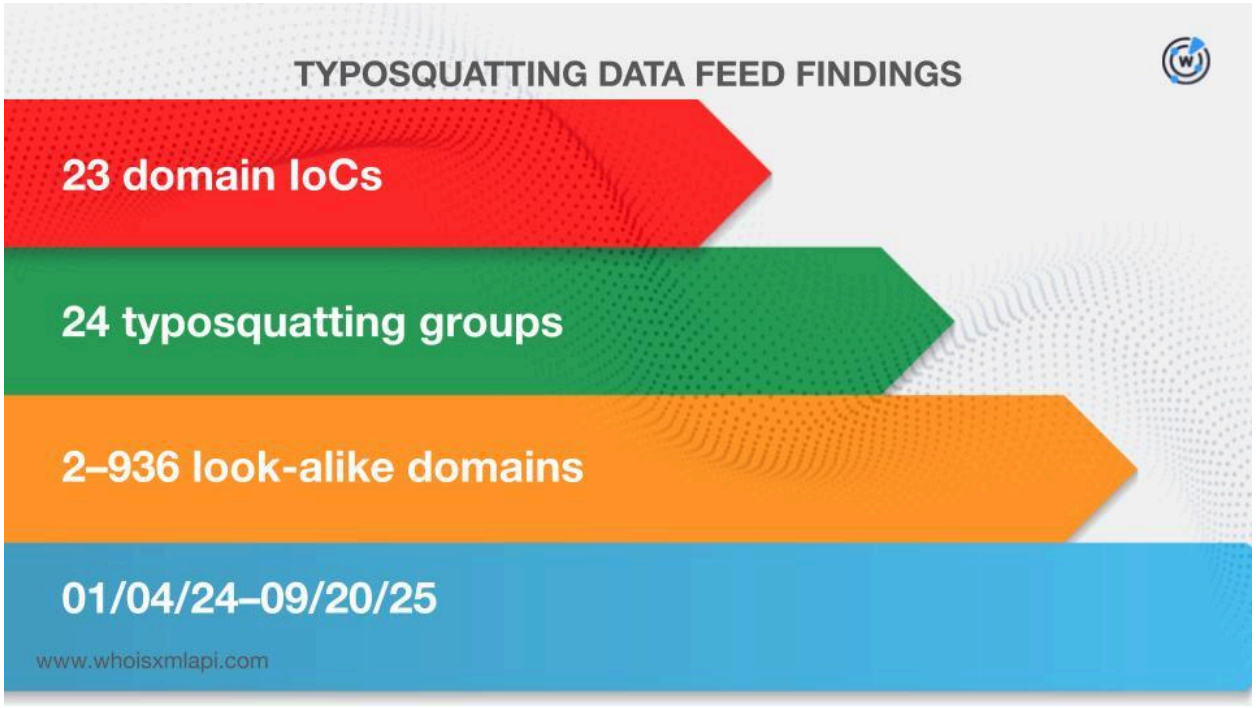
Additional DNS Facts Related to the Domain IoCs

As our next step, we sought out more details about the 104 domains identified as IoCs for the 11 threats.

Sample network traffic data from the IASC, for one, revealed that 616 unique client IP addresses under a single ASN communicated with five of the domains tagged as IoCs via a total of 4,138 DNS queries made between 21 January and 19 February 2026.



We sought to find out if any of the 104 domains named as IoCs appeared in the [Typosquatting Data Feed] and discovered that 23 were part of 24 typosquatting domain groups. Each was bulk-registered with 2–936 look-alikes between 4 January 2024 and 20 September 2025.

