Stripping Down the BlackSuit Ransomware Network Aided by DNS Data

Table of Contents

Executive Report

Nearly 1 million individuals' information was stolen and exposed when threat actors launched a BlackSuit ransomware attack on 10 April 2024. The investigation revealed that the compromised data included the victims' Social Security numbers (SSNs), birthdays, and insurance claim information.

Data breach notifications were sent in the last week of August. Around that time, specifically on 27 August 2024, the Cybersecurity and Infrastructure Security Agency (CISA) also updated its BlackSuit ransomware advisory. Their latest STIX file contains 91 indicators of compromise (IoCs) comprising 14 domain names, five subdomains, and 72 IP addresses. The agency also revealed that Blacksuit is a rebranded version of the Royal ransomware, a threat group that targeted healthcare organizations and demanded ransom payments ranging from US$250,000 to US$2 million.

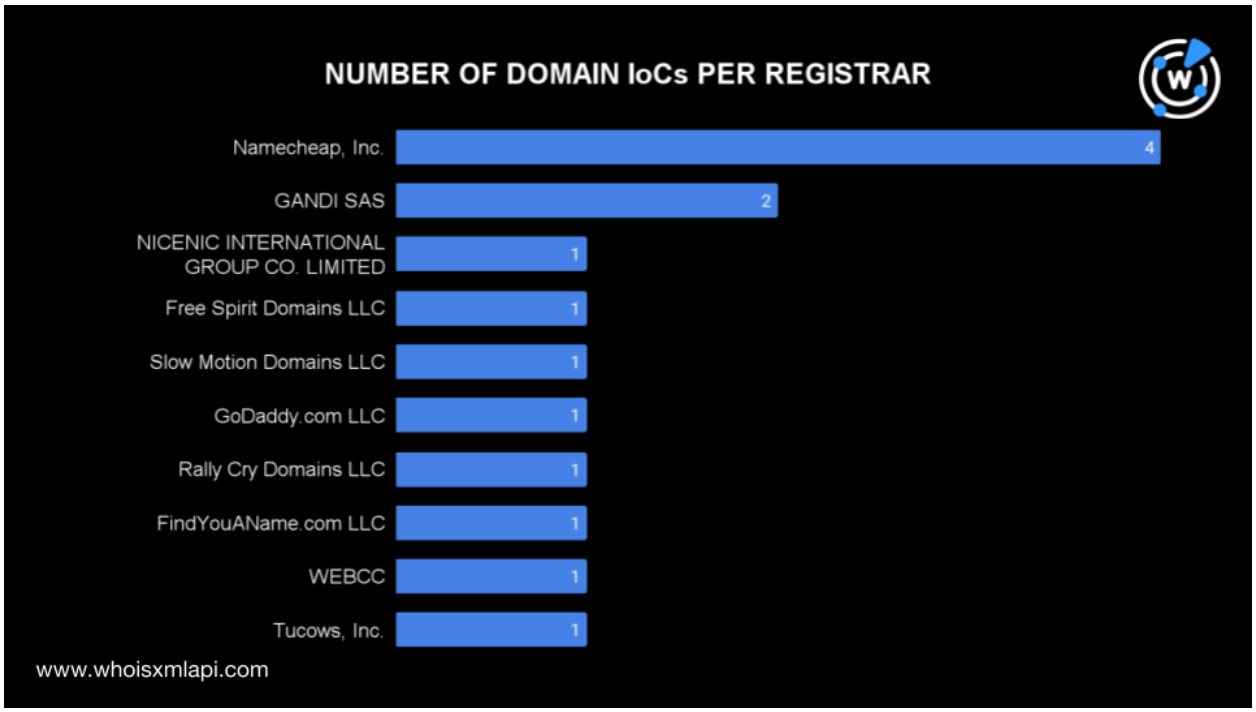
The WhoisXML API research team pivoted off these cyber resources to expand the list of IoCs and uncover relevant threat artifacts. The analysis led to the discovery of:

