WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Inspecting Konfety’s Evil Twin Apps through the DNS Lens

Table of Contents

Executive Report

Satori recently published a report on a massive fraud campaign they have dubbed “Konfety” (Russian word for “candy”). Sounds sweet, right? But that’s not the case, as the name references CaramelAds, the mobile ad SDK they abused to create evil twins or malicious duplicates of popular apps available on the world’s biggest app marketplaces. At the time of publication, 250 evil twin apps have been found on Google Play alone.

The researchers published 23 indicators of compromise (IoCs) comprising 17 domain names and six IP addresses, which the WhoisXML API research team expanded using extensive WHOIS, IP, and other DNS intelligence sources. Our in-depth investigation led to the discovery of:

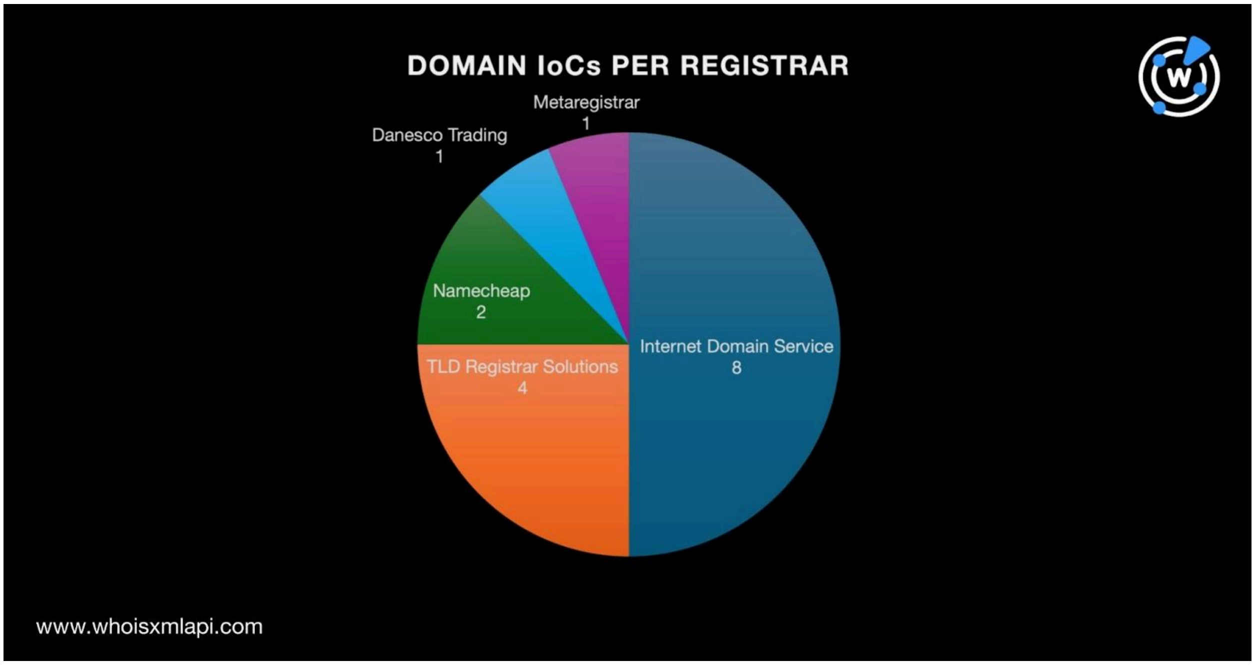
- 302 email-connected domains
- Five additional IP addresses, two of which turned out to be malicious
- Eight IP-connected domains, one of which turned out to be associated with malware distribution
- 326 string-connected domains, one of which turned out to be connected with malware distribution

