Tracking Down APT Group WIRTE's DNS Movements

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts

Executive Report

The WIRTE advanced persistent threat (APT) group has been active since at least August 2018. It has targeted government, diplomatic, financial, military, legal, and technology organizations in the Middle East and Europe.

While the group has been quiet for some time, it has resurfaced, trailing its sights on Middle Eastern entities, specifically the Palestinian Authority, Jordan, Egypt, and Saudi Arabia. According to reports, the group has been using custom loaders like IronWind in recent attacks.

Check Point Research published an in-depth analysis of WIRTE's attacks from late 2023 to the present and identified 56 indicators of compromise (IoCs) comprising 30 domains, 23 IP addresses, and three subdomains.

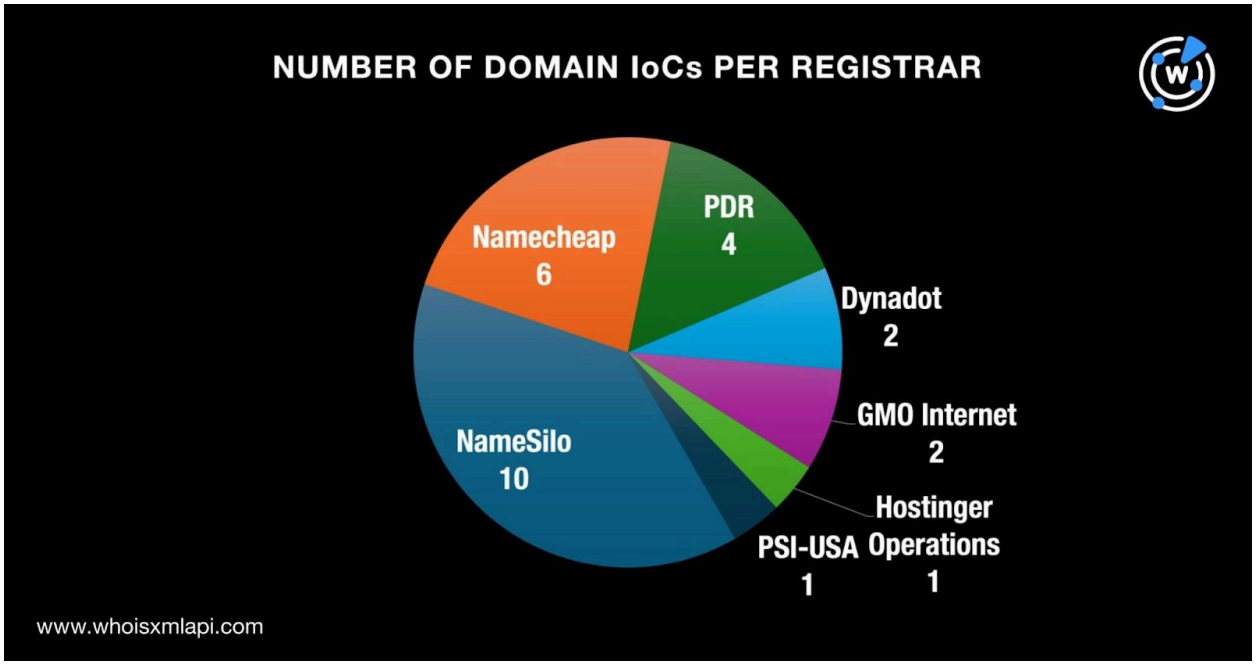
The WhoisXML API research team expanded the original list of 56 IoCs to uncover more connected artifacts and found:

- 360 email-connected domains
- 36 additional IP addresses, 35 of which turned out to be malicious
- Six IP-connected domains, one of which turned out to be malicious
- 41 string-connected domains
- 3,088 string-connected subdomains