- 112 email-connected domains
- 10 additional IP addresses, five of which were found to be malicious
- 21 IP-connected domains
- 137 string-connected domains

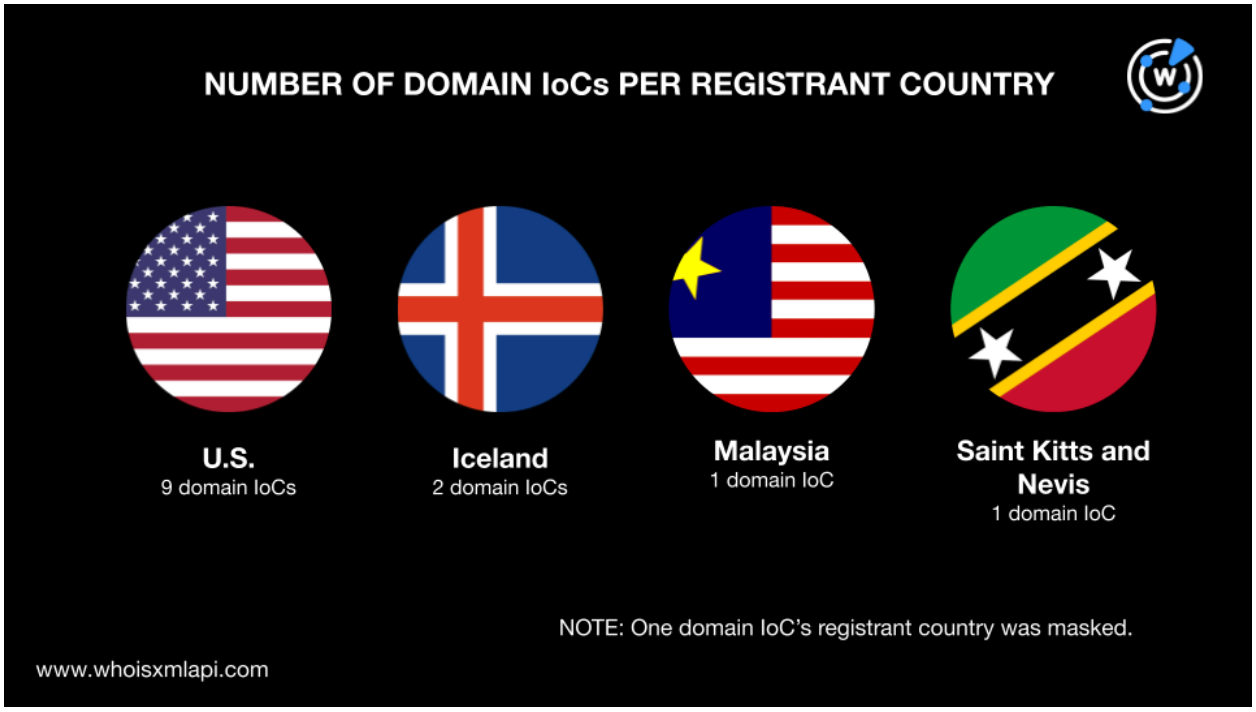
What We Know about the BlackSuit IoCs

To learn more about the published IoCs, we first ran the 15 domains, comprising the 14 domain names identified as IoCs and one domain extracted from the subdomain IoCs, on Bulk WHOIS Lookup. We found that one domain IoC did not have current WHOIS data and thus was excluded from the analysis.

- Four domain IoCs were registered with Namecheap, Inc.; two with GANDI SAS; and one domain each with NiceNIC International Group Co. Limited; Free Spirit Domains LLC; Slow Motion Domains LLC; GoDaddy.com LLC; Rally Cry Domains LLC; FindYouAName.com LLC; WEBCC; and Tucows, Inc.