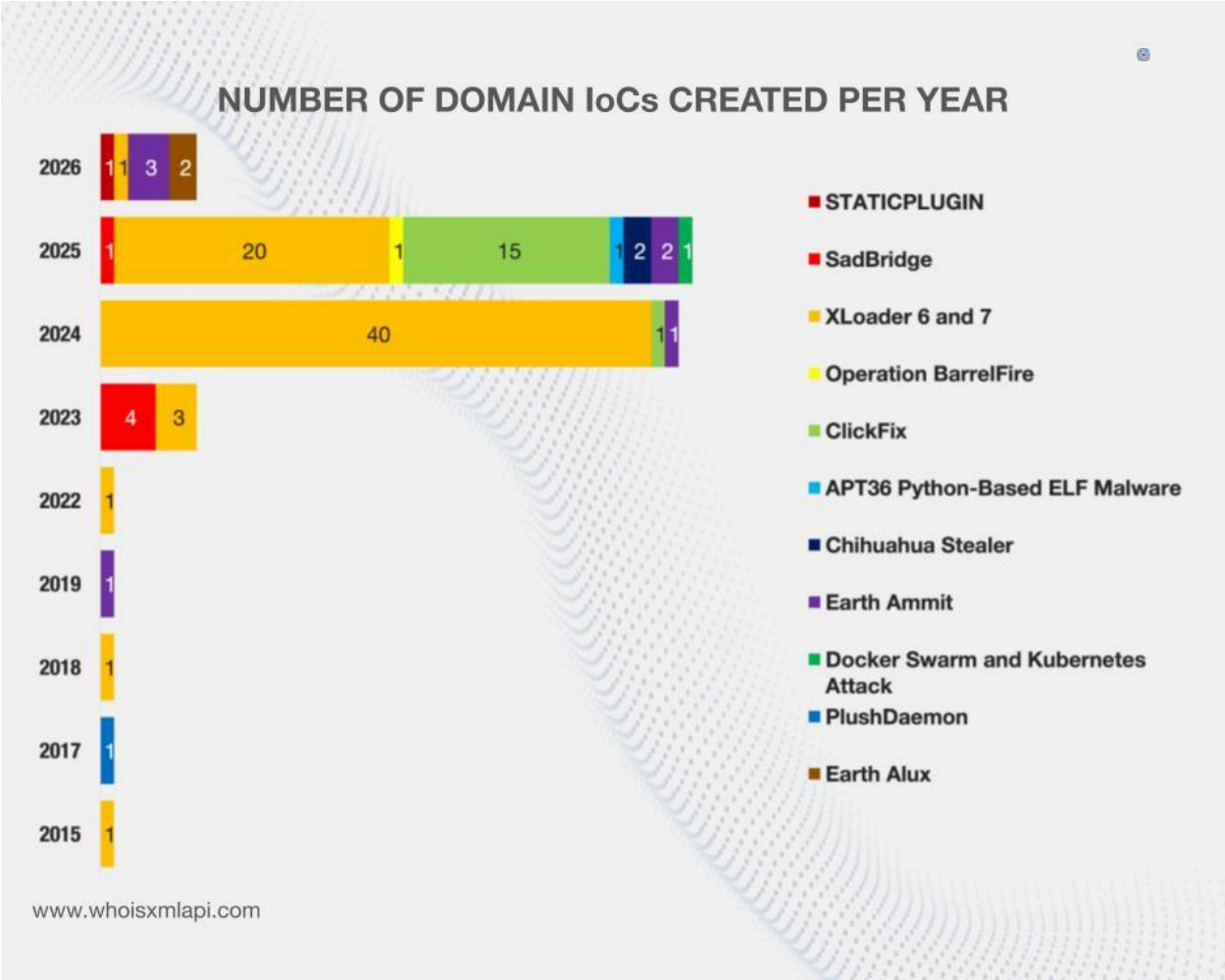


The results of our First Watch Malicious Domains Data Feed searches, meanwhile, showed that 28 of the domains categorized as IoCs for five threats could have been registered with malicious intent from the get-go. In fact, they were deemed likely to turn malicious 46–516 days before they were reported as IoCs. Take a look at more details for a domain related to each threat below.

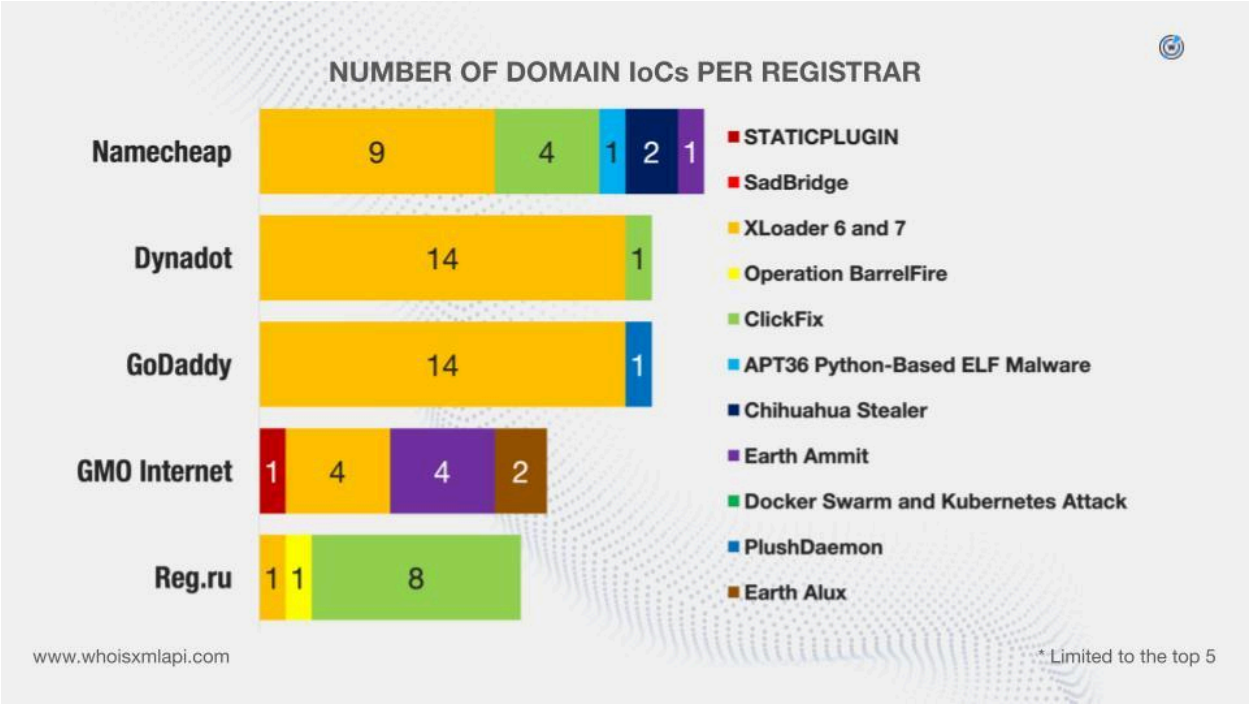
THREAT	DOMAIN IoC	FIRST WATCH INCLUSION DATE	NUMBER OF DAYS BEFORE REPORTING
STATICPLUGIN	mediareleaseupdates[.]com	07/20/24	402
XLoader 6 and 7	carpmaxxbait[.]online	11/24/23	430
ClickFix	groupewadesecurity[.]com	12/09/24	350
Chihuahua Stealer	cat-watches-site[.]xyz	01/25/25	164
Earth Ammit	symantecsecuritycloud[.]com	12/14/23	516

We then queried the 104 domains classified as IoCs on WHOIS API and discovered that:

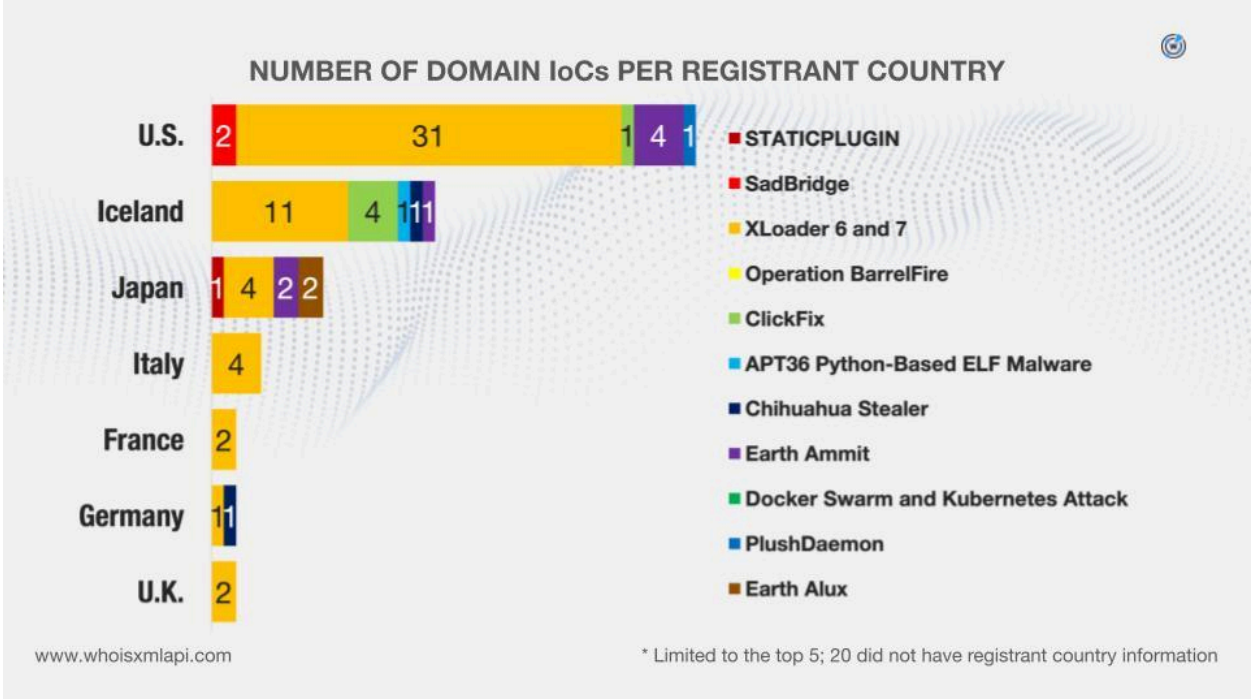
- They were created between 1 January 2015 and 9 February 2026, hinting at the threat actors' possible lack of preference in terms of domain age.



- They were administered by 29 different registrars.



- While 20 did not have registrant countries on record, the remaining 84 domains were registered in 15 different countries.



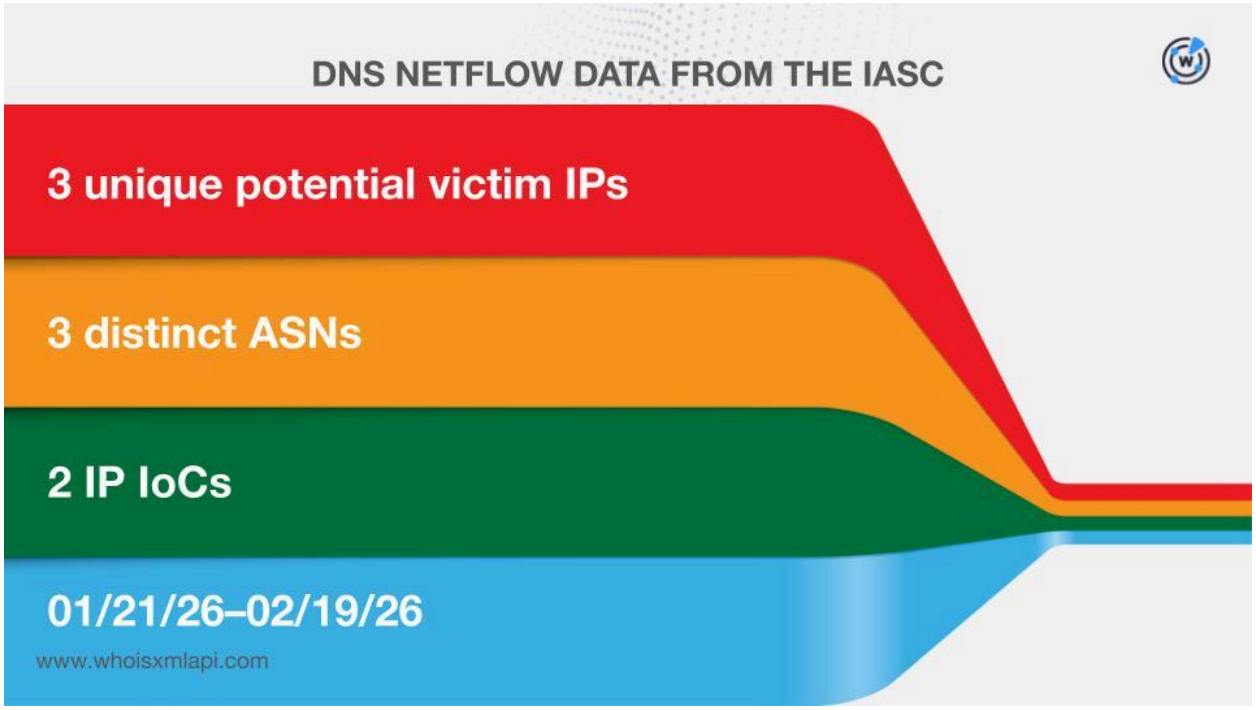
We also queried the 104 domains dubbed as IoCs on DNS Chronicle API and found out that 101 related to 10 threats have recorded 5,823 domain-to-IP resolutions over time. Here are details on a domain related to each threat.

THREAT	DOMAIN IoC	NUMBER OF RESOLUTIONS	TIME PERIOD
STATICPLUGIN	mediareleaseupdates[.]com	20	07/21/24–02/19/26
SadBridge	secssl[.]com	3	06/27/22–12/14/24
XLoader 6 and 7	alace5[.]com	519	02/05/17–02/06/26
Operation BarrelFire	wellfitplan[.]ru	8	04/14/25–02/09/26
ClickFix	galaxyswapper[.]pro	61	08/08/22–02/14/26
APT36 Python-Based ELF Malware	lionsdenim[.]xyz	3	11/03/25–11/30/25
Chihuahua Stealer	cat-watches-site[.]xyz	24	01/28/25–04/28/25
Earth Ammit	*uckeveryday[.]life	37	07/29/23–01/06/26
Docker Swarm and Kubernetes Attack	solscan[.]live	70	06/15/22–01/17/26
Earth Alux	upload-microsoft[.]com	6	11/20/23–02/19/26