A Closer Look at the IoCs

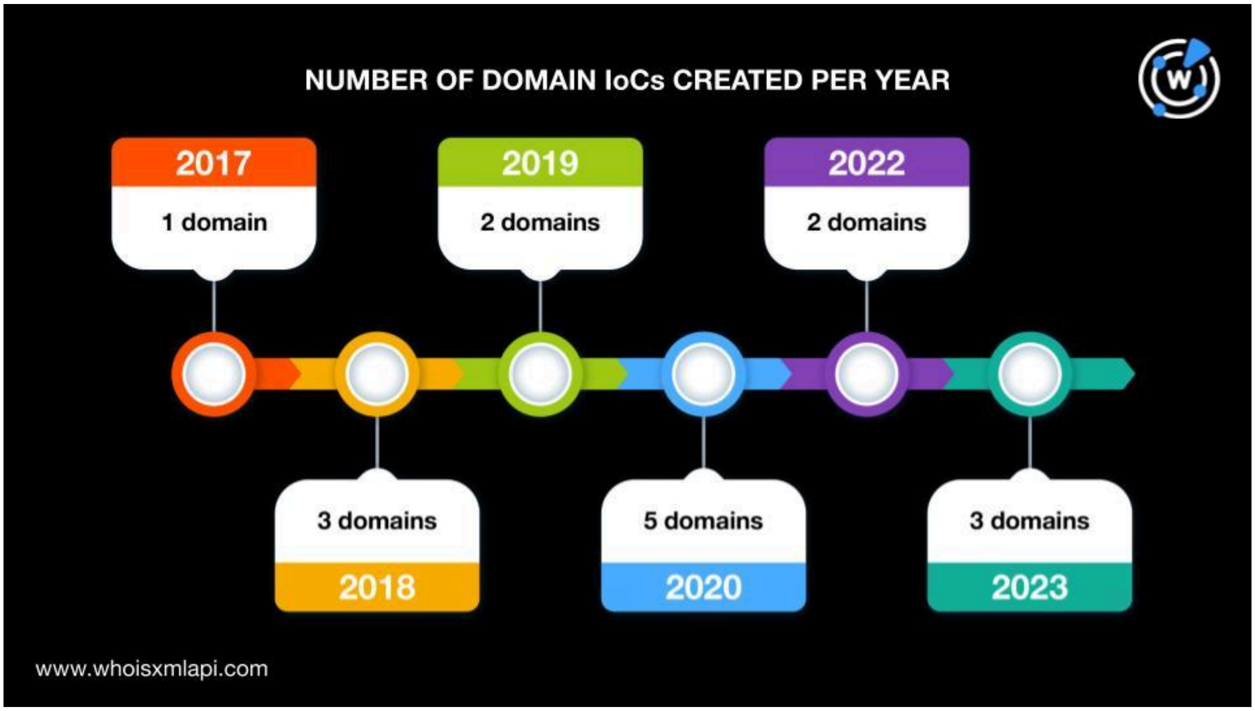
First we gathered more information about the threat by querying the 17 domains identified as Konfety IoCs on Bulk WHOIS Lookup. We found out that:

- One of the domain IoCs didn’t have details in its current WHOIS record, leaving us with 16 domain IoCs for further analysis.
- Internet Domain Service led the pack of registrars, accounting for eight domain IoCs. TLD Registrar Solutions took the second spot with four domain IoCs, followed by