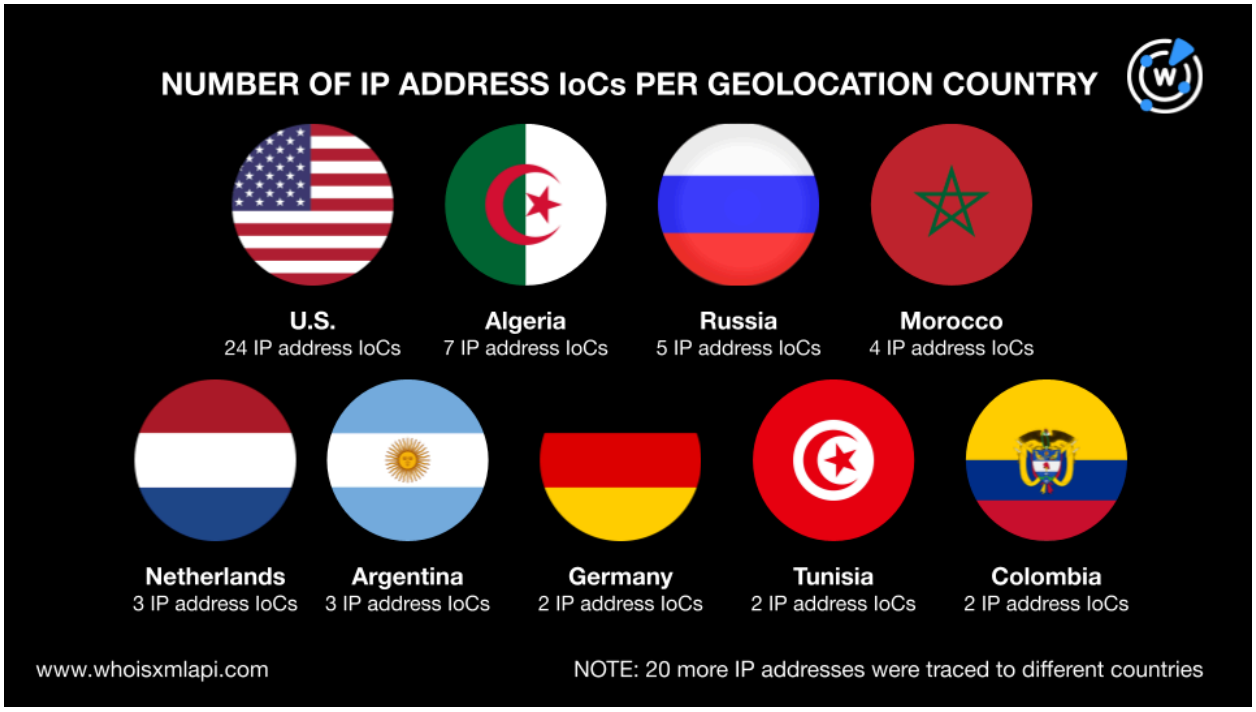


- A majority of the domain IoCs, seven to be exact, were registered in 2024. Four were created in 2023, while one IoC each was created in 2010, 2021, and 2022.
- Nine domain IoCs were registered in the U.S. and two in Iceland. Malaysia and Saint Kitts and Nevis accounted for one domain IoC each.

