WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

DNS Insights on a Free Form Builder Service Phishing Campaign

Table of Contents

Executive Report

Unit 42 of Palo Alto Networks recently uncovered a phishing campaign targeting European companies to harvest victims' account credentials and take over their Microsoft Azure cloud infrastructure. According to their report, the phishing attempts leveraging the HubSpot Free Form Builder service peaked in June 2024.

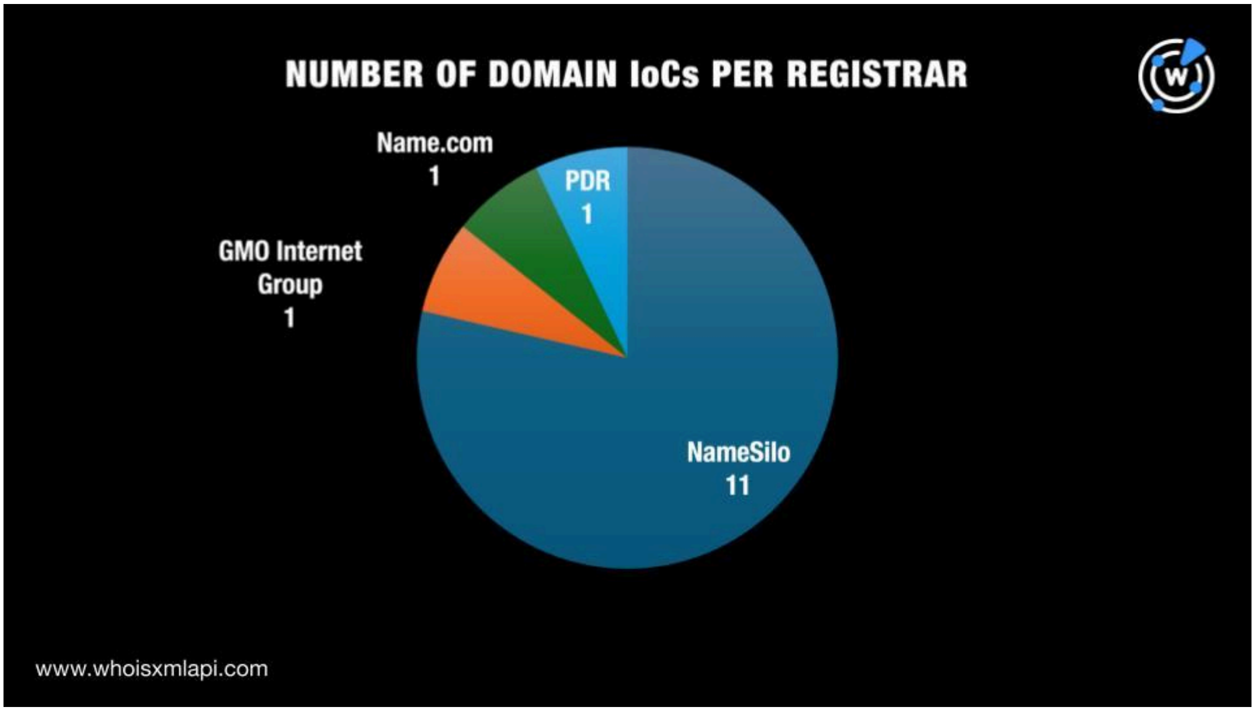
The researchers identified 18 domains and 17 IP addresses as indicators of compromise (IoCs) based on their in-depth analysis. The WhoisXML API research team expanded the IoC list in a bid to uncover other potentially connected artifacts. Note, however, that since two domain IoCs—cloudfront[.]net and hsforms[.]com—are owned by legitimate companies, we opted to exclude them from our expansion analysis. As a result, we were left with 33 IoCs—16 domains and 17 IP addresses. Our hunt for connected artifacts led to the discovery of:

- 16 email-connected domains
- Four additional IP addresses
- 185 IP-connected domains
- 289 string-connected domains