Further DNS Discoveries about the IP IoCs

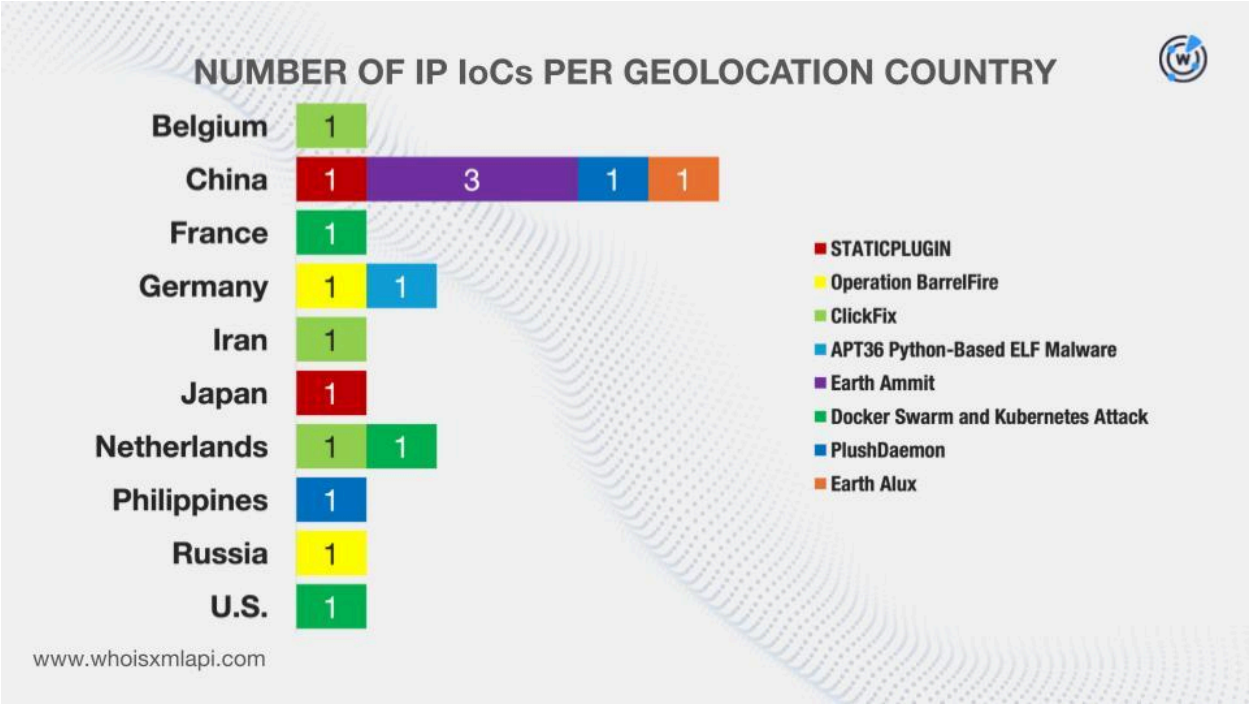
Next, we scoured the DNS for more information about the 17 IP addresses identified as IoCs for eight threats.

Sample network data from the IASC, for instance, revealed that three unique potential victim IP addresses under three distinct ASNs communicated with two IP addresses tagged as IoCs between 21 January and 19 February 2026.

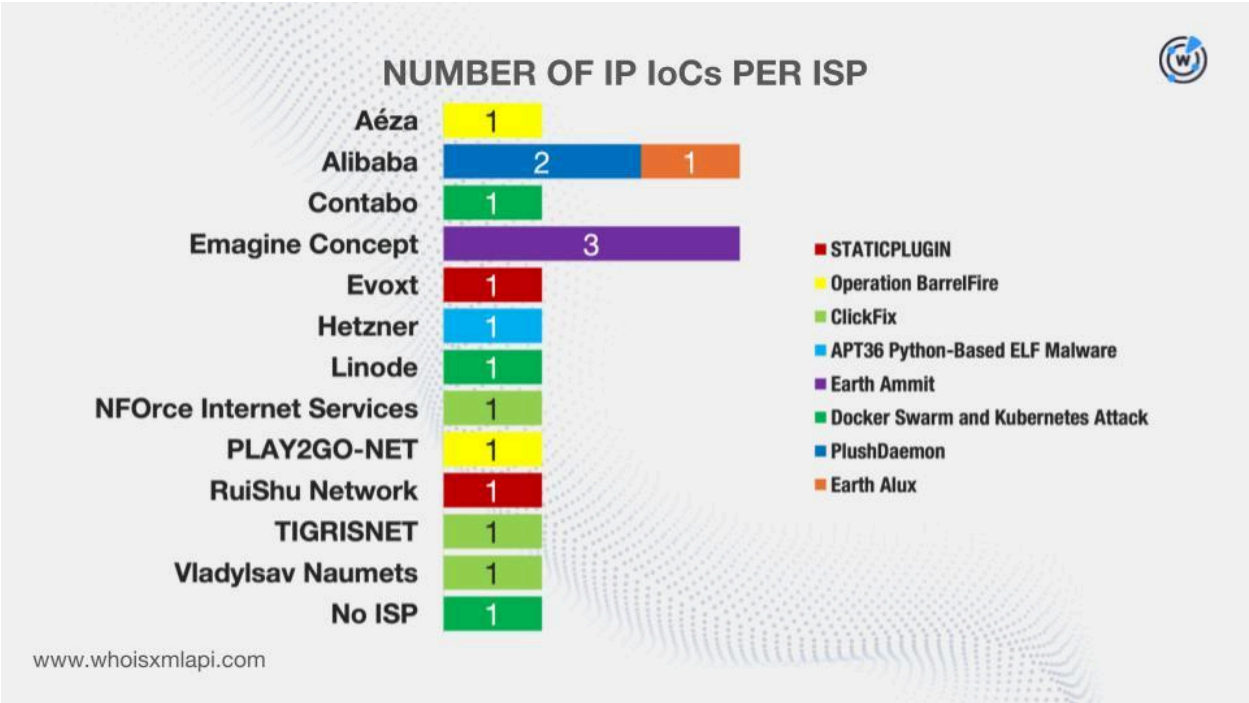


We then queried them on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in 10 countries. Note that five of them—China, France, Germany, Japan, and the U.S.—were also among the list of registrant countries of the domains classified as IoCs.