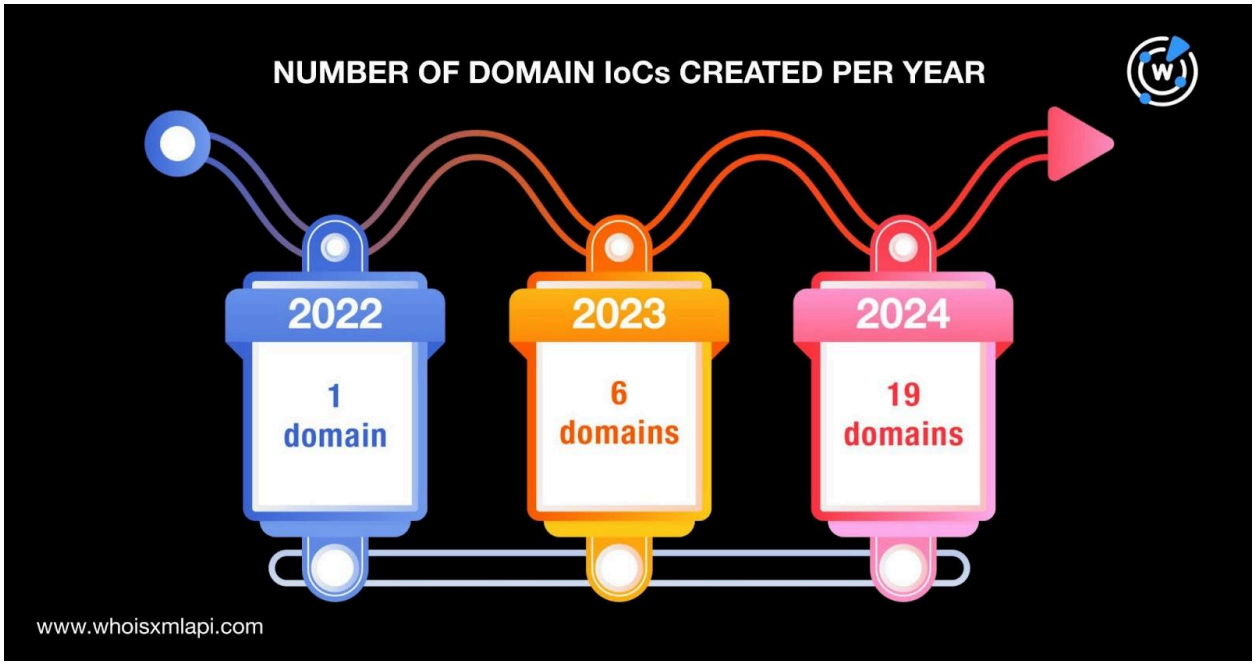
More on the WIRTE Attack IoCs

We first took a closer look at the 56 WIRTE attack IoCs beginning with the 30 domains. We queried the domain IoCs on Bulk WHOIS Lookup and found that only 26 of them had current WHOIS records. The results revealed that:

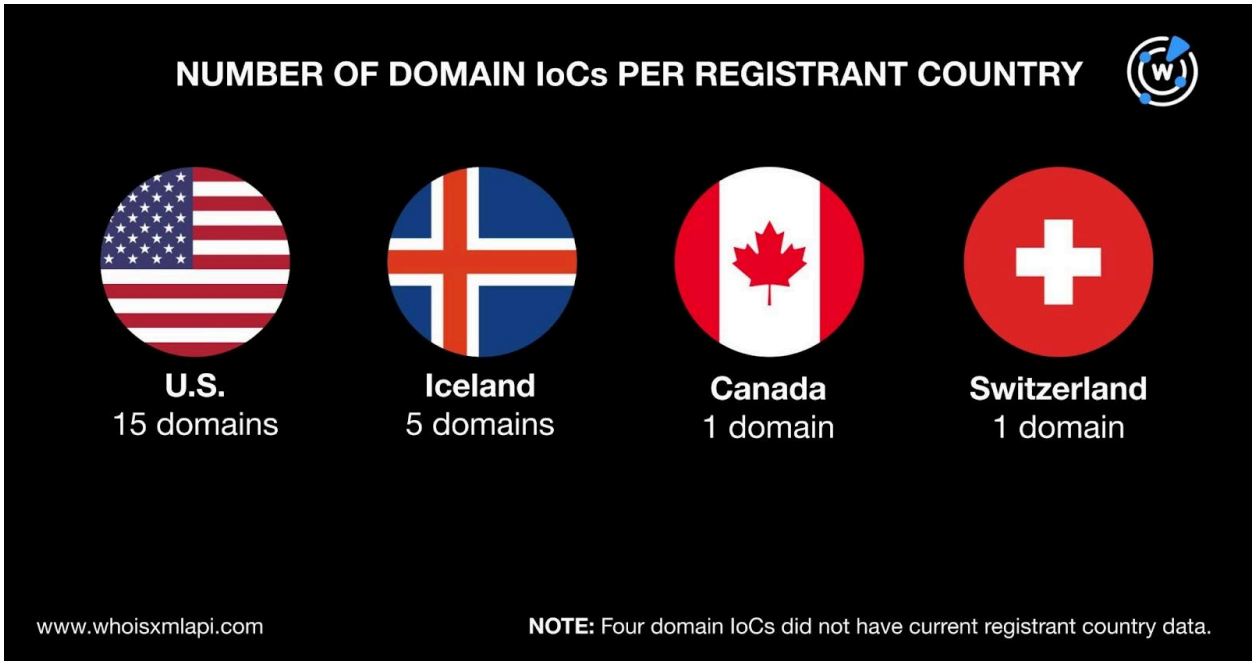
- They were spread across seven registrars led by NameSilo, which accounted for 10 domains. Namecheap administered six domains; PDR, four domains; Dynadot and GMO Internet, two domains each; and Hostinger Operations and PSI-USA, one domain each.



- They were created between 2022 and 2024. Specifically, one domain in 2022, six in 2023, and 19 in 2024.



- They were scattered across four registrant countries led by the U.S., which accounted for 15 domains. Iceland came in second place with five domains, while one domain each was registered in Canada and Switzerland. Four domains did not have current registrant country data.