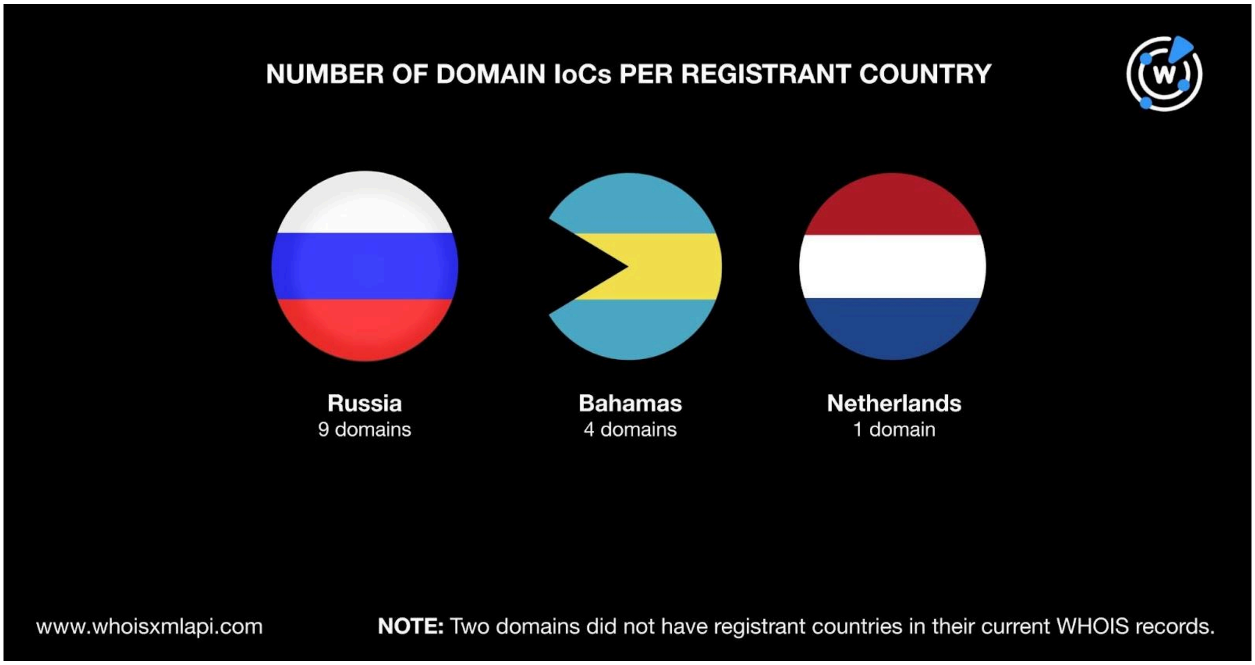
Namecheap with two. Danesco Trading and Metaregistrar tied in last place with one domain IoC each.



- The domain IoCs were created between 2017 and 2023, which shows the threat actors didn’t favor using newly registered domains (NRDs). The highest number of domain IoCs, five to be exact, were created in 2020, in fact.



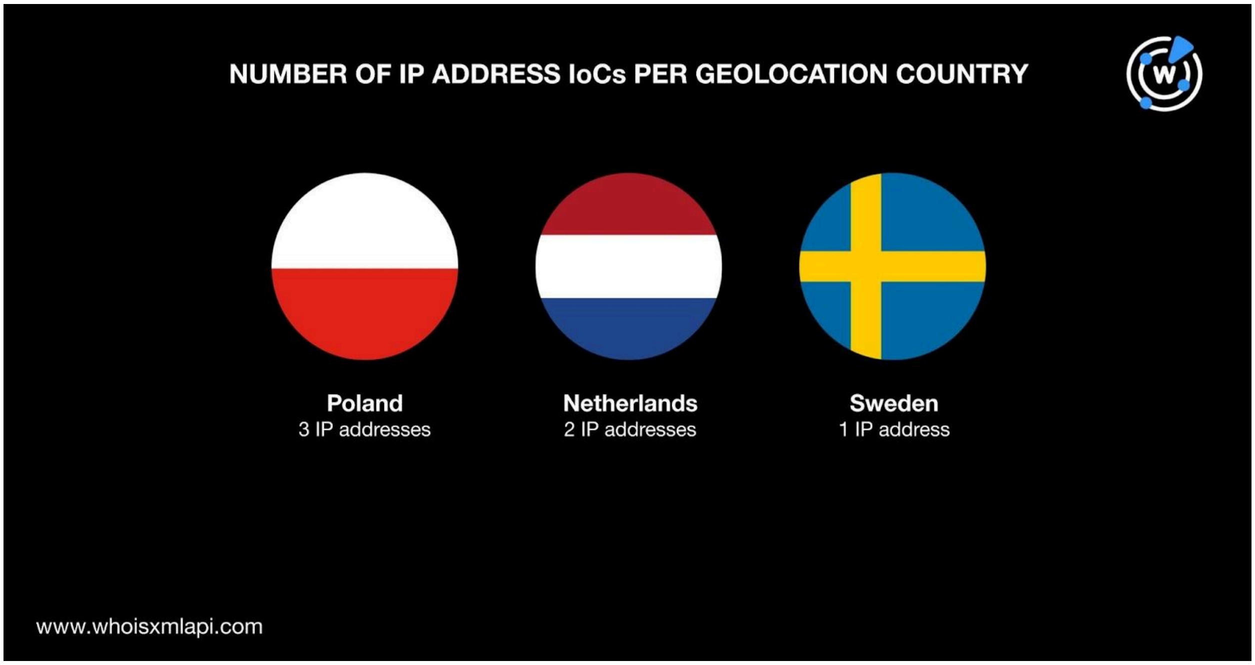
- A majority of the domain IoCs, nine to be exact, were registered in Russia. Bahamas accounted for four domain IoCs, while the Netherlands accounted for one. Two domain IoCs didn’t have registrant countries in their current WHOIS records.