- While one did not have an ISP on record, the remaining 16 were administered by 12 ISPs.



DNS Chronicle API queries for the 17 IP addresses named as IoCs showed that 16 IPs related to eight threats recorded 1,842 IP-to-domain resolutions over time. Take a look at more information on an IP address related to each threat below.

THREAT	IP IoC	NUMBER OF RESOLUTIONS	TIME PERIOD
STATICPLUGIN	166[.]88[.]2[.]90	88	07/09/18–02/11/26
Operation BarrelFire	178[.]159[.]94[.]8	18	12/10/17–03/04/18
ClickFix	141[.]98[.]80[.]175	12	10/03/25–02/19/26
APT36 Python-Based ELF Malware	185[.]235[.]137[.]90	33	09/01/24–04/09/25
Earth Ammit	45[.]121[.]50[.]30	19	03/14/20–01/31/26
Docker Swarm and Kubernetes Attack	192[.]155[.]94[.]199	763	02/06/17–01/21/26
PlushDaemon	47[.]242[.]198[.]250	6	07/31/24–08/24/24
Earth Alux	8[.]218[.]222[.]216	2	01/23/26–02/15/26

Additional Threat Artifacts Unearthed

After gathering more details about the IoCs, we then scoured the DNS for additional connected artifacts.

First, we queried the 104 domains identified as IoCs on WHOIS History API and found out that 58 had 125 unique email addresses in their historical WHOIS records. Careful scrutiny allowed us to discern that 28 were public email addresses.

Reverse WHOIS API queries for the 28 public email addresses revealed that four could belong to domainers. This step also led to the discovery of 7,770 unique email-connected domains after those already listed as IoCs were filtered out.

According to Threat Intelligence API, 25 email-connected domains have already been weaponized for various threats. Here are more details for five of them.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
acrislegt[.]su	Malware distribution	09/09/25–02/19/26
averiryvx[.]su	Malware distribution	09/09/25–02/19/26
basilicros[.]su	Malware distribution	01/02/26–02/19/26
boustrn[.]su	Malware distribution	09/26/25–02/19/26
broguenko[.]su	Malware distribution	01/02/26–02/19/26

Next, we queried the 104 domains tagged as IoCs on DNS Lookup API. We learned that 73 of them resolved to 56 unique IP addresses not yet named as IoCs.

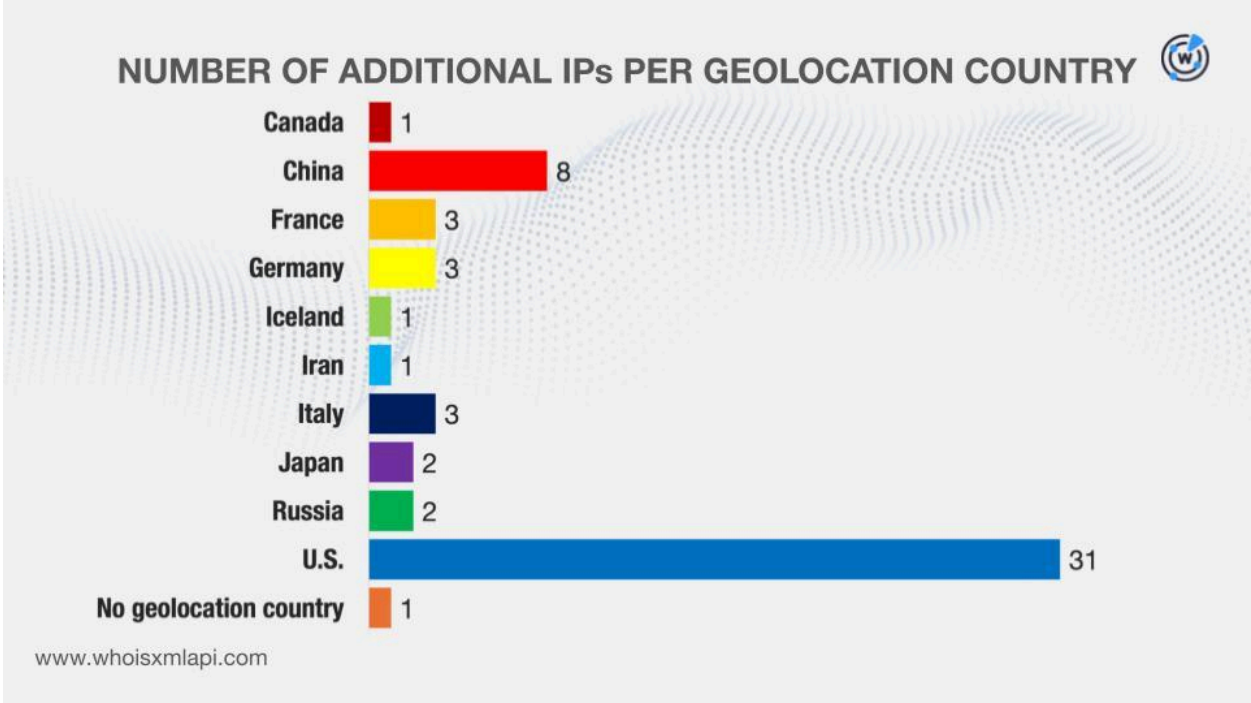
Threat Intelligence API queries for the 56 additional IP addresses showed that 46 have already figured in various attacks. Here are five examples.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
13[.]248[.]169[.]48	Phishing Generic threat Malware distribution C&C Spam campaign Suspicious activity	03/28/23–02/20/26 03/28/23–02/19/26 03/29/23–02/19/26 04/05/23–02/14/26 04/14/23–02/10/26 04/05/23–01/31/26
15[.]197[.]148[.]33	Phishing C&C Generic threat Malware distribution Spam campaign Suspicious activity	05/05/23–05/03/26 05/03/23–02/19/26 05/03/23–02/19/26 05/05/23–02/19/26 02/17/24–02/10/26 04/29/23–01/13/26
172[.]234[.]24[.]211	Phishing Malware distribution Generic threat C&C Spam campaign Suspicious activity	11/21/25–02/19/26 11/22/25–02/19/26 11/22/25–02/19/26 11/24/25–02/14/26 12/02/25–02/10/26 12/02/25–01/31/26
172[.]239[.]57[.]117	Malware distribution Phishing Generic threat	11/22/25–02/19/26 11/21/25–02/19/26 11/22/25–02/19/26