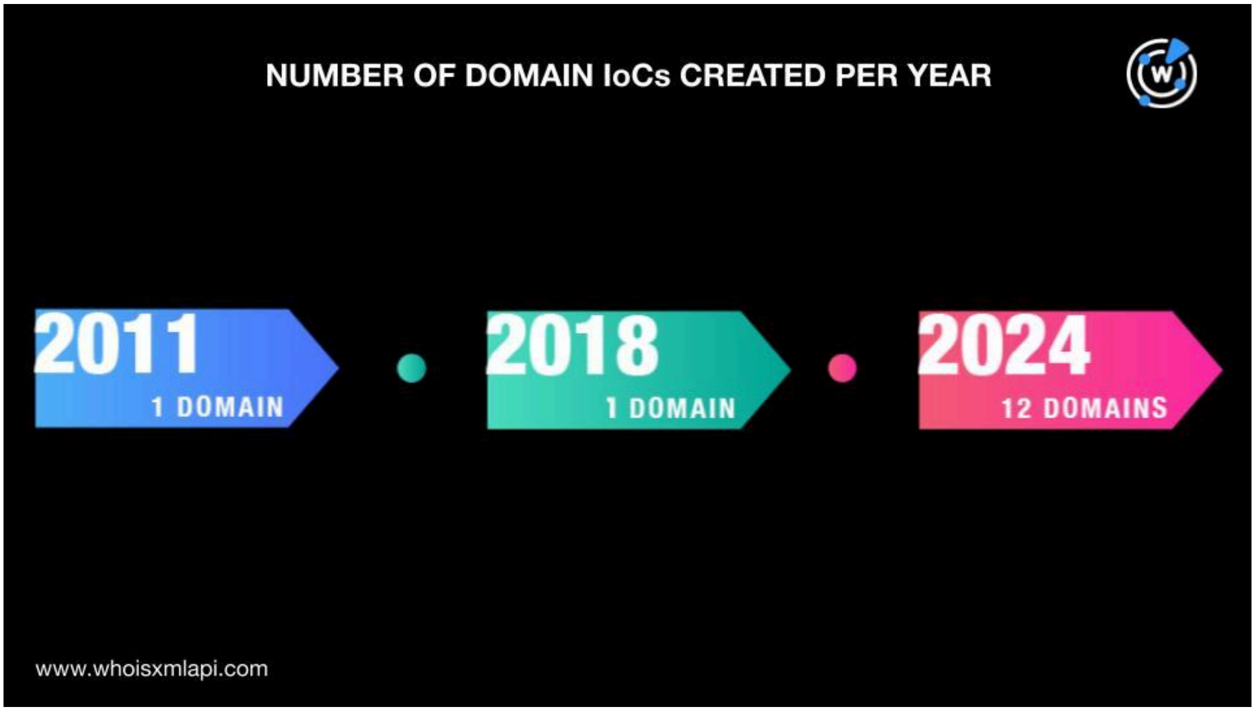
More Facts about the IoCs

First off, we sought to find more information about the 33 IoCs starting with a Bulk WHOIS Lookup query for the 16 domains tagged as IoCs. We discovered that only 14 of them had current WHOIS records.

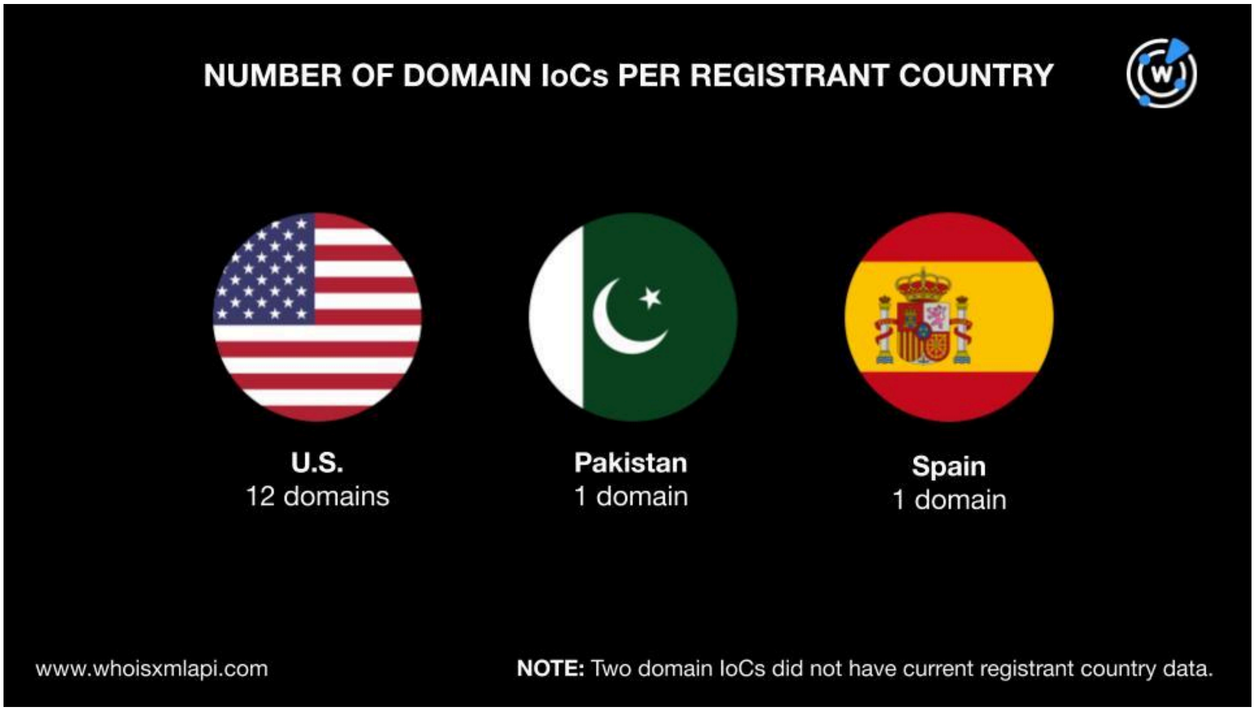
- They were administered by four different registrars. NameSilo took the top spot with 11 domains. GMO Internet Group, Name.com, and PDR administered one domain each.