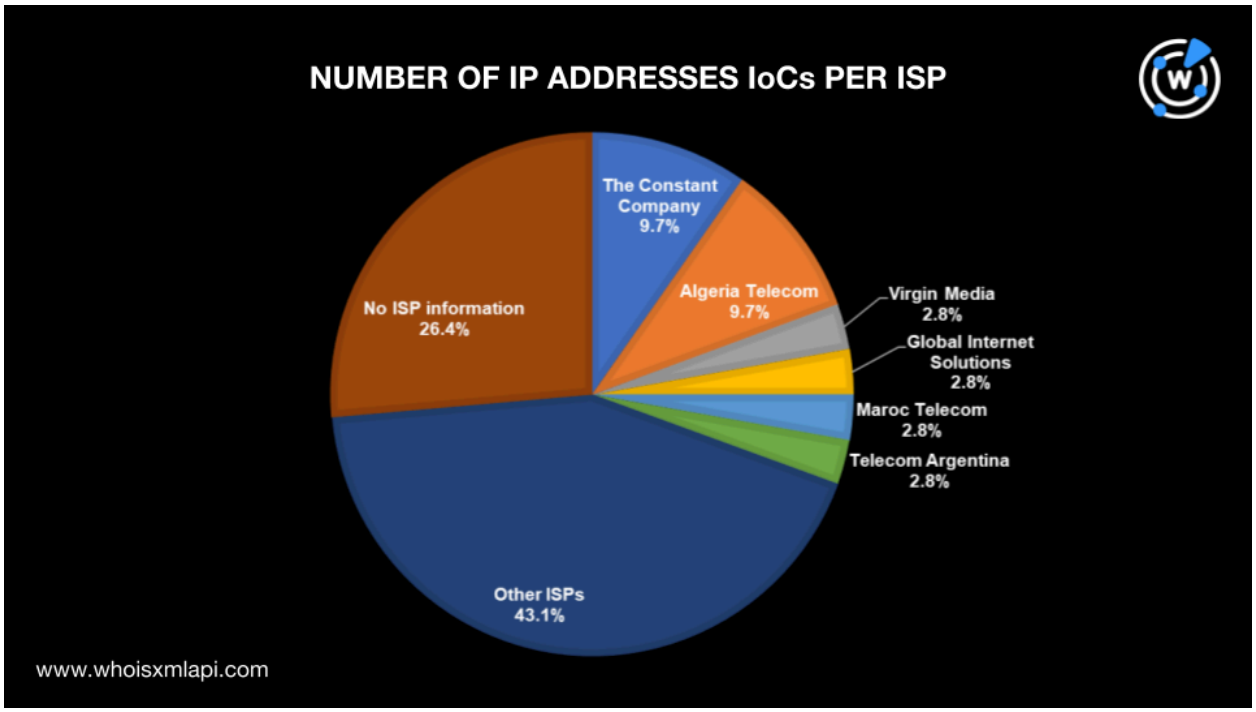


Next, we ran a bulk IP geolocation lookup for the 72 IP addresses identified as IoCs and found that:

- Their geolocations were distributed across 29 countries. A majority were traced to the U.S. (24 IP addresses), Algeria (seven IP addresses), Russia (five IP addresses), and Morocco (four IP addresses). Three IP address IoCs each were geolocated in the Netherlands and Argentina, while two each were geolocated in Germany, Tunisia, and Colombia. Twenty other countries accounted for one IP address IoC each.



- The Constant Company and Algeria Telecom administered seven IP addresses each, while Virgin Media, Global Internet Solutions, Maroc Telecom, and Telecom Argentina administered two IP addresses each. Thirty-one other ISPs accounted for one IP address IoC each, while 19 IP addresses did not have current ISP information.



Uncovering Potential BlackSuit Ransomware Threat Artifacts

To proactively hunt for potential BlackSuit-related threats, we queried the 14 domain IoCs and one subdomain IoC root domain on WHOIS History API. The results showed that they had 31 email addresses in their historical WHOIS records, five of which were public.