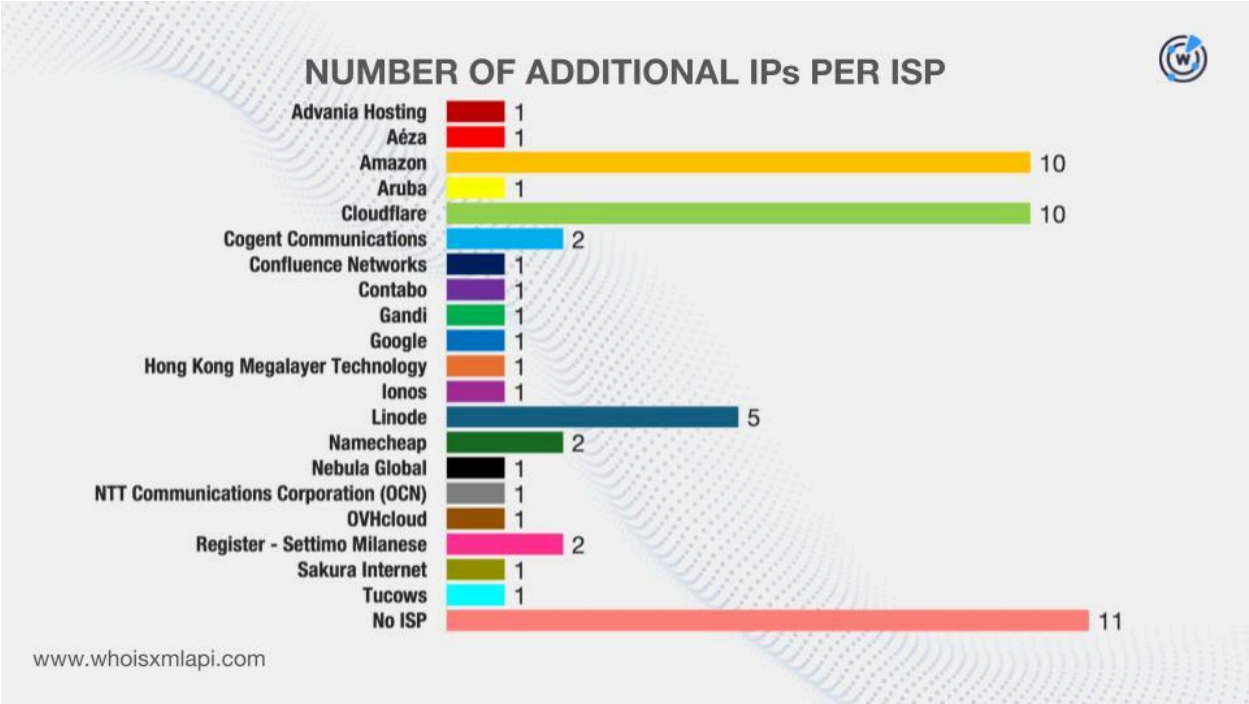
	C&C Spam campaign Suspicious activity	11/24/25–02/14/26 12/02/25–02/10/26 12/02/25–01/31/26
3[.]33[.]130[.]190	Phishing C&C Generic threat Malware distribution Spam campaign Suspicious activity	05/05/23–02/20/26 05/03/23–02/19/26 05/03/23–02/19/26 05/05/23–02/19/26 02/17/24–02/10/26 04/29/23–01/13/26

To know more about the 56 additional IP addresses, we queried them on Bulk IP Geolocation Lookup and discovered that:

- While one did not have a geolocation country on record, the remaining 55 were geolocated in 10 countries. Note, too, that they shared seven geolocation countries—China, France, Germany, Iran, Japan, Russia, and the U.S.—with the IP addresses classified as IoCs.



- While one did not have an ISP on record, the remaining 55 were administered by 20 ISPs, including Aéza, Contabo, and Linode, which also figured in the ISP list for the IP addresses listed as IoCs.



To continue the search for more artifacts, we queried the 73 IP addresses (17 categorized as IoCs and 56 additional) on Reverse IP API. Apart from learning that 17 of them could be dedicated hosts, we also uncovered 186 unique IP-connected domains after those already identified as IoCs and the email-connected domains were filtered out.

Threat Intelligence API showed that 143 of them have already been weaponized for various threats. Take a look at five examples below.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
absoluod[.]cyou	Malware distribution	01/24/26–02/19/26
aliengp[.]cyou	Malware distribution	01/30/26–02/19/26
aliveto[.]cyou	Malware distribution	02/16/26–02/19/26
amerimq[.]cyou	Malware distribution	01/30/26–02/19/26
apostrwz[.]cyou	Malware distribution	01/24/26–02/19/26

As our final step, we looked for domains that started with the same text strings as those already tagged as IoCs using Domains & Subdomains Discovery. We found 2,106 unique string-connected domains after those already named as IoCs and the email- and

IP-connected domains were filtered out. Here are some of the strings that appeared in the new artifacts:

- mediareleaseupdates.
- 030002304.
- aromavida.
- childlesscatlady.
- electra-airways.
- haftplicht.
- inf30027group23.
- moncoop.
- pethut.
- promasterev.
- sansensors.
- torex33.
- weatherbook.
- exposqw.
- xpoalswwkjddsljsy.
- symantecsecuritycloud.
- azure-clouds.

Threat Intelligence API queries for the string-connected domains revealed that two have already figured in malicious campaigns. An example is galaxyswapper[.]ru, which has already been involved with malware distribution between 23 March 2023 and 19 February 2026.