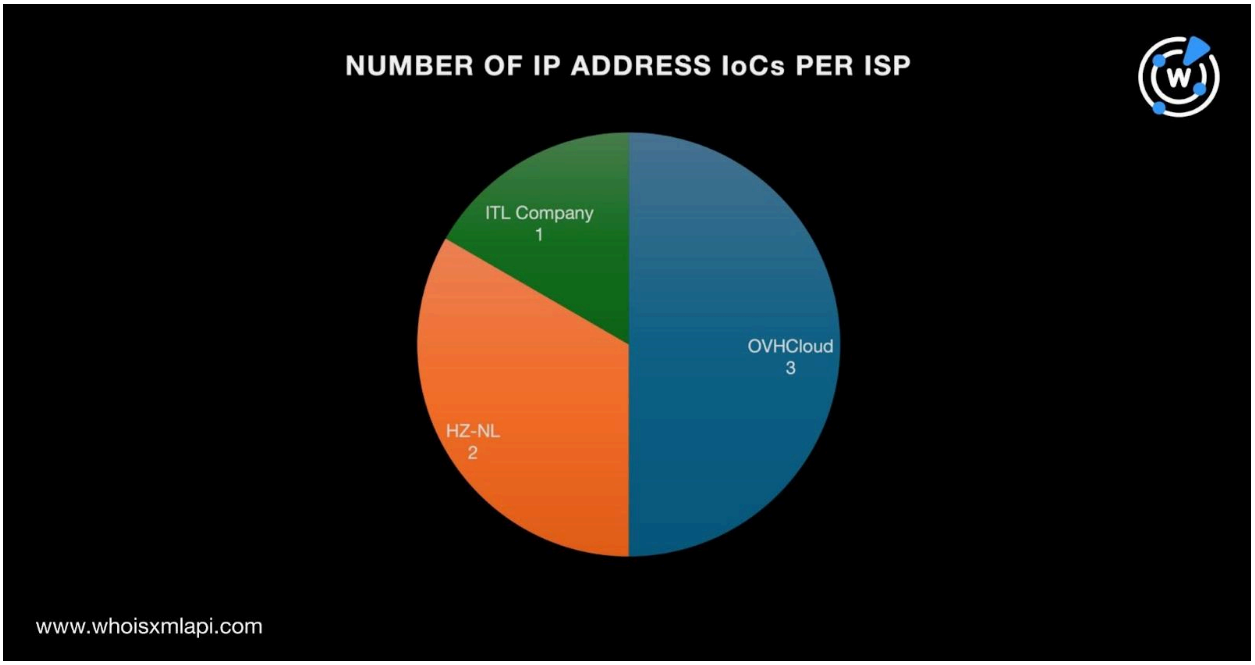
NOTE: Two domains did not have registrant countries in their current WHOIS records.

