New MITRE ATT&CK Groups for 2025: A DNS Deep Dive

Table of Contents

Executive Report

The MITRE Corporation updates its list of groups on the ATT&CK page every six months, specifically in April and October each year. The Updates - April 2025 advisory listed seven new groups with corresponding lists of indicators of compromise (IoCs) listed in the References section. Take a look at specific IoC-related details for each group below.

GROUP	NUMBER OF DOMAIN IoCs	NUMBER OF IP ADDRESS IoCs	TOTAL NUMBER OF IoCs
APT42	148	2	150
BlackByte	3	2	5
RedEcho	15	43	58
Salt Typhoon	0	2	2
Sea Turtle	13	50	63
Storm-1811	10	8	18
Velvet Ant	0	2	2

In a bid to uncover more potentially connected artifacts, WhoisXML API expanded the current IoC lists in this post. Our in-depth analysis led to the discovery of:

- Three alleged victim IP records obtained from the Internet Abuse Signal Collective (IASC) tied to three Autonomous System (AS) numbers
- 638 email-connected domains, six are malicious
- 26 additional IP addresses, 16 are malicious

- 221 IP-connected domains
- 4,195 string-connected domains, 37 are malicious

New MITRE ATT&CK Group IoC Facts

We began our analysis by querying the 189 domains identified as IoCs on Bulk WHOIS API by group.

We found that only 99 of the 189 domains had current WHOIS records. Here is a summary of our creation date-related findings for the five groups with domain IoCs.

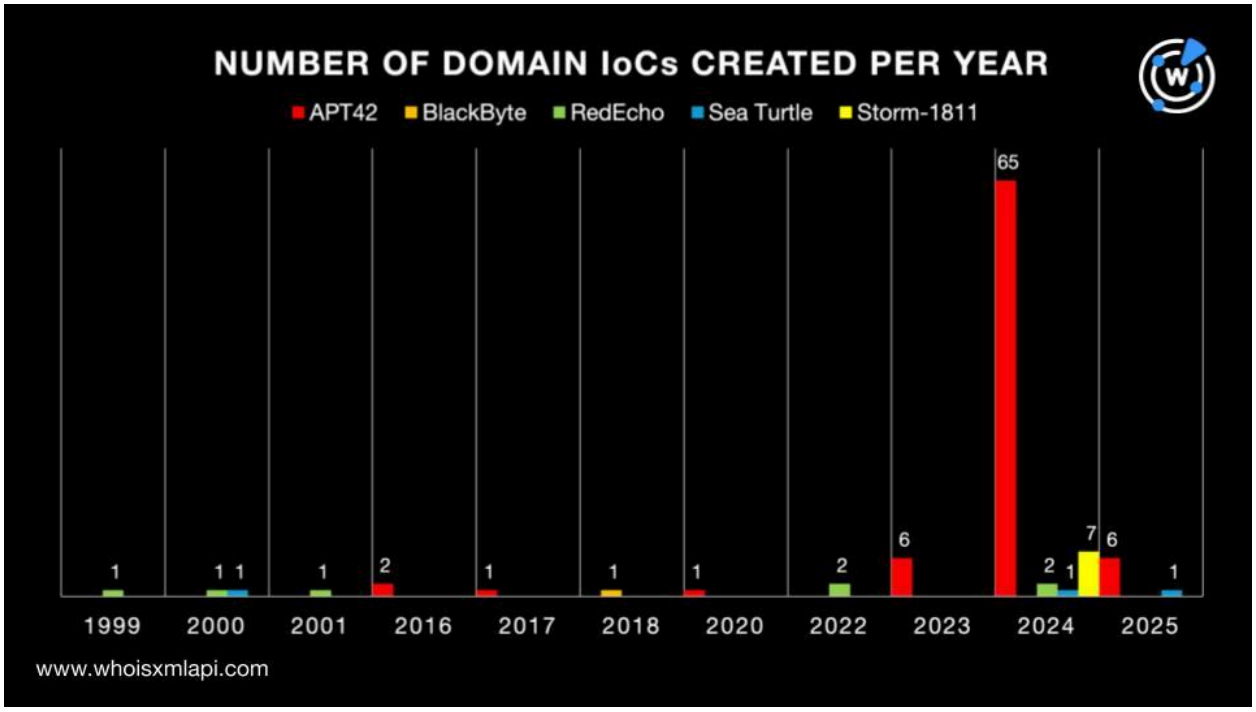
- **APT42:** Only 81 of the 148 domains identified as IoCs had current WHOIS records. The 81 domains were created between 2016 and 2025.

- **BlackByte:** One of the three domain IoCs had a current WHOIS record. The domain was created in 2018.

- **RedEcho:** Only seven of the 15 domain IoCs had current WHOIS records. The seven domains were created between 1999 and 2024.