The Last Word

Our in-depth investigation of 11 threats connected to the top 10 MITRE ATT&CK techniques used in 2025 and featured in Picus Security's Red Report 2026 revealed that 616 unique client IP addresses communicated with five of the domains identified as IoCs. We discovered, too, that 23 domains classified as IoCs were bulk-registered with 2–936 look-alikes each. We also learned that 28 domains tagged as IoCs were deemed likely to turn malicious upon registration. In addition, three distinct potential victim IP addresses communicated with two IP addresses named as IoCs.

We were also able to collate 10,118 new artifacts comprising 7,770 email-connected domains, 56 additional IP addresses, 186 IP-connected domains, and 2,106 string-connected domains. It is worth noting that, to date, 216 of these newly discovered artifacts have already been weaponized for various 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

- 020jtcar[.]net
- 020x[.]net
- 021shanghaifap8[.]com
- a-1insurance[.]net
- a-1lawn1[.]net
- a-67[.]net
- b00r[.]com
- b20[.]xyz
- b21[.]xyz
- c-moderator[.]net
- c-oneschool[.]com
- c98[.]xyz
- d-slr-photo[.]com
- d-slr-photo[.]net
- d0zy[.]com
- e-juntas[.]net
- e-xiao[.]net
- e21[.]xyz
- f-morita[.]net
- f23[.]xyz
- fabricsofcolor[.]com
- g23[.]xyz
- g29[.]xyz
- g89[.]xyz
- h12[.]xyz
- h13[.]xyz
- h23[.]xyz
- i-hairstyle[.]net
- i-hp[.]net
- iak[.]us
- j3axx5[.]net
- jacksoncosmeticdentists[.]com
- jacksonpawn[.]com
- k23[.]xyz
- k29[.]xyz
- k77777[.]net
- l2argus[.]net
- l2orion[.]net
- labglassware[.]net
- m-c-h[.]net
- m-sign[.]net
- m-signature[.]net
- n16[.]xyz
- n22[.]xyz
- n23[.]xyz
- o32[.]xyz
- o89[.]xyz
- oabalegacyrenewed[.]com
- p23[.]xyz
- p67[.]xyz
- p92[.]xyz
- q91[.]xyz
- q92[.]xyz
- qalby[.]net
- r22[.]xyz
- r23[.]xyz
- r29[.]xyz
- sabayan[.]net
- sabiluna[.]net
- sabiri[.]net
- t-shits[.]net
- t123[.]xyz
- t21[.]xyz
- u-hoops[.]net
- u23[.]xyz
- u28[.]xyz
- v-care[.]net
- v-excel[.]net
- v98[.]xyz
- w2wtechnologysolutions[.]com
- w32[.]xyz
- w35[.]xyz
- x19[.]xyz
- x78[.]xyz

- x81[.]xyz
- y100[.]xyz
- y21[.]xyz
- y22[.]xyz
- z92[.]xyz
- zaba[.]info
- zafarsazangroup[.]com

Sample Additional IP Addresses

- 13[.]248[.]169[.]48
- 15[.]197[.]148[.]33
- 172[.]234[.]24[.]211
- 172[.]239[.]57[.]117
- 3[.]33[.]130[.]190
- 76[.]223[.]54[.]146
- 91[.]195[.]240[.]94
- 172[.]233[.]221[.]214
- 172[.]234[.]199[.]15
- 172[.]237[.]145[.]27
- 208[.]91[.]197[.]27
- 34[.]41[.]139[.]193
- 103[.]224[.]212[.]211
- 104[.]21[.]78[.]169
- 172[.]67[.]136[.]4
- 195[.]110[.]124[.]133
- 217[.]70[.]184[.]38
- 3[.]238[.]30[.]69
- 34[.]209[.]195[.]255
- 37[.]77[.]150[.]171
- 52[.]27[.]79[.]221
- 54[.]146[.]6[.]253
- 81[.]88[.]63[.]46

Sample IP-Connected Domains

- 28s[.]me
- 28wad[.]top
- 28wbd[.]top
- absoluod[.]cyou
- admin[.]rxhbjl[.]bfres[.]xyz
- aliengp[.]cyou
- backsan[.]cyou
- ballisr[.]cyou
- belloww[.]cyou
- c7niu[.]cc
- capacif[.]cyou
- capitamx[.]cyou
- dameagm[.]cyou
- darkisq[.]cyou
- dearlove520vip[.]top
- ebonizz[.]cyou
- ectrodm[.]cyou
- editorr[.]cyou
- fistens[.]com
- fomodog[.]org
- francek[.]cyou
- g17c198[.]tz2[.]iflvopx[.]net
- g204c31[.]tz4[.]iflvopx[.]net
- g5d3dbe[.]tz3[.]iflvopx[.]net
- haeccee[.]cyou
- hanggxx[.]cyou
- hook[.]rxbjpk10[.]bfres[.]xyz
- imageod[.]cyou
- inconsk[.]cyou
- interrg[.]cyou
- judicis[.]cyou
- kenaifj[.]live
- khantym[.]cyou
- killnnk[.]cyou
- lacevcnt[.]cyou
- lawyer-online[.]online
- leafyrm[.]cyou
- manufao[.]cyou
- marktwx[.]cyou
- marrueye[.]cyou

- ng015[.]com
- oculusr[.]cyou
- odovakmc[.]cyou
- offdutd[.]cyou
- penmank[.]cyou
- pepperz[.]cyou
- personrg[.]cyou
- recyclqb[.]cyou
- regreso[.]cyou
- requieiy[.]cyou
- sanicue[.]cyou
- saudiab[.]cyou
- scarfkn[.]cyou
- tasselg[.]cyou
- theengn[.]cyou
- thoughg[.]cyou
- unaideg[.]cyou
- unchewq[.]cyou
- underpt[.]cyou
- versedv[.]cyou
- vesicak[.]cyou
- vetchir[.]cyou
- wc28[.]ws
- wc288[.]app
- wd22[.]vip
- xn--2hv367j[.]co
- xn--4fa[.]cc
- xn--53ts49arxx[.]cc
- yarddrq[.]cyou
- yelloww[.]cyou
- ziziphe[.]cyou
- zsdoaoockamkwsmna[.]com