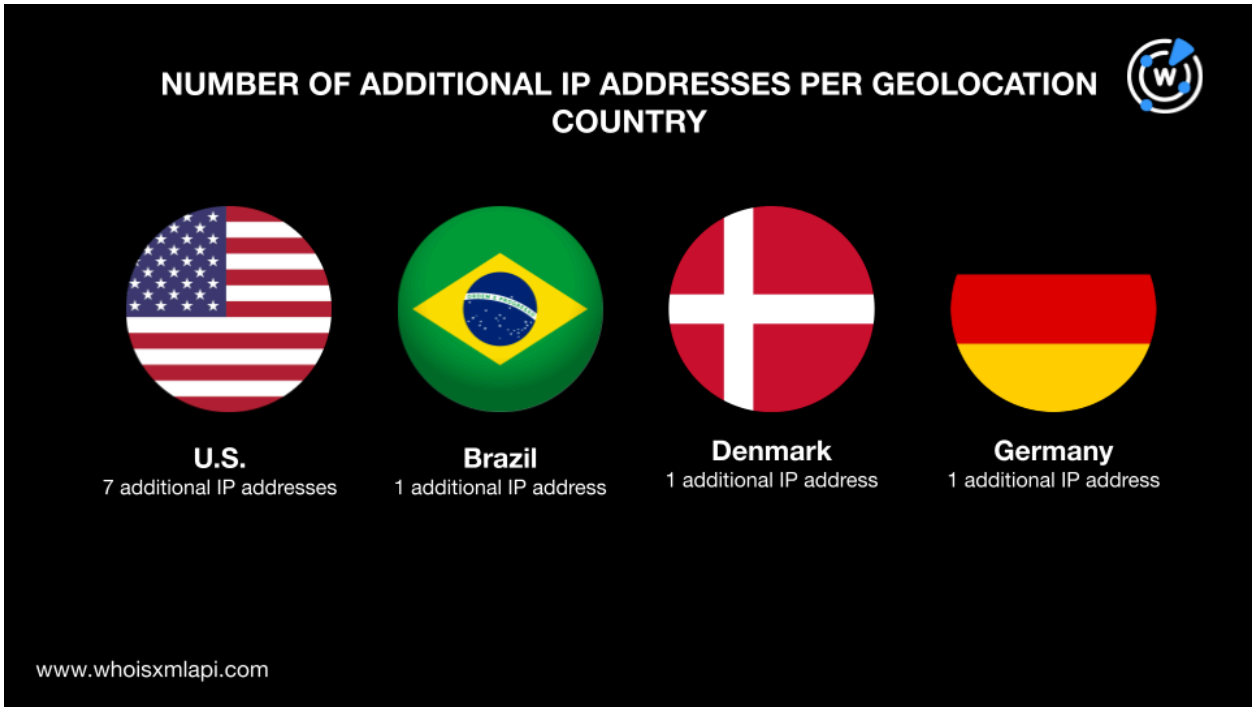
Jumping off the five public email addresses, our Reverse WHOIS API queries led to the discovery of 112 email-connected domains after removing duplicates and the IoCs.

We then ran the 14 domain IoCs and five subdomain IoCs on DNS Lookup and found out that while four did not have active IP resolutions, the remaining 15 resolved to 10 IP addresses not on the original IoC list. Threat Intelligence Lookup revealed that five of them were associated with various threats. Two examples are shown below.