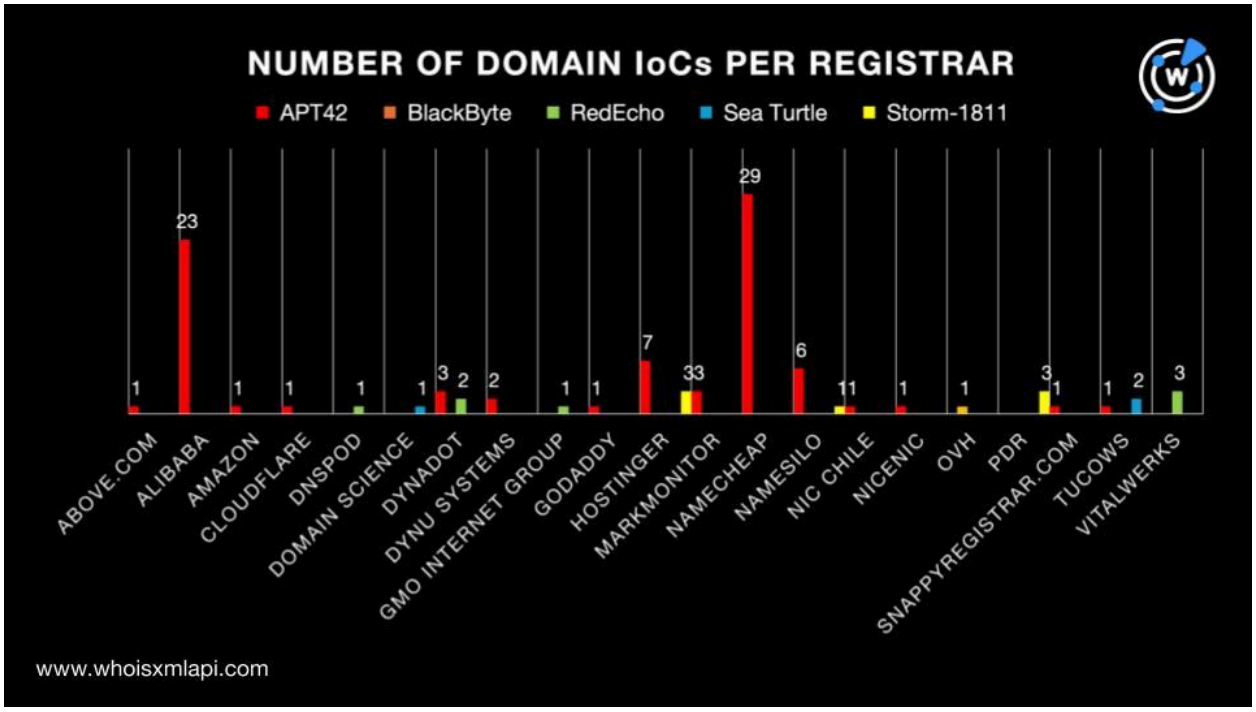
- **Sea Turtle:** Three of the 13 domain IoCs had current WHOIS records. The three domains were created between 2000 and 2025.

- **Storm-1811:** Only seven of the 10 domain IoCs had current WHOIS records. The seven domains were created in 2024.



Below is a summary of our registrar-related findings for the 99 domain IoCs with current WHOIS records.

- **APT42:** The 81 domain IoCs were split across 15 registrars led by Namecheap, which accounted for 29 domains.
- **BlackByte:** The domain IoC was administered by OVH.
- **RedEcho:** The seven domain IoCs were spread among four registrars topped by Vitalwerks, which accounted for three domains.
- **Sea Turtle:** The three domain IoCs were split across two registrars led by Tucows, which accounted for two domains.
- **Storm-1811:** The seven domain IoCs were spread among three registrars topped by Hostinger and PDR, which accounted for three domains each.



Next, we summed up our registrant country-connected findings for the 99 domains with current WHOIS records below.

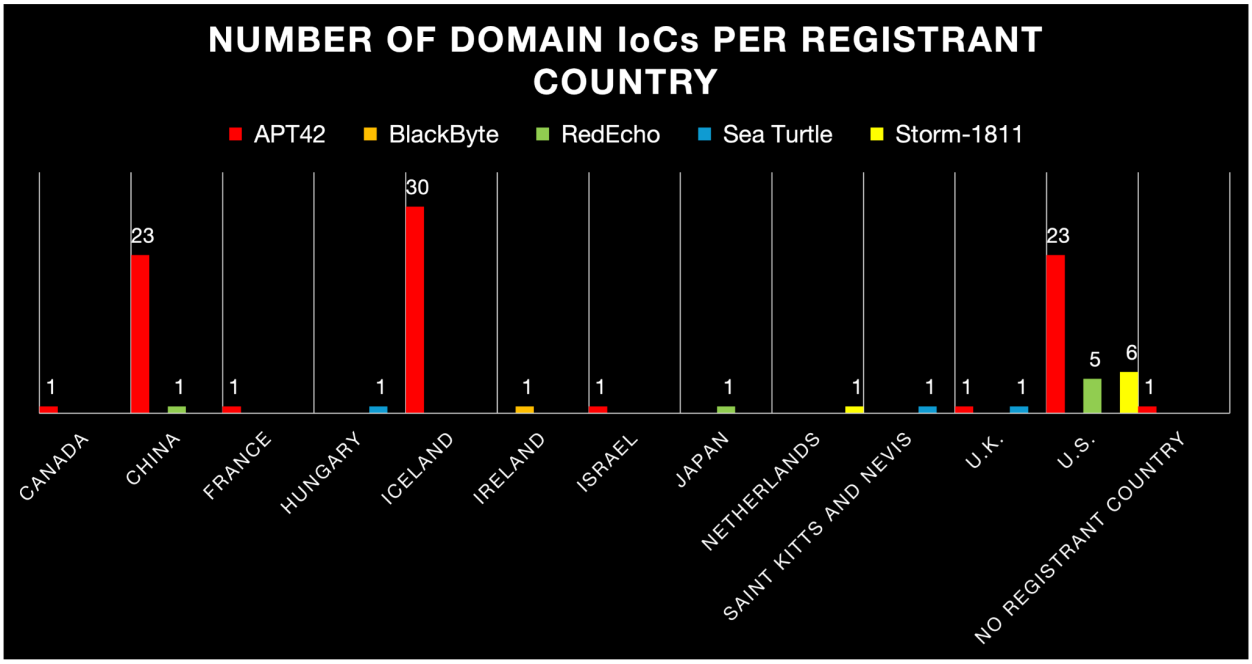
- **APT42:** While one of the domain IoCs did not have a registrant country on record, the 80 remaining ones were split across seven nations led by Iceland, which accounted for 30 domains.

- **BlackByte:** The domain IoC was registered in Ireland.

- **RedEcho:** The seven domain IoCs were spread among three registrant countries topped by the U.S., which accounted for five domains.

- **Sea Turtle:** One domain IoC each was registered in Hungary, Saint Kitts and Nevis, and the U.K.

- **Storm-1811:** The seven domain IoCs were split across two registrant countries led by the U.S., which accounted for six domains.