- They were created between 2011 and 2024. Specifically, 12 were created in 2024, while one domain each was created in 2011 and 2018.



- They were registered in three countries—12 in the U.S. and one each in Pakistan and Spain. Two domains did not have current registrant country data.



NUMBER OF DOMAIN IoCs PER REGISTRANT COUNTRY

U.S.
12 domains

Pakistan
1 domain

Spain
1 domain

www.whoisxmlapi.com

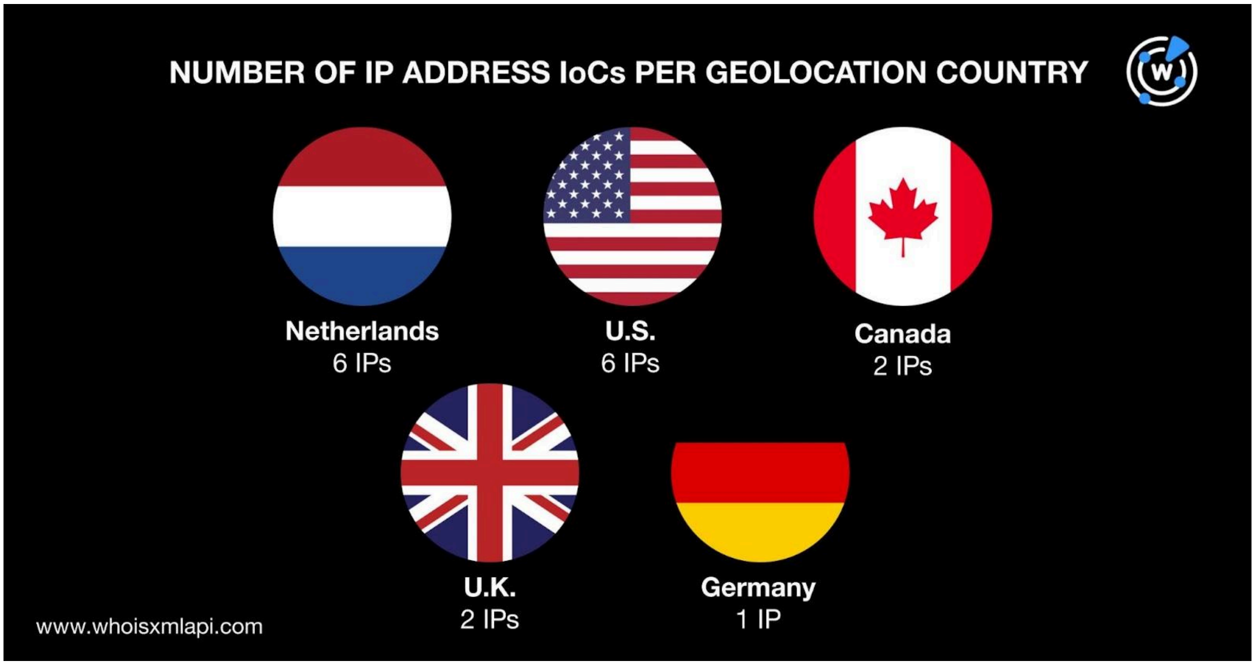
NOTE: Two domain IoCs did not have current registrant country data.