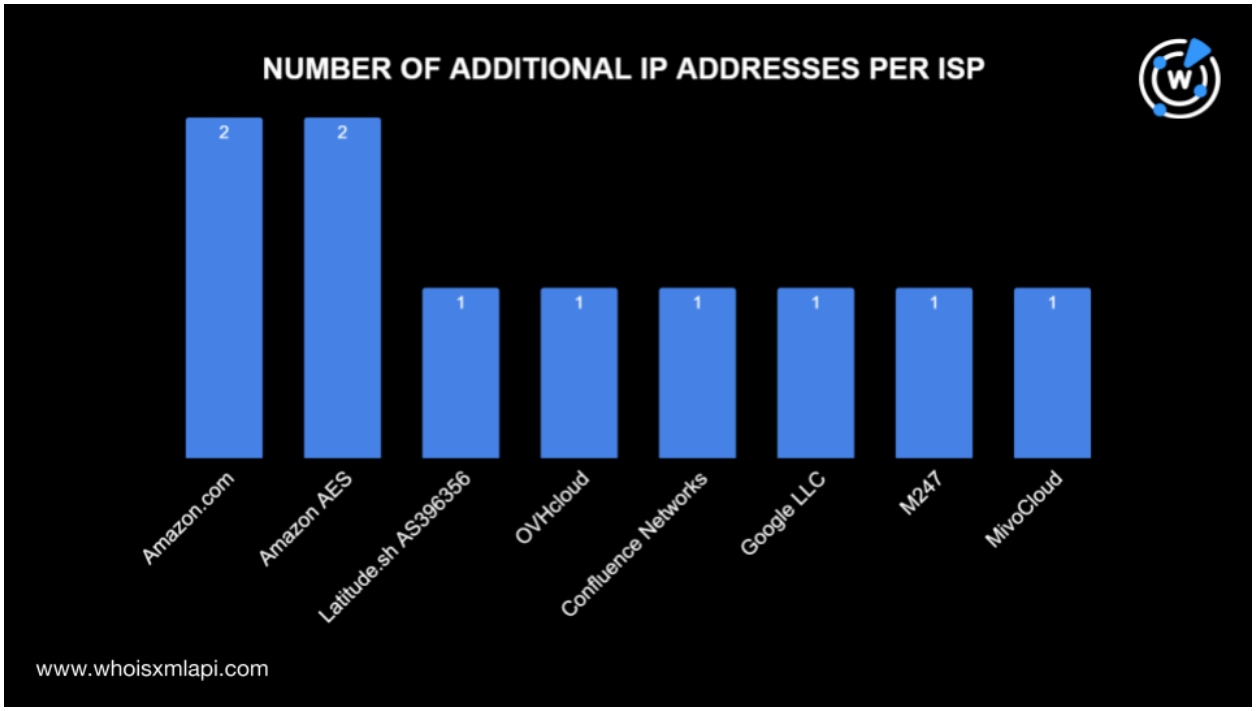
ADDITIONAL IP ADDRESS	ASSOCIATED THREAT TYPES
45[.]12[.]221[.]10	Malware Command-and-control (C&C)
52[.]223[.]13[.]41	Attack C&C Generic Malware Phishing

A bulk IP geolocation lookup for the 10 additional IP addresses revealed that:

- They were spread across four geolocation countries, with the U.S. accounting for a majority of the IP addresses—seven to be exact. Brazil, Denmark, and Germany each accounted for one additional IP address.



- Amazon.com and Amazon AES administered two additional IP addresses each, while Latitude.sh AS396356, OVHcloud, Confluence Networks, Google LLC, M247, and MivoCloud accounted for one additional IP address each.



Next, we queried the 82 IP addresses (72 identified as IoCs and 10 additional ones) on Reverse IP Lookup and found that while 58 had no resolving domains, 21 could be dedicated. They led to 21 IP-connected domains after filtering out duplicates, the IoCs, and the email-connected domains.

We then searched the DNS for domains that started with similar text strings as the domain IoCs, specifically:

- **turnovercheck**
- **tumbleproperty**
- **turnovercheck.com**
- **abbeymathiass.com**
- **sombrat**
- **softeruplive**
- **sombrat**
- **softeruplive**
- **recruitment + interview**
- **parkerpublic**
- **bublup**
- **myappearinc**
- **megupdate**
- **hourlyprofitstore**
- **gororama**
- **ciborkumari**
- **altocloud**
- **abbeymathiass**
- **zoom** + contains **manager**
- **recruitment** + contains **interview**

Since some of the IoCs were also subdomains residing on turnovercheck[.]com and abbeymathiass[.]com, we also queried the domains on Subdomains Lookup. Overall, we found 137 string-connected web properties after filtering out duplicates, the IoCs, and the email- and IP-connected domains. One of them was associated with malware attacks, according to Threat Intelligence API.