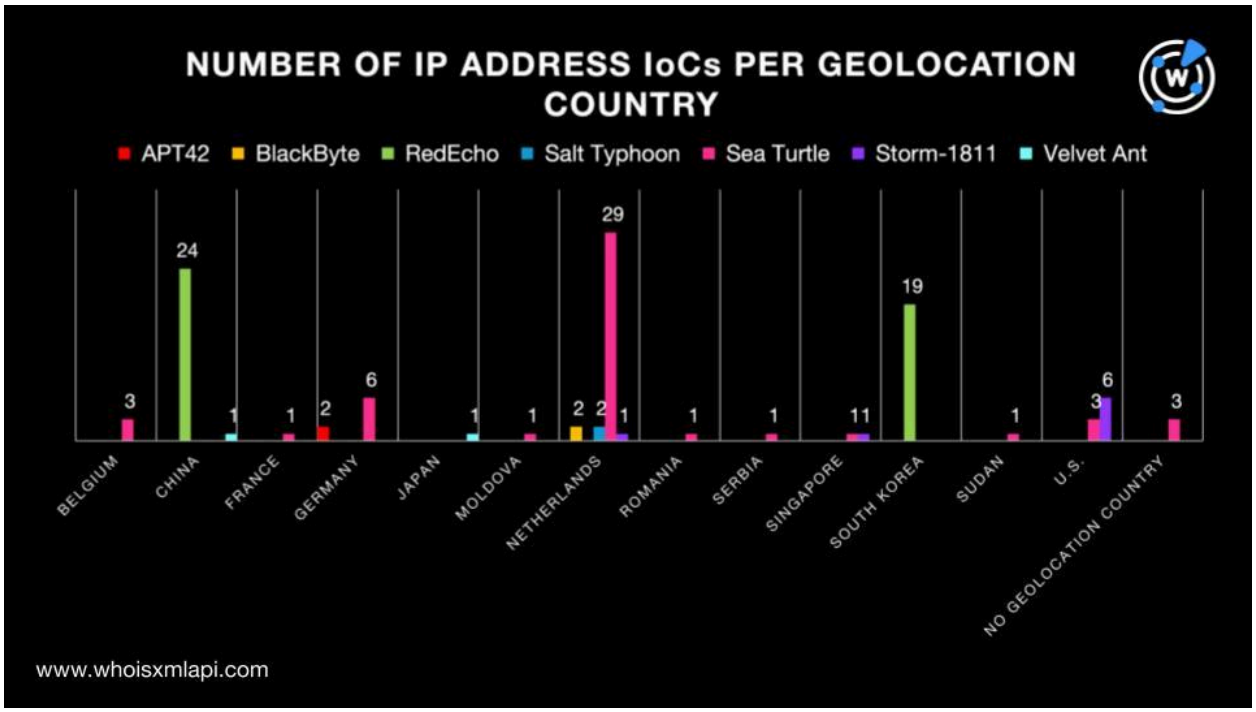
Next, we queried the 189 domains identified as IoCs on DNS Chronicle API and discovered that 186 of them had historical domain-to-IP address resolutions over time. In fact, the 186 domain IoCs recorded 9,190 IP resolutions in all. In addition, the domain IoC for APT42 webredirect[.]org posted the oldest resolution date to the IP address 207[.]38[.]70[.]29, that is, 7 February 2017. Take a look at historical DNS details for a domain IoC for each of the five groups with available data below.

GROUP	DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
APT42	acconut-signin[.]com	97	12 September 2023
BlackByte	alteksecurity[.]org	17	17 January 2023
RedEcho	astudycarsceu[.]net	118	7 January 2022
Sea Turtle	al-marsad[.]co	4	8 October 2024
Storm-1811	antispam2[.]com	125	5 February 2017

We then queried the 109 IP addresses identified as IoCs on Bulk IP Geolocation Lookup by group. Take a look at the summary of our geolocation country-related findings below.

- **APT42:** The two IP address IoCs were geolocated in Germany.

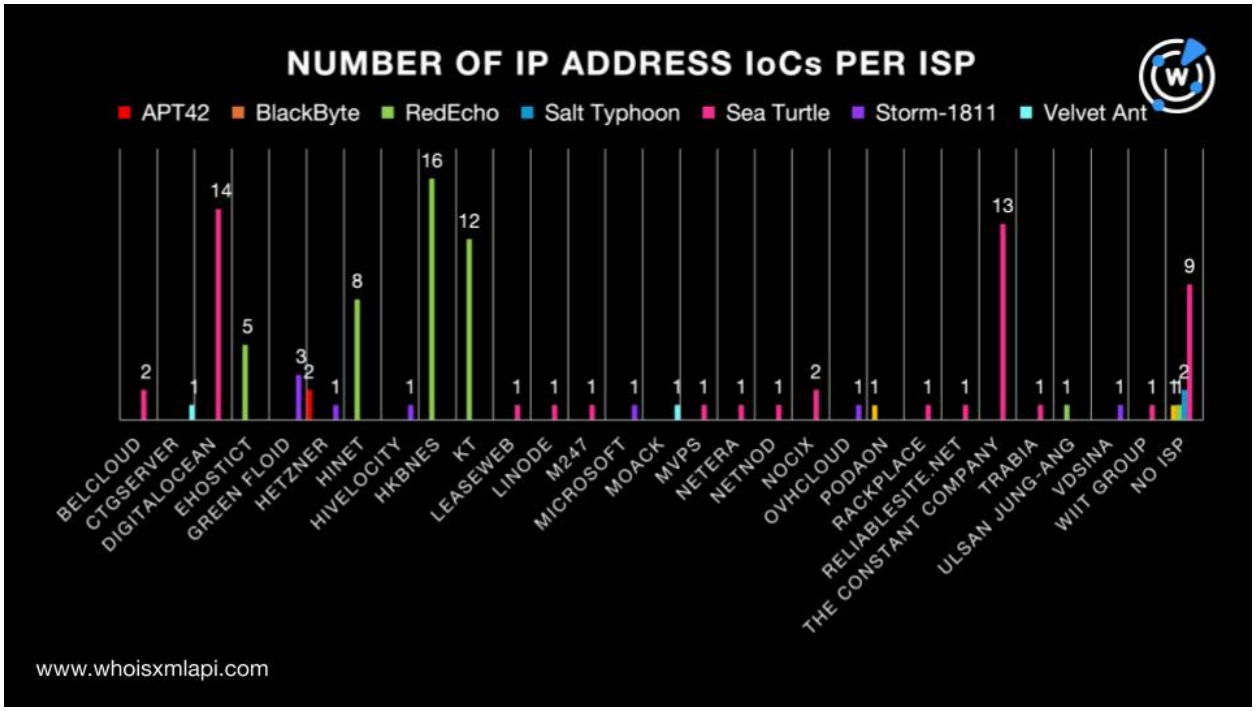
- **BlackByte:** The two IP IoCs were geolocated in the Netherlands.
- **RedEcho:** The 43 IP IoCs were geolocated in two countries—China and South Korea.
- **Salt Typhoon:** The two IP IoCs were geolocated in the Netherlands.
- **Sea Turtle:** While three IP IoCs did not have geolocation countries on record, the remaining 47 were scattered across 10 nations—Belgium, France, Germany, Moldova, the Netherlands, Romania, Serbia, Singapore, Sudan, and the U.S.
- **Storm-1811:** The eight IP IoCs were scattered across three countries, namely, the Netherlands, Singapore, and the U.S.
- **Velvet Ant:** One IP IoC each was geolocated in China and Japan.