A query on DNS Chronicle API revealed that all 16 domains tagged as IoCs had historical IP resolutions. The domain cyptech[.]com[.]au had the oldest first IP resolution date—6 October 2019. It also had 41 IP resolutions over time. Altogether, the 16 domain IoCs had 1,432 IP resolutions so far. Take a look at the details for five other domains below.

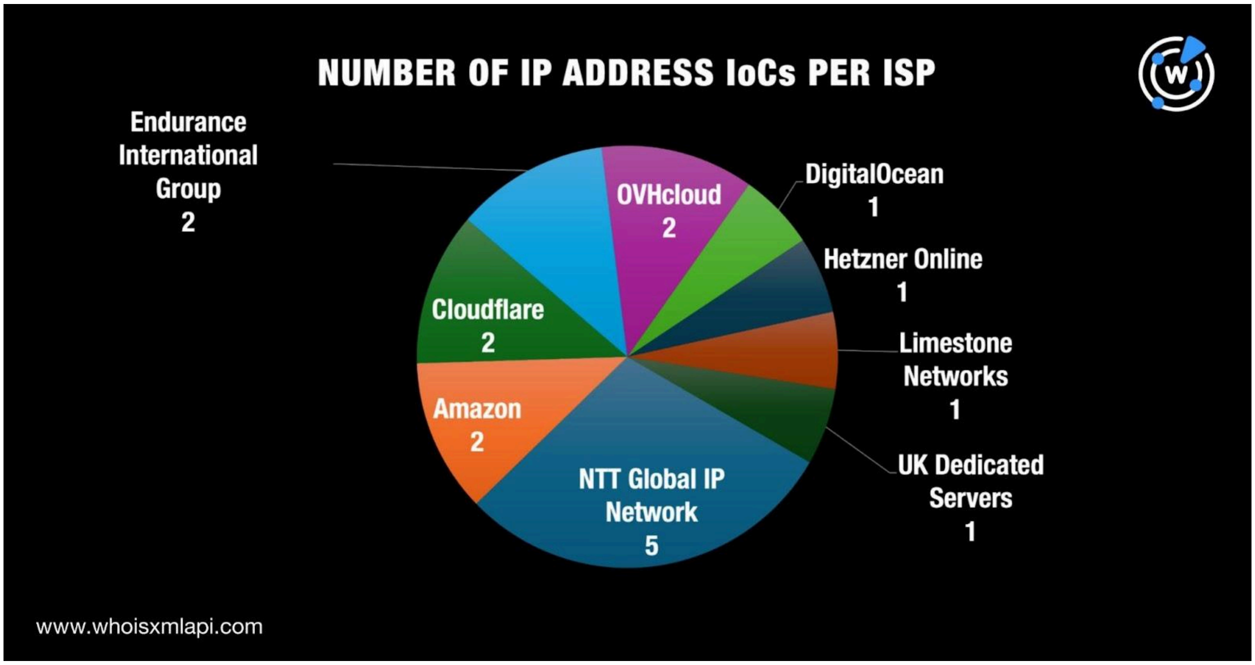
DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION START DATE	LAST IP RESOLUTION START DATE
espersonal[.]org	130	8 September 2022	11 October 2024
vigaspino[.]com	78	9 October 2019	13 November 2024
qeanonsop[.]xyz	13	25 June 2024	9 August 2024
doc2rprevn[.]buzz	6	26 June 2024	3 November 2024
dgpropertyconsultants[.]buzz	5	25 June 2024	30 August 2024

Next, we queried the 17 IP addresses tagged as IoCs on Bulk IP Geolocation Lookup and found that:

- They were geolocated in five countries led by the Netherlands and the U.S., which accounted for six IP addresses each. Two IoCs each were geolocated in Canada and the U.K., while one originated from Germany.



- They were administered by nine ISPs led by NTT Global IP Network, which accounted for five IP addresses. Two IoCs each were administered by Amazon, Cloudflare, Endurance International Group, and OVHcloud. Finally, one IP address each was administered by DigitalOcean, Hetzner Online, Limestone Networks, and UK Dedicated Servers.