Next, we queried the six IP addresses identified as IoCs on Bulk IP Geolocation Lookup and discovered that:

- They were spread across three geolocation countries led by Poland, which accounted for three IP address IoCs. Two IP address IoCs were geolocated in the Netherlands and one in Sweden. Only the Netherlands appeared in both the lists of registrant and geolocation countries.



- OVHCloud was the top ISP with three IP address IoCs, followed by HZ-NL with two. ITL Company accounted for the last IP address IoC.



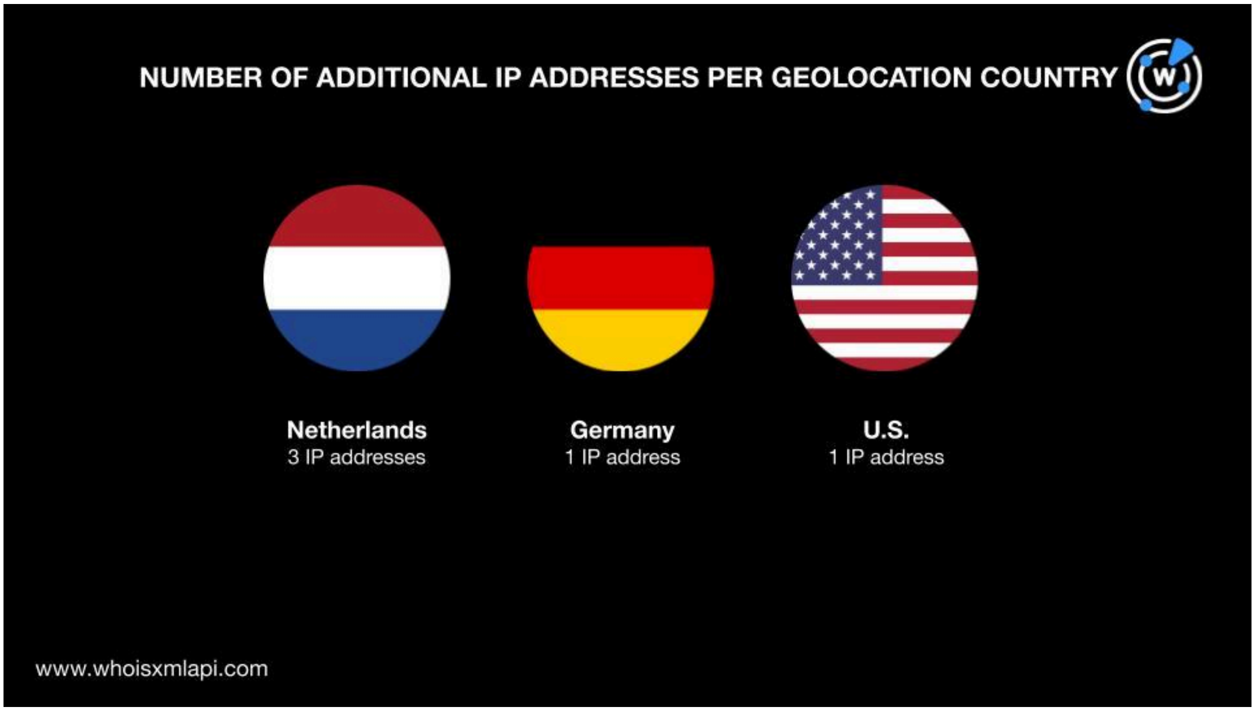
IoC List Expansion Findings

We started our hunt for connected threat artifacts with WHOIS History API queries for the 16 domains identified as IoCs. That led to the discovery of 30 email addresses in their historical WHOIS records. Eight of them were public email addresses that we then used as search terms for Reverse WHOIS API. Our queries allowed us to unearth 302 email-connected domains after filtering out duplicates and the IoCs.