We also uncovered the following ISP-connected findings for the 109 IP address IoCs:

- **APT42:** The two IP IoCs were administered by Hetzner.
- **BlackByte:** While one IP IoC did not have an ISP on record, the other was administered by Podaon.

- **RedEcho:** While one IP IoC did not have an ISP on record, the remaining 42 were split across five ISPs led by HKBNES, which accounted for 16 IP addresses.
- **Salt Typhoon:** None of the two IP IoCs has ISPs on record.
- **Sea Turtle:** While nine IP IoCs did not have ISPs on record, the remaining 41 were administered by 14 ISPs topped by DigitalOcean, which accounted for 14 IP addresses.
- **Storm-1811:** The eight IP IoCs were distributed among six ISPs led by Green Floid, which accounted for three IP addresses.
- **Velvet Ant:** One IP IoC each was administered by CTGServer and MOACK.



Next, we queried the 109 IP addresses identified as IoCs on DNS Chronicle API and found that 77 of them had historical IP address-to-domain resolutions. The 77 IP addresses, in particular, recorded 10,980 domain resolutions over time. The IP addresses 114[.]34[.]10[.]80, 114[.]35[.]16[.]182, 114[.]35[.]191[.]224, 122[.]116[.]165[.]62, 122[.]116[.]234[.]73, 220[.]132[.]106[.]193, and 220[.]133[.]141[.]117 associated with RedEcho; 178[.]17[.]167[.]51 with Sea Turtle; and 202[.]61[.]136[.]158 with Velvet Ant posted the oldest resolution date, that is, 4 February 2017. Here are historical DNS details for a domain IoC for each of the seven groups below.

GROUP	IP ADDRESS IoC	NUMBER OF DOMAIN RESOLUTIONS	FIRST DOMAIN RESOLUTION DATE
APT42	49[.]13[.]194[.]118	4	24 December 2021
BlackByte	185[.]93[.]6[.]31	15	5 September 2021
RedEcho	101[.]78[.]177[.]227	2	22 October 2019
Salt Typhoon	185[.]141[.]24[.]28	633	28 April 2020
Sea Turtle	108[.]61[.]103[.]186	296	5 February 2017
Storm-1811	195[.]123[.]233[.]42	154	14 January 2018
Velvet Ant	103[.]138[.]13[.]31	1	21 July 2020

In addition, using sample netflow data our researchers obtained from the IASC, we further analyzed three IP addresses identified as IoCs—88[.]119[.]171[.]248, 91[.]90[.]195[.]52, and 62[.]115[.]255[.]163—that served as command-and-control (C&C) server addresses related to the threat. The sample data revealed three alleged victim IP records sent data to the three IP IoCs 10 times. Take a look at ISP and AS data for the IP addresses below.

IP ADDRESS IoC (Destination IP)	ISP	ASN
88[.]119[.]171[.]248	N/A	61272
91[.]90[.]195[.]52	Green Floid	204957
62[.]115[.]255[.]163	Arelion (Twelve99)	1299

On the flipside, we also analyzed communications coming from seven IP addresses identified as IoCs and found 60 IP addresses contacted 216 times. Here are ISP and AS data for the IP addresses.

IP ADDRESS IoC (Source IoC)	ISP	ASN
15[.]235[.]218[.]150	OVHcloud	16276
31[.]13[.]195[.]52	Neterra	34224

45[.]9[.]148[.]114	N/A	49447
62[.]115[.]255[.]163	Arelion (Twelve99)	1299
88[.]119[.]171[.]248	N/A	61272
91[.]107[.]150[.]184	Hetzner Online	24940
91[.]90[.]195[.]52	Green Floid	204957

IoC List Expansion Findings

We kicked off our search for connected artifacts with a WHOIS History API query for the 189 domains identified as IoCs and found that 63 of them had 254 email addresses in their historical WHOIS records after duplicates were filtered out. Closer scrutiny of the email addresses revealed that 43 were public email addresses.

We then queried the 43 public email addresses on Reverse WHOIS API and discovered that while none of them appeared in current WHOIS records, 36 did so in historical WHOIS records. Our search led to the discovery of 638 email-connected domains after duplicates and those already identified as IoCs were filtered out.

A Threat Intelligence API query for the 638 email-connected domains showed that six have already figured in various attacks. Take a look at three examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT TYPES
account-logins[.]com	Malware distribution
brownstoneexpediting[.]com	Generic threat
mailer-daemon[.]net	Malware distribution

Next, we queried the 189 domains identified as IoCs on DNS Lookup API and found that 35 had active IP resolutions. We ended up with 26 additional IP addresses after filtering out duplicates and those already tagged as IoCs.