Our DNS Chronicle API query for the 17 IP addresses tagged as IoCs showed that all of them had 6,456 historical domain resolutions so far. The IP addresses 144[.]217[.]158[.]133, 167[.]114[.]27[.]228, 208[.]91[.]198[.]96, and 74[.]119[.]239[.]234 recorded the oldest first domain resolution date—4 October 2019. Take a look at specific details for five other IP address IoCs below.

IP ADDRESS IoC	NUMBER OF DOMAIN RESOLUTIONS	FIRST DOMAIN RESOLUTION START DATE	LAST DOMAIN RESOLUTION START DATE
104[.]21[.]25[.]8	1,000	14 January 2021	28 August 2021
172[.]67[.]221[.]137	1,000	28 May 2020	17 October 2020
18[.]67[.]38[.]155	223	19 November 2021	15 November 2024
13[.]40[.]68[.]32	34	19 November 2021	3 November 2024
208[.]115[.]208[.]118	14	27 January 2020	18 August 2024

The Hunt for Connected Artifacts

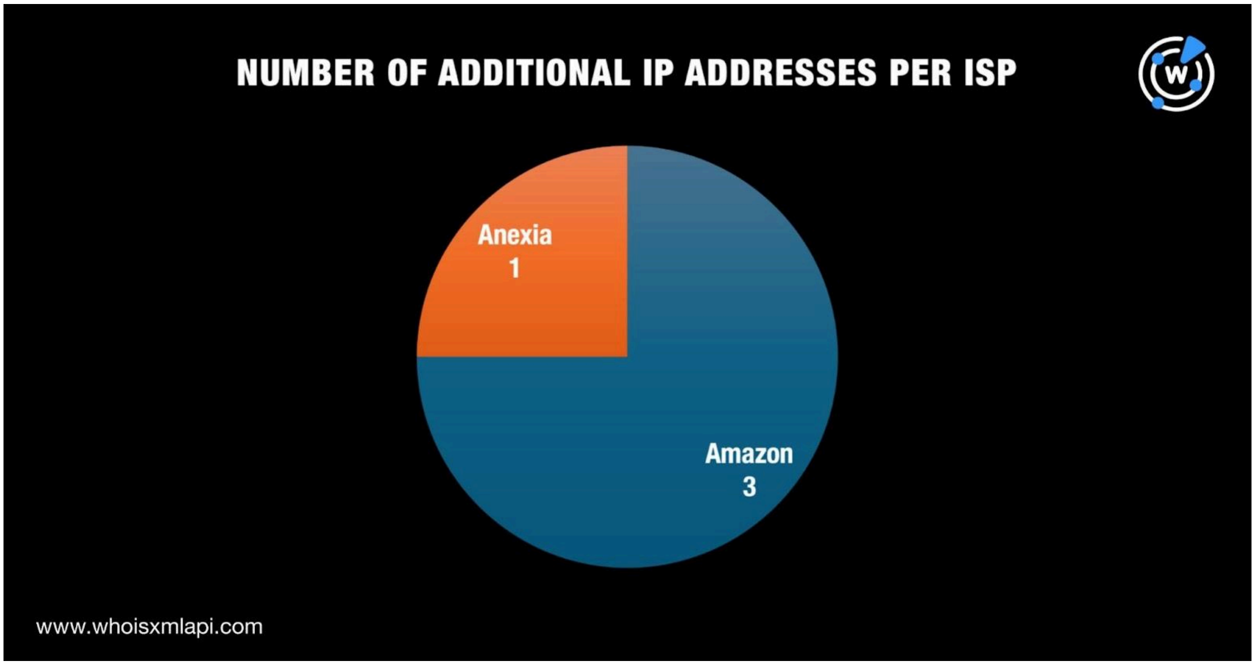
We began our search for connected artifacts with a WHOIS History API query for the 16 domains tagged as IoCs. We found that two of them had four email addresses in their historical WHOIS records after duplicates were filtered out. Three of them were public email addresses.

Only two of the public email addresses appeared in the current WHOIS records of other domains. One of them, however, could belong to a domainer, leaving us with only one email address for our analysis. The sole public email address left on our list was shared by 16 domains after duplicates and the IoCs were filtered out.

A DNS Lookup API query for the 16 domains tagged as IoCs revealed that five of them actively resolved to four IP addresses not yet identified as IoCs.