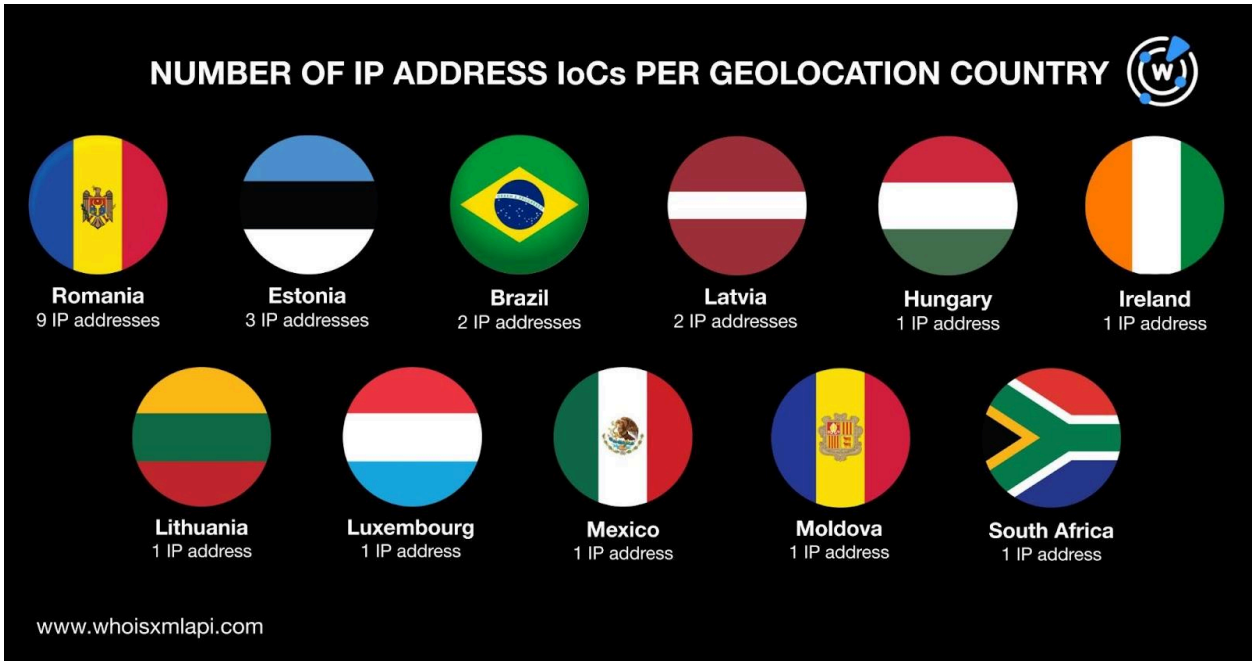


Next, we queried the 30 domain IoCs on DNS Chronicle API and found that they recorded a total of 1,692 IP resolutions between 4 October 2019 and 29 November 2024. Take a look at the DNS history of five domain IoCs below.

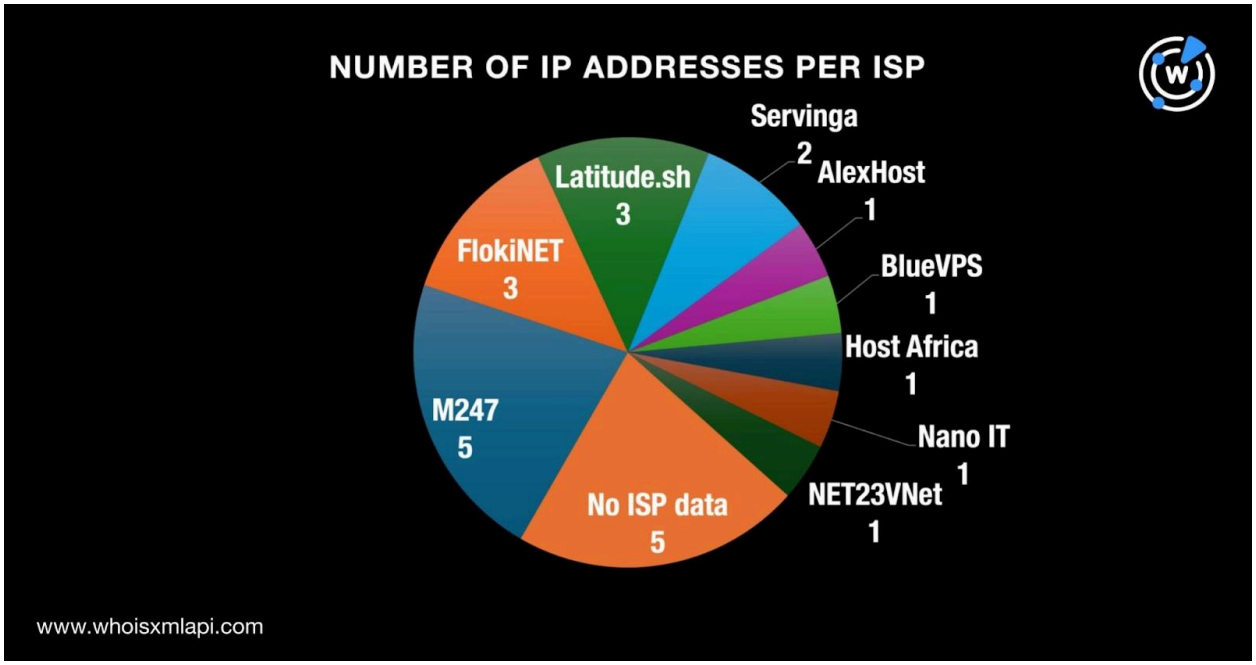
DOMAIN IoC	START DATE	LAST DATE	NUMBER OF IP RESOLUTIONS
bankjordan[.]com	06/11/24	06/29/24	8
dentalaccord[.]com	10/28/19	09/02/24	86
easybackupcloud[.]com	10/04/19	09/06/23	40
finance-analyst[.]com	10/26/19	07/04/24	24
healthcarb[.]com	10/05/19	11/16/24	75

After that, we looked more closely at the 23 IP addresses tagged as IoCs by querying them first on Bulk IP Geolocation Lookup, which revealed that:

- They were spread across 11 geolocation countries led by Romania, which accounted for nine IP addresses. Estonia came in second with three IP addresses. Two IP addresses each were geolocated in Brazil and Latvia, while one each originated from Hungary, Ireland, Lithuania, Luxembourg, Mexico, Moldova, and South Africa.