Overall, we uncovered 270 connected domains (i.e., email-, IP-, and string-connected). Aside from the commonalities in the email address, IP resolution, and text strings, how else do they compare with the domain IoCs? After obtaining the WHOIS information of all the connected domains, we discovered that:

- 11 connected domains shared the domain IoCs' registrars
- 16 of them were created in the same years as a majority of the domain IoCs (i.e., 2024 and 2023)
- 31 connected domains were registered in the same countries as the domain IoCs

—

Our DNS deep dive into the latest BlackSuit ransomware campaign began with 91 IoCs comprising 14 domains, five subdomains, and 72 IP addresses. WHOIS, IP, and string analyses of these properties led to the discovery of 280 artifacts made up of 112 email-connected

domains, 10 additional IP addresses, 21 IP-connected domains, and 137 string-connected domains. Five of the 10 additional IP addresses and one string-connected domain 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

- joyfulpetwork[.]com
- wintervacation[.]rentals
- lookatmeowrescue[.]org
- euthlist[.]org
- findmeow[.]org
- pawscrossednyc[.]org
- dspca[.]org
- joyfulpetpark[.]org
- joyfulpetnetwork[.]org
- joyfulpetworking[.]org
- tinykittencafe[.]org
- tinykittenrescue[.]org
- urgentpetnation[.]org
- sickkittens[.]org
- fostermekitten[.]org
- sickkitten[.]org
- photooftheday[.]style
- photooftheday[.]dog
- joyfulpets[.]mobi
- joyfulpets[.]online
- eastcoastrescueme[.]com
- bestpuppynames[.]org
- puppynursery[.]org
- fostercaredirectory[.]org
- fipkittens[.]org
- joyfulpettherapy[.]org
- petjoytherapy[.]org
- petlovetherapy[.]org
- citykittycafe[.]org
- urgentkittens[.]org
- searchapet[.]org
- awwsomepets[.]org
- urgentcatrescue[.]org
- ezpetsearch[.]org
- adoptforgood[.]org
- dailykitten[.]org
- kittenfoundation[.]org
- applicationzoom[.]org
- petrescuenation[.]org
- lostcatnetwork[.]info
- lostcatnetwork[.]org
- ivyzoom[.]org
- puppiestoadopt[.]org
- therehomery[.]org
- adoptuspetsfoundation[.]org
- adoptuspet[.]org

- adoptuspets[.]org
- lovemeowrescue[.]org
- akiam[.]org
- padopt[.]org

Sample IP-Connected Domains

- dyn98-143-70-147[.]hsia[.]mnsi[.]net
- padresixnine[.]com
- xn----8sbafosdfg6ael2aijgya3cyf7a[.]xn--p1ai
- cpc4-lock3-2-0-cust196[.]6-1[.]cable[.]virginm[.]net
- changelemon[.]com
- onemore404[.]com
- beamofthemoon[.]com
- elsa3eedhosting[.]com
- hubspotdashboard[.]com
- ns102290[.]ip-147-135-36[.]us

Sample String-Connected Domains

- bublup[.]support
- bublupshop[.]com
- bublupstaging[.]me
- bublup[.]fun
- bublupvcdn[.]com
- bublupmcdn[.]com
- bublupdev[.]info
- bubluprolls[.]com
- bublup[.]us
- bublup[.]dev
- bublupdevops[.]com
- bubluproll[.]com
- bublupbackup[.]com
- bublup[.]photos
- bublup[.]net
- bublup[.]tv
- bublup[.]co[.]uk
- bublup[.]in
- bublup[.]de
- bublup[.]top
- bublup[.]cloud
- bublup[.]com
- bublupimports[.]com
- bublupmedia[.]com
- bubluptest[.]com
- bublupdcdn[.]com
- bublupqa[.]com
- bublupstaging[.]com
- bublup[.]uk
- bublupper[.]com
- bublup[.]nl
- bublup[.]info
- bublup[.]jp
- bublupcdn2[.]com
- bublup[.]es
- bublup[.]app
- bubluptesting[.]com
- bublup[.]io
- bublupdevopscdn[.]com
- bublup[.]sale
- bublupnotices[.]com
- bubluphq[.]com
- bublup[.]xyz
- bublup[.]business
- bublup[.]events
- bublup[.]news
- bublup[.]design
- bublup[.]org
- bublup[.]co
- bublup[.]marketing