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

- They were geolocated in two countries—three in the U.S. and one in Austria.
- They were administered by two ISPs—three by Amazon and one by Anexia.



Now, we have a total of 21 IP addresses that we queried on Reverse IP API, which revealed that only 15 resolved domains. Seven of the 15 IP addresses could be dedicated hosts. Altogether, they hosted 185 domains after we filtered out duplicates, those already identified as IoCs, and the email-connected domains.

As our last step, we queried the 16 text strings from the 16 domains tagged as IoCs on Domains & Subdomains Discovery and found that 10 of them started other domains. These strings were:

- cyptech.
- dgpropertyconsultants.
- espersonal.
- europeanfreightleaders.
- fundament-advisory.
- industrialization.
- netlify.
- symmetric.
- tekfenconstruction.
- vermeernigeria.

We uncovered 289 string-connected domains after filtering out duplicates, those already identified as IoCs, and the email- and IP-connected domains.

—

Our IoC list expansion analysis for the phishing campaign targeting the HubSpot Free Form Builder service led to the discovery of 494 connected artifacts comprising 16 email-connected domains, four additional IP addresses, 185 IP-connected domains, and 289 string-connected domains.

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

- aislamientoslurgoien[.]com
- caminodesantiagowalkingtours[.]com
- euskaraelkargoa[.]org
- laverandagastrobar[.]com
- microaudioburlada[.]com
- oinezbasoa[.]net
- oinezbasoa[.]org
- pilimili[.]net

Sample Additional IP Addresses

- 13[.]52[.]115[.]166
- 152[.]53[.]111[.]110

Sample IP-Connected Domains

- adeem[.]ae
- alfalakmedia[.]com
- alhammadimpex[.]com
- alkarampackages[.]com[.]pk
- altas[.]ae
- army-share[.]com
- atta-e-ghazi[.]com
- aysis[.]ae
- bauersy[.]top
- bnoosasowiped[.]xyz
- burhanbaig[.]com
- d1qlfzaj83ldxx[.]cloudfront[.]net
- d37unsldgykj8z[.]cloudfront[.]net
- dataviewsolution[.]com
- ddexchange[.]com
- doc2viewsn[.]top
- docfil024pdft[.]top
- docs2signview2024us[.]top
- docscanus2024[.]top
- docsvius[.]buzz
- doimoscis[.]xyz
- dtek[.]pk
- fabgroup[.]com[.]pk
- faisalplastic[.]com
- fildocspre024[.]top
- foursquaretravels[.]com
- ftp[.]adeem[.]ae
- ftp[.]alfalakmedia[.]com
- ftp[.]alhammadimpex[.]com
- ftp[.]alkarampackages[.]com[.]pk
- ftp[.]altas[.]ae
- ftp[.]atta-e-ghazi[.]com
- ftp[.]aysis[.]ae
- ftp[.]burhanbaig[.]com
- ftp[.]dataviewsolution[.]com
- ftp[.]ddexchange[.]com
- ftp[.]dtek[.]pk
- ftp[.]fabgroup[.]com[.]pk
- ftp[.]faisalplastic[.]com
- ftp[.]foursquaretravels[.]com
- ftp[.]imagenextgen[.]com
- ftp[.]innovix[.]com[.]pk
- ftp[.]isdulara[.]com
- ftp[.]jaffzimpex[.]com
- ftp[.]jordan[.]org[.]pk
- ftp[.]lassani[.]com[.]pk
- ftp[.]seaimpressions[.]com[.]pk
- ftp[.]solar360[.]pk
- ftp[.]superauto[.]ae
- ftp[.]think-com[.]com

Sample String-Connected Domains

- cyptech[.]co[.]ke
- cyptech[.]co[.]uk
- cyptech[.]com
- dgpropertyconsultants[.]co[.]uk
- dgpropertyconsultants[.]com
- dgpropertyconsultants[.]in
- espersonal[.]com
- espersonal[.]com[.]br
- espersonal[.]cz
- europeanfreightleaders[.]eu
- fundament-advisory[.]com
- fundament-advisory[.]de
- industrialization[.]africa
- industrialization[.]arab
- industrialization[.]art
- netlify[.]ai
- netlify[.]asia
- netlify[.]at

- symmetric[.]academy
- symmetric[.]ae
- symmetric[.]africa
- tekfenconstruction[.]com
- tekfenconstruction[.]com[.]tr