- They were distributed among nine ISPs led by M247, which accounted for five IP addresses. FlokiNET and Latitude.sh administered three IP addresses each; Servinga, two; and AlexHost, BlueVPS, Host Africa, Nano IT, and NET23VNet, one each. Five IP addresses had no ISP data.



Like the domains tagged as IoCs, we also queried the 23 IP address IoCs on DNS Chronicle API. We found that they historically resolved 981 domains between 4 October 2019 and 29 November 2024. Take a look at the DNS history of five examples below.

IP ADDRESS IoC	START DATE	LAST DATE	NUMBER OF DOMAIN RESOLUTIONS
185[.]158[.]248[.]161	06/07/22	06/19/24	26
213[.]252[.]244[.]234	11/19/21	11/02/24	131
37[.]120[.]247[.]22	03/24/23	09/14/23	4
45[.]59[.]118[.]145	09/05/21	11/11/24	102
5[.]42[.]221[.]151	05/06/23	11/18/23	6

WIRTE Attack IoC DNS Connections

Our search for WIRTE-connected artifacts took off with a WHOIS History API query for the 30 domains tagged as IoCs, which uncovered 88 email addresses from their historical WHOIS records after duplicates were filtered out. A total of 31 of them turned out to be public email addresses.

A Reverse WHOIS API query for the 31 public email addresses returned 360 email-connected domains after duplicates and the IoCs were filtered out.

Next, we queried the 30 domains tagged as IoCs on DNS Lookup API and found that they resolved to 36 IP addresses after duplicates and the IP address IoCs were filtered out.

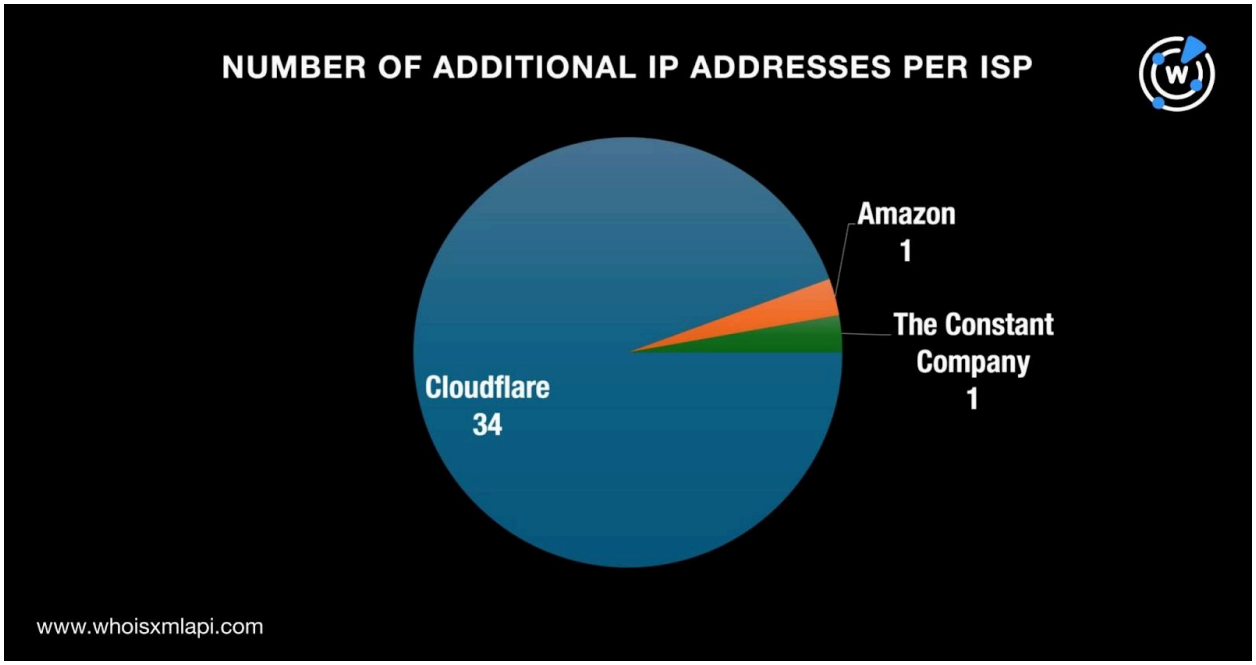
A Threat Intelligence API query for the 36 additional IP addresses showed that 35 of them have seemingly already been weaponized for various malicious campaigns. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]10[.]180	Generic Malware Phishing
104[.]21[.]13[.]166	Generic Malware Suspicious
172[.]67[.]129[.]40	Attack Malware
199[.]59[.]243[.]227	Attack Command and control (C&C) Generic Malware Phishing Suspicious
70[.]34[.]210[.]52	Malware