Next, we performed DNS lookups for the 16 domains tagged as IoCs, which revealed that eight didn't have active IP resolutions. The remaining eight had corresponding IP addresses. They resolved to five IP addresses after duplicates and the IoCs were removed. Threat intelligence lookups for the five additional IP addresses showed that two were associated with various threats. The IP address 69[.]162[.]95[.]2, for instance, was associated with attacks, command-and-control (C&C), generic threats, malware distribution, phishing, and suspicious campaigns.

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

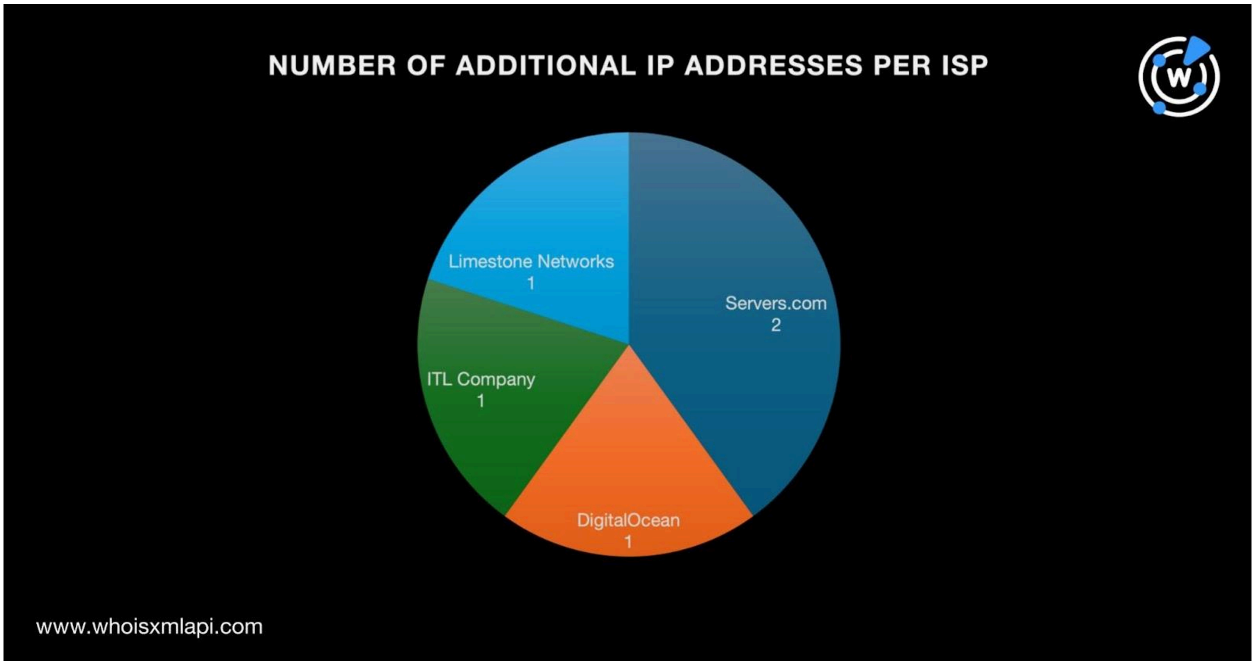
- They were spread across three geolocation countries topped by the Netherlands with three of the additional IP addresses. Germany and the U.S. accounted for one IP address each. The Netherlands appeared as a geolocation country akin to some of the IP address IoCs.



NUMBER OF ADDITIONAL IP ADDRESSES PER GEOLOCATION COUNTRY

www.whoisxmlapi.com

- Servers.com was the top ISP, accounting for two of the additional IP addresses. DigitalOcean, ITL Company, and Limestone Networks accounted for one each. Note that ITL Company also administered one of the ISPs of the IP address IoCs.