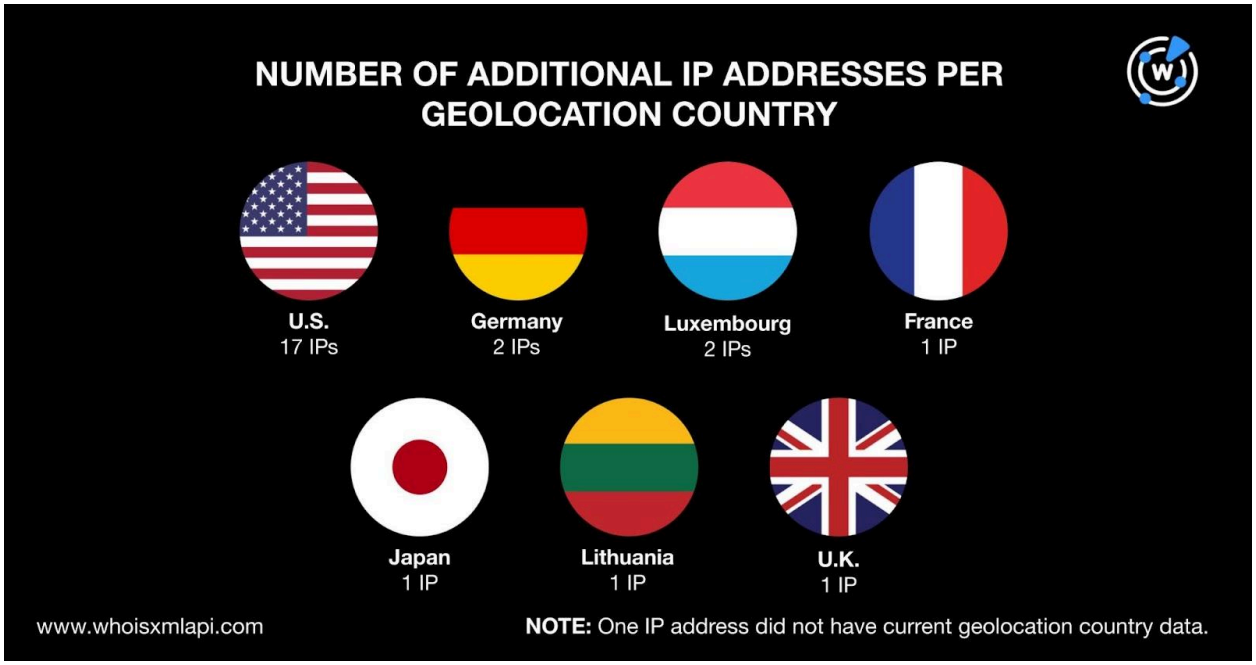
A Threat Intelligence API query for the 26 additional IP addresses showed that 16 have already been weaponized for various attacks. Take a look at five examples below.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT TYPES

103[.]224[.]182[.]217	Attack C&C Generic threat Malware distribution Phishing Suspicious activity
104[.]21[.]48[.]1	Attack C&C Generic threat Malware distribution Phishing Spam campaign Suspicious activity
54[.]146[.]6[.]253	C&C Generic threat Malware distribution
84[.]32[.]84[.]33	Attack C&C Generic threat Malware distribution Phishing Suspicious activity
91[.]195[.]240[.]12	Attack C&C Generic threat Malware distribution Phishing Suspicious activity

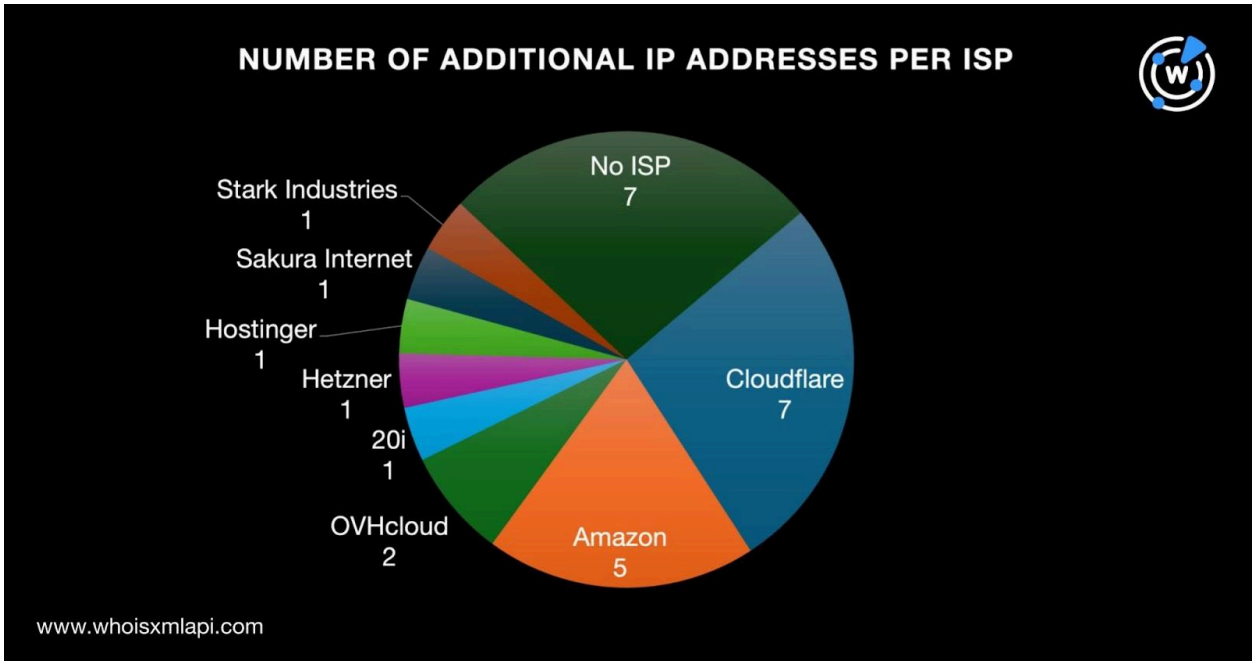
We then queried the 26 additional IP addresses on Bulk IP Geolocation Lookup and discovered that:

- While one IP address did not have a geolocation country on record, the 25 remaining IPs were geolocated in seven countries led by the U.S., which accounted for 17 IP addresses. Two IPs each originated from Germany and Luxembourg. Finally, one IP each was geolocated in France, Japan, Lithuania, and the U.K.