We then queried the 36 additional IP addresses on Bulk IP Geolocation Lookup and found that:

- They were geolocated in just two countries with a majority, 35 to be exact, in the U.S. The remaining additional IP address originated from Sweden.

- They were spread across three ISPs led by Cloudflare, which accounted for 34 additional IP addresses. One additional IP address each was administered by Amazon and The Constant Company.



Next, our Reverse IP API query for the 36 additional IP addresses showed that five of them could be dedicated. Altogether, they hosted six IP-connected domains after duplicates, the IoCs, and the email-connected domains were filtered out. One of them—heylele[.]com—has already been weaponized to seemingly serve as a C&C server.

We then used Domains & Subdomains Discovery to search for other domains starting with the exact strings found among the 30 domains tagged as IoCs. We obtained results for these 13 strings:

- easybackupcloud.
- economymentor.
- egyptican.
- finances-news.
- inclusive-economy.
- jordanrefugees.
- jordansons.
- master-dental.
- microsoftwindowshelp.
- saudiarabianow.
- saudiday.
- suppertools.
- wellhealthtech.

We uncovered 41 string-connected domains in all after duplicates, the IoCs, and the email- and IP-connected domains were filtered out.

Lastly, we also looked for subdomains starting with the same strings as the three subdomains tagged as IoCs. We found results for these two strings:

- support-api.
- trendingcharts.

Our search led to the discovery of 3,088 string-connected subdomains.

—

Our IoC expansion analysis for the most recent WIRTE attack uncovered a total of 3,531 artifacts comprising 360 email-connected domains, 36 additional IP addresses, six IP-connected domains, 41 string-connected domains, and 3,088 string-connected subdomains. It is also worth noting that to date, 36 of these artifacts have already figured in various malicious campaigns.

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

- abcchristmas2015[.]com
- alera-group[.]info
- alera-group[.]org
- b-luron[.]info
- bahrain-onlinetourism[.]com
- bahrainonline-travels[.]com
- cambodia-onlinetrip[.]com
- cambodia-onlinevisit[.]com
- cambodia-touronline[.]com
- dating-101[.]info
- dffapplication[.]com
- discoveraussie[.]com
- eckoneko[.]org
- ecofunhouse[.]info
- ecofunhouse[.]org
- fastweightlossplan[.]info
- financialhanck[.]com
- fleetgraph[.]info
- gabon-onlinetourism[.]com
- gabononline-travels[.]com