NUMBER OF ADDITIONAL IP ADDRESSES PER ISP

www.whoisxmlapi.com

Combining the six IP addresses identified as IoCs earlier and the five additional ones we uncovered, we had 11 IP addresses in all to further analyze. We performed reverse IP lookups for the 11 IP addresses and found out that three didn't host any domains at present. Seven of the remaining IP addresses could be dedicated hosts, while one was shared. The lookups allowed us to gather eight IP-connected domains after duplicates, the IoCs, and the email-connected domains were filtered out.

One of the IP-connected domains—jetselect[.]xyz—turned out to be associated with malware distribution based on the results of our Threat Intelligence API queries.

To cover all the bases, we performed Domains & Subdomains Discovery searches for the following text strings that appeared in the 16 domains tagged as IoCs but we only found results for 10 of them, namely:

- **amzuu.**
- **atswe.**
- **crypto-change.**
- **cryptonomiconf.**
- **jetengine.**
- **onetwofire.**
- **poolpush.**
- **sandbahn.**
- **swe.**
- **thild.**

Note that we used the parameters **Domains only**, **Added since 1 January 2017** (since the oldest domain IoC was created in 2017), and **Starts with**. We found 326 string-connected domains after removing duplicates, the IoCs, and the email- and IP-connected domains.

One of the string-connected domains—jetengine[.]be—turned out to be associated with malware distribution.

It's interesting to note that the IoC jetengine[.]it, the IP-connected domain jetselect[.]xyz, and the string-connected domain jetengine[.]be all had the string **jet**.

—

Our IoC expansion analysis for Konfety led to the discovery of 641 possibly connected artifacts comprising 302 email-connected domains, five additional IP addresses, eight IP-connected domains, and 326 string-connected domains. It also revealed that at least four of these web properties—two IP addresses and two domains—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

- 12305[.]com[.]cn
- 17107[.]xyz
- 17702[.]xyz
- 17707[.]xyz
- 32207[.]xyz
- 37720[.]xyz
- absence55[.]com
- absent65[.]com
- academic75[.]com
- activities7[.]com
- ad[.]ac[.]cn
- admission94[.]com
- admissions85[.]com
- ai[.]ac[.]cn
- ajisaisanba[.]com
- allspicee[.]net
- alumni65[.]com
- antitrust8[.]com
- arasukaaaa[.]info
- arpa[.]cn
- assault104[.]com
- assembly54[.]com
- assignm2ent[.]com
- attend67[.]com
- autocrat4[.]com
- baconr[.]net
- baseproduct[.]xyz
- basill[.]net
- batter1y[.]com
- bayleafe[.]net
- bestestofyoutube[.]com
- bh[.]ac[.]cn
- bh[.]gx[.]cn
- bh[.]net[.]cn
- bh[.]org[.]cn
- bh3d[.]cn
- bhg[.]js[.]cn
- bhg[.]org[.]cn
- bhzp[.]com[.]cn
- binhai[.]com[.]cn
- biology654[.]com
- bluemondays[.]xyz
- bodily98[.]com
- bolognal[.]net
- bonitoz[.]net
- bouillonz[.]net
- breasty[.]net
- buttere[.]net
- ca[.]ac[.]cn
- cannedw[.]net

Sample Additional IP Addresses

- 207[.]154[.]200[.]7
- 217[.]12[.]201[.]190

- 23[.]109[.]79[.]44

Sample IP-Connected Domains

- bestgiganews[.]com
- first[.]app-mainconfig[.]com
- getsearchit[.]com
- jetselect[.]xyz

Sample String-Connected Domains

- amzuu[.]cn
- amzuu[.]shop
- amzuu[.]top
- atswe[.]com
- atswe[.]science
- atswe[.]wang
- crypto-change[.]cc
- crypto-change[.]ch
- crypto-change[.]club
- cryptonomiconf[.]com
- jetengine[.]ai
- jetengine[.]app
- jetengine[.]be
- onetwofire[.]music
- poolpush[.]com
- poolpush[.]men
- sandbahn[.]de
- swe[.]ac
- swe[.]ac[.]th
- swe[.]academy
- thild[.]co
- thild[.]com
- thild[.]de