Note that four of the additional IP addresses' geolocation countries were the same as those of the IoCs—France, Germany, Japan, and the U.S.

- While seven IP addresses did not have ISPs on record, the 19 remaining IPs were administered by eight ISPs topped by Cloudflare, which accounted for seven IPs. Amazon came in second place with five IPs while OVHcloud placed third with two IPs. One IP each was administered by 20i, Hetzner, Hostinger, Sakura Internet, and Stark Industries.



- Only two ISPs—Hetzner and OVHcloud—also appeared in the list of ISPs for the IP addresses identified as IoCs.

Next, we queried the 135 IP addresses (i.e., 109 identified as IoCs and 26 additional ones) on Reverse IP API and discovered that 44 hosted other domains. A closer look at the IPs showed that 25 of them could be dedicated hosts. Altogether, they hosted 221 IP-connected domains after duplicates, those already tagged as IoCs, and the email-connected domains were filtered out.

As our final step, we searched for other connected domains via Domains & Subdomains Discovery. We used the **Starts with** parameter for the 185 unique text strings found in the domains identified as IoCs. We uncovered connections for these 105 strings:

- account-signin.
- accounts-mails.
- advission.
- al-marsad.
- alhurra.
- alteksecurity.
- anfturkce.
- antispam2.
- antispam3.
- aspenInstitute.
- besvision.
- bitly.
- book-download.
- boord.
- briview.
- brookings.
- businessInsider.
- chat-services.
- cjcomputing.
- confirmation-process.

- coordinate.
- d75.
- daemon-mailer.
- ddns.
- dloffice.
- drive-access.
- ecomonist.
- email-daemon.
- foreiqnaffairs.
- forieqnaffairs.
- g-online.
- geaviews.
- go-forward.
- greekpool.
- gview.
- hopto.
- intersecdns.
- ixrails.
- jpost.
- khaleejtimes.
- khalejtimes.
- ksview.
- limitedtoday.
- loriginal.
- loseyourip.
- m85.
- maariv.
- mail-roundcube.
- mailer-daemon.
- mailerdaemon.
- mcsoft.
- meeting-online.
- mega.
- mterview.
- myaccount-signin.
- n9.
- nmcbcd.
- nterview.
- online-processing.
- online-video-services.
- ovcloud.
- pandorarve.
- panel-view.
- ptciocl.
- querryfiles.
- quomodocunquize.
- reconsider.
- rewilivak13.
- s20.
- s3api.
- s51.
- s59.
- secrsys.
- short-url.
- short-view.
- shortenurl.
- shortlinkview.
- shoting-urls.
- signin-accounts.
- signin-mail.
- signin-mails.
- signin-myaccounts.
- smaaaal.
- support-account.
- systemctl.
- sytes.
- tcvision.
- temp.
- twision.
- understandingthewar.
- upd5.
- upd7.
- upd9.
- ushrt.
- vanityfaire.
- view-panel.
- viewstand.
- viewtop.
- w3spaces.
- washinqtonpost.

- we-transfer.
- webredirect.
- ybcd.
- ynetnews.
- youtransfer.

Specifically, we unearthed 4,195 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 4,195 string-connected domains revealed that 37 have already figured in various attacks. Here are five examples.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT TYPES
bitly[.]best	Malware distribution
brookings[.]cloud	Malware distribution
confirmation-process[.]at	Malware distribution
daemon-mailer[.]com	Malware distribution
email-daemon[.]online	Malware distribution

—

Our DNS deep dive into the seven new group additions to the MITRE ATT&CK page led to the discovery of 5,080 new artifacts comprising 638 email-connected domains, 26 additional IP addresses, 221 IP-connected domains, and 4,195 string-connected domains. It is also worth noting that 59 of the artifacts we found 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.*

References

- **APT42**
    - https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations
    - https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/
- **BlackByte**
    - https://www.picussecurity.com/resource/ttps-used-by-blackbyte-ransomware-targeting-critical-infrastructure
    - https://www.security.com/threat-intelligence/blackbyte-exbyte-ransomware
    - https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/
    - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/blackbyte-ransomware-pt-1-in-depth-analysis/
- **RedEcho**
    - https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf
    - https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf
- **Salt Typhoon**
    - https://blog.talosintelligence.com/salt-typhoon-analysis/
- **Sea Turtle**
    - https://blog.talosintelligence.com/seaturtle/
    - https://blog.talosintelligence.com/sea-turtle-keeps-on-swimming/
    - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/tortoise-and-malwahare.html
    - https://www.huntandhackett.com/blog/turkish-espionage-campaigns
- **Storm-1811**
    - https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

    - https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators

- **Velvet Ant**

    - https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/

Appendix: Sample Artifacts

Sample Email-Connected Domains

- 000bx[.]com
- 0044h[.]com
- 0087w[.]com
- a-mcowen[.]com
- a0a6[.]com
- a4andhra[.]com
- b4bengal[.]com
- b9p4lf[.]com
- ba558[.]com
- c4chennai[.]com
- cag01[.]com
- calvinklein-ck[.]us
- d4205[.]com
- d8bx[.]com
- dainik-bhaskar[.]press
- ec912[.]com
- edisatech[.]com
- edomovina[.]com
- face-of-pro[.]com
- fastbtc[.]net
- feaniq[.]com
- geopolitics[.]press
- ghhrt[.]com
- gi555[.]com
- haaretz[.]press
- hamacasdecolombia[.]com
- hardox400gb[.]com
- icaststone[.]com
- ie698[.]com
- ihre-seite[.]com
- jacobgoldman[.]design
- jamarchitect[.]com
- jaygoldman[.]nyc
- k1xij5[.]com
- k4kerala[.]com
- k4kolkatha[.]com
- larrytarr[.]com
- larrytarr[.]net
- larrytarr[.]org
- m8o191[.]com
- ma528[.]com
- maariv[.]info
- n3310[.]net
- national-geographic[.]press
- naturaldietsystems[.]com
- opengeu[.]com
- orbtrade[.]net
- ovjja0[.]com
- panel-sshpremiums[.]com
- partridge[.]press
- pavpai-account[.]com
- q345bhg[.]com
- qayqal-service[.]com
- qq0k[.]com
- r1ynw[.]com
- rapidoputumayo[.]com
- raze2games[.]us
- sacguess[.]org
- safsch[.]com
- sakshi[.]press
- tacticasenseguridad[.]com
- taole99[.]com
- tarr[.]us
- uggbootswolaile[.]net
- uhvy4x[.]com
- uk3ii1[.]com
- vayanasala[.]com
- vertify404x[.]com
- veteransaffairshome[.]com
- w2sq[.]com
- w3chef[.]com
- w3listings[.]com