Sample String-Connected Domains

- 030002304[.]ph
- 030002304[.]ws
- 44ddw[.]com
- 44ddw[.]ph
- airbatchnow[.]cloud
- airbatchnow[.]com
- airbatchnow[.]info
- allsolar[.]app
- allsolar[.]be
- allsolar[.]berlin
- allthingsjasmin[.]ph
- allthingsjasmin[.]ws
- aromavida[.]com
- aromavida[.]com[.]ar
- aromavida[.]com[.]br
- azure-clouds[.]ph
- azure-clouds[.]ws
- bendavo[.]com
- bkexclusivecars[.]com
- bkexclusivecars[.]eu
- bkexclusivecars[.]fr
- bluegirls[.]be
- bluegirls[.]biz
- bluegirls[.]ch
- carpmaxxbait[.]com
- chalet-tofane[.]com
- chalet-tofane[.]eu
- chalet-tofane[.]info
- childlesscatlady[.]art
- childlesscatlady[.]biz
- childlesscatlady[.]blog
- conxmsw[.]ph
- conxmsw[.]ws
- d27dm[.]info
- d27dm[.]ph
- d27dm[.]ws
- dto20[.]com
- dto20[.]ph
- dto20[.]ws
- easestore[.]ca
- easestore[.]club
- easestore[.]cn
- eeja[.]art
- eeja[.]cc
- eeja[.]club
- electra-airways[.]biz

- electra-airways[.]co
- electra-airways[.]com
- everycreation[.]cn
- everycreation[.]com
- everycreation[.]in
- exposqw[.]ph
- exposqw[.]ws
- fghytr[.]club
- fghytr[.]cn
- fghytr[.]net
- fraternize[.]arab
- fraternize[.]biz
- fraternize[.]cc
- fuckeveryday[.]club
- fuckeveryday[.]com
- fuckeveryday[.]info
- galaxyswapper[.]cc
- galaxyswapper[.]com
- galaxyswapper[.]fun
- getmylinks[.]club
- getmylinks[.]co
- getmylinks[.]co[.]uk
- googledns[.]app
- googledns[.]biz
- googledns[.]ch
- greekhause[.]ph
- greekhause[.]ws
- haftplicht[.]de
- haftplicht[.]online
- haftplicht[.]versicherung
- happiluv[.]com[.]my
- hentaistgma[.]ph
- hentaistgma[.]ws
- hk9[.]ae
- hk9[.]app
- hk9[.]aquila[.]it
- huemanstudio[.]agency
- huemanstudio[.]co[.]uk
- huemanstudio[.]com
- inf30027group23[.]ph
- iwin[.]abogado
- iwin[.]ac
- iwin[.]ac[.]vn
- komart[.]at
- komart[.]au
- komart[.]az
- lojashelp[.]com
- lojashelp[.]com[.]br
- lojashelp[.]online
- mag-flex[.]online
- mag-flex[.]pl
- mediareleaseupdates[.]ph
- mediareleaseupdates[.]ws
- metyp9[.]ph
- microsoftsvc[.]ph
- microsoftsvc[.]ws
- moncoop[.]cat
- moncoop[.]com
- moncoop[.]com[.]es
- myhosting[.]ag
- myhosting[.]agency
- myhosting[.]ai
- ngmr[.]bid
- ngmr[.]biz
- ngmr[.]cfd
- ntn[.]ac[.]cn
- ntn[.]academy
- ntn[.]ae
- ohio-adr[.]com
- ohio-adr[.]info
- ohio-adr[.]org
- opera-x[.]co[.]uk
- opera-x[.]com
- opera-x[.]info
- ozonelf[.]ph
- ozonelf[.]ws
- pethut[.]au
- pethut[.]ca
- pethut[.]cc
- platinumkitchens[.]ca
- platinumkitchens[.]co[.]uk
- platinumkitchens[.]com

- polarmuseum[.]co[.]uk
- polarmuseum[.]com
- polarmuseum[.]net
- portfutures[.]africa
- portfutures[.]biz
- portfutures[.]co[.]uk
- projectimprov[.]org
- promasterev[.]ai
- promasterev[.]app
- promasterev[.]club
- queima[.]club
- queima[.]com
- queima[.]com[.]br
- resumeyourway[.]blog
- resumeyourway[.]ca
- resumeyourway[.]co[.]nz
- revelationfithub[.]co[.]uk
- rtpngk[.]club
- rtpngk[.]online
- rtpngk[.]ph
- sansensors[.]biz
- sansensors[.]co[.]in
- sansensors[.]com
- scwspark[.]co[.]uk
- secssl[.]cn
- secssl[.]de
- secssl[.]online
- securitysettings[.]app
- securitysettings[.]cf
- securitysettings[.]com
- serverplay[.]click
- serverplay[.]com
- serverplay[.]com[.]br
- softillery[.]co
- softillery[.]com
- softillery[.]net
- solscan[.]ad
- solscan[.]agency
- solscan[.]ai
- squatje[.]ph
- squatje[.]ws
- symantecsecuritycloud[.]ph
- symantecsecuritycloud[.]ws
- teledown-cn[.]ph
- theproselytizer[.]ai
- theproselytizer[.]com
- theproselytizer[.]info
- torex33[.]ph
- torex33[.]ru
- torex33[.]ws
- tracy[.]ac
- tracy[.]agency
- tracy[.]ai
- trisixnine[.]com
- trisixnine[.]eu
- trisixnine[.]it
- upload-microsoft[.]ph
- upload-microsoft[.]vg
- upload-microsoft[.]ws
- vegastinyhomes[.]ai
- vegastinyhomes[.]app
- vegastinyhomes[.]com
- vmwaresync[.]ph
- vmwaresync[.]ws
- wcsset[.]ph
- wcsset[.]top
- wcsset[.]ws
- wdeb18[.]ph
- wdeb18[.]ws
- weatherbook[.]cn
- weatherbook[.]co
- weatherbook[.]com
- wellfitplan[.]com
- windowswns[.]tk
- xpoalswwkjddsljsy[.]ph
- yu35n[.]cc
- yu35n[.]cn
- yu35n[.]tech