- gardimon[.]com
- haj1438[.]com
- haj1439[.]com
- haj2017[.]com
- iamexpo2020[.]com
- ibtissamalebanon[.]com
- ibtissamalebanon[.]org
- japantravel-online[.]com
- jordan-tourism[.]com
- jordan-trip[.]com
- kazakhstantourism-online[.]com
- kelseyandben[.]life
- kenya-visitonline[.]com
- laosonlinetourism[.]com
- logisticeconomy[.]com
- m1nsk[.]club
- malawitourism-online[.]com
- malaysiaonline-tourism[.]com
- natalia-akulich[.]org
- nationalday87[.]com
- nbramad[.]com
- ogermonthly[.]com
- oknabrest[.]click
- oman-onlinetourism[.]com
- podomam[.]org
- prebooking[.]cn
- promartialarts[.]info
- qatar-onlinetourism[.]com
- qataronline-travels[.]com
- radio-mir[.]org
- raisethegaze[.]org
- raskopki[.]org
- saudiarabiaglobaltourism[.]com
- saudiarabiatour-online[.]com
- saudiarabiatouronline[.]com
- taiwantourismonline[.]com
- taiwantravel-services[.]com
- tajikistan-onlinetourism[.]com
- uganada-onlinetourism[.]com
- uganadaonline-travels[.]com
- uganda-visitonline[.]com
- vezard[.]biz
- viabiz[.]org
- vietnam-tourismonline[.]com
- wemarkt[.]biz
- wemarkt[.]info
- wemarkt[.]org
- xzinfo[.]org
- yunix[.]biz
- zabelov[.]info
- zambia-onlinetourism[.]com
- zambiaonline-travels[.]com

Sample Additional IP Addresses

- 104[.]21[.]0[.]157
- 104[.]21[.]10[.]180
- 104[.]21[.]13[.]166
- 172[.]67[.]129[.]40
- 172[.]67[.]133[.]188
- 172[.]67[.]140[.]16
- 199[.]59[.]243[.]227
- 70[.]34[.]210[.]52

Sample IP-Connected Domains

- ftp[.]teamviewer-9[.]ru
- heylele[.]com
- mail[.]teamviewer-9[.]ru

Sample String-Connected Domains

- easybackupcloud[.]eu
- economymentor[.]online
- egyptican[.]net
- finances-news[.]club
- finances-news[.]ml
- finances-news[.]online
- inclusive-economy[.]org
- jordanrefugees[.]info
- jordanrefugees[.]net
- jordanrefugees[.]org
- jordansons[.]co[.]uk
- master-dental[.]co[.]uk
- master-dental[.]com[.]tw
- master-dental[.]net
- microsoftwindowshelp[.]cf
- microsoftwindowshelp[.]online
- microsoftwindowshelp[.]press
- saudiarabianow[.]com
- saudiarabianow[.]net
- saudiday[.]com
- saudiday[.]net
- saudiday[.]online
- suppertools[.]com[.]pk
- suppertools[.]live
- suppertools[.]online
- wellhealthtech[.]ca
- wellhealthtech[.]org

Sample String-Connected Subdomains

- support-api[.]2010traefik[.]app[.]fidelity[.]com
- support-api[.]academig[.]auth0[.]com
- support-api[.]acc[.]env[.]hiber[.]cloud
- support-api[.]aile[.]auth0[.]com
- support-api[.]airbnb[.]bnnr[.]com
- support-api[.]airbnb[.]graphics[.]com
- support-api[.]airbnb[.]logview[.]com
- support-api[.]airbnb[.]macadmin[.]com
- support-api[.]airbnb[.]manufacturers[.]com
- support-api[.]airbnb[.]pages[.]com
- support-api[.]apicw[.]cs[.]scania[.]com
- support-api[.]app[.]optimizely[.]com
- support-api[.]ascentcloud-prod-cd-ti8t1jcfztiwqgai[.]auth0[.]com
- support-api[.]ashaya[.]pam-cudaops[.]com
- support-api[.]assist[.]parokistmarkusmelak[.]org
- support-api[.]at[.]icdc[.]io
- support-api[.]autotaal[.]bizt-1[.]stg[.]ivf[.]basepairtech[.]com
- support-api[.]avantllc[.]auth0[.]com
- support-api[.]aws[.]dblabs[.]net
- support-api[.]battlenet[.]ces[.]co
- support-api[.]bgonz[.]pam-cudaops[.]com
- support-api[.]blog[.]hotelscombined[.]com
- support-api[.]blue[.]edayinsure[.]co[.]uk
- support-api[.]bofl01mstr5pe8minte[.]app[.]optimizely[.]com
- trendingcharts[.]org[.]clearwebstats[.]com