- xb4y7[.]com
- xd139[.]com
- xmwxh[.]net
- ymp8[.]com
- yoserlota[.]com
- yossi-sagi[.]com
- zagranpassport[.]net
- zg591[.]com
- zutetv[.]com

Sample Additional IP Addresses

- 0[.]0[.]0[.]0
- 103[.]224[.]182[.]217
- 216[.]137[.]39[.]14
- 45[.]89[.]53[.]22
- 5[.]78[.]118[.]89
- 66[.]203[.]124[.]30
- 84[.]32[.]84[.]33
- 91[.]195[.]240[.]12

Sample IP-Connected Domains

- 04678c98-4e51-4f45-a70b-d4593be987d1[.]random[.]100yearsoftshirts[.]com
- 100yearsoftshirts[.]com
- 185-93-6-31[.]netherlands-2[.]vps[.]ac
- a024b5eb-9855-4980-8f34-a4b19a4fdc1f[.]random[.]limitedtoday[.]com
- a86ab3c3-ef2b-4cc7-8752-4bac22018900[.]random[.]30secondbinaryoptions[.]com
- aaaa[.]limitedtoday[.]com
- bdf2ec35-2824-46f6-979d-093fa4f9be8a[.]random[.]100yearsoftshirts[.]com
- blunt[.]bio
- boot-01[.]net[.]anydesk[.]com
- c1-euw1[.]limitedtoday[.]com
- c9922f54-f1d2-49e3-a861-40de93eb6191[.]random[.]anachakauto[.]com
- caliconnect[.]site
- dados[.]portaldotransportador[.]tecnoatende[.]com[.]br
- dash[.]primary[.]blunt[.]bio
- dashboard-config[.]blunt[.]bio
- email25[.]limitedtoday[.]com
- espacoholisticoodara[.]limitedtoday[.]com
- f3st[.]pro
- fb538364-13b3-4a4e-8417-4e26894c5d96[.]random[.]limitedtoday[.]com
- fgvb[.]info
- gff[.]pw
- gif[.]limitedtoday[.]com
- glory[.]30secondbinaryoptions[.]com
- hiso[.]love
- historicalsimslife[.]limitedtoday[.]com
- ickdfuki1kztijjfcyrexeg2o34a9999[.]fqqpsrxl1e3bzubcsey1wli9[.]claudfront[.]net
- instance-ss[.]blunt[.]bio
- iri[.]30secondbinaryoptions[.]com
- jingcaibifenzhibo[.]limitedtoday[.]com
- jnh[.]one
- kacky[.]synology[.]me
- kmga[.]group
- kyr[.]at
- lefflernas[.]direct[.]quickconnect[.]to
- libraries[.]limitedtoday[.]com
- localhost[.]100yearsoftshirts[.]com
- m8ch[.]org

- mail[.]100yearsoftshirts[.]com
- mail[.]30secondbinaryoptions[.]com
- n3tx[.]ink
- nissan[.]limitedtoday[.]com
- offspringsofcomedypeople[.]limitedtoday[.]com
- olagragasport[.]limitedtoday[.]com
- oldfashionedtoyshop[.]co[.]uk
- play[.]anachakauto[.]com
- plfn[.]co
- plga[.]me
- reflect[.]limitedtoday[.]com
- ricky[.]limitedtoday[.]com
- robfpzslqwi[.]100yearsoftshirts[.]com
- s1076[.]limitedtoday[.]com
- s11[.]homegamesuperior20240[.]online
- salty[.]blunt[.]bio
- thefrugalcrafter[.]limitedtoday[.]com
- tomgurgel[.]limitedtoday[.]com
- trk[.]amazeen[.]top
- umami[.]blunt[.]bio
- v5ry4sa9[.]ozrsvmvwuqds1qa64t3lyd5tgifq9999[.]aowiyfncehuuv25yc2baobi9[.]claudfront[.]net
- vavadasms[.]com
- vgos480[.]blunt[.]bio
- wadham[.]limitedtoday[.]com
- webdisk[.]blunt[.]bio
- webdisk[.]kmga[.]group
- xn--80aegbkvxddlre[.]limitedtoday[.]com
- xod[.]info
- xxccaallsspp[.]fun
- yry[.]at
- zdd[.]one
- zzq[.]at

Sample String-Connected Domains

- account-signin[.]biz
- account-signin[.]buzz
- account-signin[.]cards
- accounts-mails[.]cf
- accounts-mails[.]ga
- accounts-mails[.]gq
- advission[.]com
- advission[.]monster
- al-marsad[.]com
- al-marsad[.]net
- al-marsad[.]online
- alhurra[.]ae
- alhurra[.]app
- alhurra[.]biz
- alteksecurity[.]co[.]uk
- alteksecurity[.]com
- alteksecurity[.]ws
- anfturkce[.]com
- anfturkce[.]info
- anfturkce[.]net
- antispam2[.]co[.]pw
- antispam2[.]com[.]ph
- antispam2[.]go[.]pw
- antispam3[.]com[.]ws
- antispam3[.]edu[.]ws
- antispam3[.]nhs[.]uk
- besvision[.]com
- besvision[.]info
- besvision[.]nl
- bitly[.]ac
- bitly[.]accountants
- bitly[.]ad
- book-download[.]accountant
- book-download[.]casa
- book-download[.]cf
- boord[.]app

- boord[.]be
- boord[.]bet
- briview[.]cn
- briview[.]co[.]uk
- briview[.]com
- brookings[.]app
- brookings[.]asia
- brookings[.]at
- businesslnsider[.]cf
- businesslnsider[.]club
- businesslnsider[.]com
- chat-services[.]cc
- chat-services[.]com
- chat-services[.]de
- cjcomputing[.]co[.]uk
- confirmation-process[.]at
- confirmation-process[.]com
- coordinate[.]abudhabi
- coordinate[.]academy
- coordinate[.]ae
- d75[.]asia
- d75[.]at
- d75[.]bar
- daemon-mailer[.]com
- daemon-mailer[.]net
- daemon-mailer[.]online
- ddns[.]abc[.]br
- ddns[.]ac
- ddns[.]af
- dloffice[.]cn
- dloffice[.]com
- dloffice[.]com[.]cn
- drive-access[.]com
- drive-access[.]fr
- ecomonist[.]com
- email-daemon[.]online
- foreiqnaffairs[.]biz
- foreiqnaffairs[.]blog
- foreiqnaffairs[.]careers
- g-online[.]at
- g-online[.]biz
- g-online[.]cc
- geaviews[.]cf
- go-forward[.]at
- go-forward[.]be
- go-forward[.]biz
- greekpool[.]de
- greekpool[.]eu
- greekpool[.]ws
- gview[.]ae
- gview[.]app
- gview[.]biz
- hopto[.]ai
- hopto[.]asia
- hopto[.]au
- intersecdns[.]co[.]za
- ixrails[.]ws
- jpost[.]ae
- jpost[.]ai
- jpost[.]app
- khaleejtimes[.]ae
- khaleejtimes[.]agency
- khaleejtimes[.]app
- khalejtimes[.]com
- ksview[.]cn
- ksview[.]co[.]jp
- ksview[.]com
- limitedtoday[.]ml
- limitedtoday[.]online
- limitedtoday[.]shop
- loriginal[.]barcelona
- loriginal[.]be
- loriginal[.]biz
- loseyourip[.]top
- loseyourip[.]us
- loseyourip[.]ws
- m85[.]ae
- m85[.]app
- m85[.]at
- maariv[.]ai

- maariv[.]app
- maariv[.]biz
- mail-roundcube[.]com
- mailer-daemon[.]app
- mailer-daemon[.]aquila[.]it
- mailer-daemon[.]biz
- mailerdaemon[.]app
- mailerdaemon[.]buzz
- mailerdaemon[.]ch
- mcsoft[.]app
- mcsoft[.]at
- mcsoft[.]biz
- meeting-online[.]at
- meeting-online[.]ch
- meeting-online[.]co[.]uk
- mega[.]ac
- mega[.]academy
- mega[.]accountants
- mterview[.]ca
- mterview[.]com
- myaccount-signin[.]info
- n9[.]ae
- n9[.]af
- n9[.]ag
- nmcbcd[.]com
- nterview[.]ai
- nterview[.]co
- nterview[.]co[.]kr
- online-processing[.]cf
- online-processing[.]cfd
- online-processing[.]co[.]uk
- ovcloud[.]biz
- ovcloud[.]cf
- ovcloud[.]cl
- pandorarve[.]ph
- panel-view[.]com
- ptciocl[.]ph
- ptciocl[.]ws
- querryfiles[.]ph
- quomodocunquize[.]click
- quomodocunquize[.]co
- quomodocunquize[.]co[.]uk
- reconsider[.]ai
- reconsider[.]app
- reconsider[.]asia
- rewilivak13[.]ph
- rewilivak13[.]ws
- s20[.]africa
- s20[.]ai
- s20[.]am
- s3api[.]cf
- s3api[.]com
- s3api[.]io
- s51[.]am
- s51[.]arab
- s51[.]bet
- s59[.]am
- s59[.]biz
- s59[.]cam
- secrsys[.]ph
- short-url[.]app
- short-url[.]asia
- short-url[.]auction
- short-view[.]com
- short-view[.]de
- shortenurl[.]ai
- shortenurl[.]app
- shortenurl[.]at
- shortlinkview[.]xyz
- shoting-urls[.]net[.]ws
- signin-accounts[.]email
- signin-accounts[.]info
- signin-accounts[.]limited
- signin-mail[.]email
- signin-mail[.]mobi
- signin-mail[.]net
- signin-myaccounts[.]cf
- signin-myaccounts[.]ga
- signin-myaccounts[.]ml
- smaaaal[.]tk

- support-account[.]asia
- support-account[.]biz
- support-account[.]business
- systemctl[.]app
- systemctl[.]blog
- systemctl[.]ca
- sytes[.]academy
- sytes[.]app
- sytes[.]ar
- tcvision[.]ai
- tcvision[.]au
- tcvision[.]cloud
- temp[.]ac
- temp[.]academy
- temp[.]accountants
- twision[.]agency
- twision[.]ch
- twision[.]co
- understandingthewar[.]com
- understandingthewar[.]ph
- understandingthewar[.]ws
- upd5[.]com
- upd5[.]com[.]ws
- upd5[.]info
- upd7[.]arab
- upd7[.]com[.]ph
- upd7[.]com[.]ws
- upd9[.]cn
- upd9[.]icu
- upd9[.]vg
- ushrt[.]bid
- ushrt[.]cc
- ushrt[.]cf
- vanityfaire[.]com
- vanityfaire[.]com[.]sg
- vanityfaire[.]info
- view-panel[.]com
- viewstand[.]com
- viewstand[.]net
- viewtop[.]at
- viewtop[.]ca
- viewtop[.]ch
- w3spaces[.]co
- w3spaces[.]fr
- washinqtonpost[.]com
- we-transfer[.]biz
- we-transfer[.]cam
- we-transfer[.]cf
- webredirect[.]arab
- webredirect[.]at
- webredirect[.]belau[.]pw
- ybcd[.]arab
- ybcd[.]asia
- ybcd[.]bid
- ynetnews[.]co
- ynetnews[.]co[.]il
- ynetnews[.]co[.]uk
- youtransfer[.]app
- youtransfer[.]cn
- youtransfer[.]co