Following the DNS Trail of APT Group Newbie Unfading Sea Haze

Table of Contents

Executive Report

A new advanced persistent threat (APT) group dubbed “Unfading Sea Haze” has been trailing its sights on various organizations based in countries surrounding the South China Sea. As it turns out, the group has been active since at least 2018 and targeted eight known victims, mostly military and government entities, in support of Chinese interests so far.

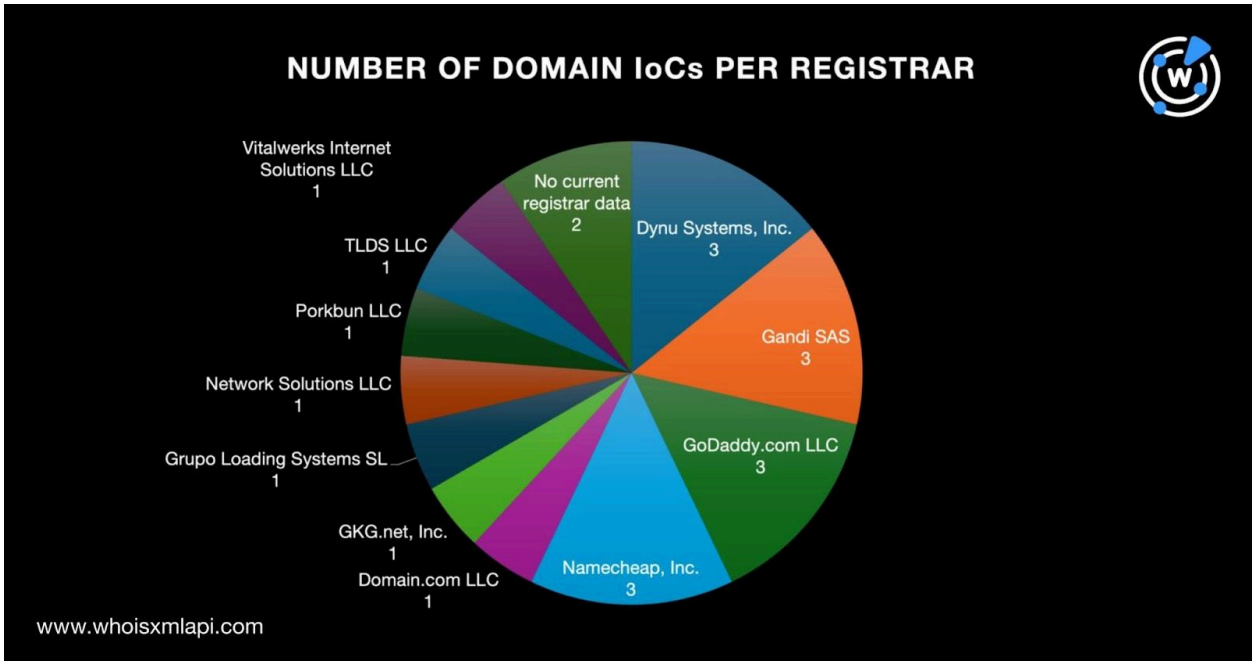
Bitdefender Labs published a list of indicators of compromise (IoCs) related to this attack. The WhoisXML API research team expanded the list comprising 21 domain names (some of which were extracted from subdomains) and 13 IP addresses and uncovered:

- 758 email-connected domains, one of which turned out to be malicious
- 16 additional IP addresses, 11 of which were associated with threats
- 272 IP-connected domains, 73 of which turned out to be malicious
- 253 string-connected domains

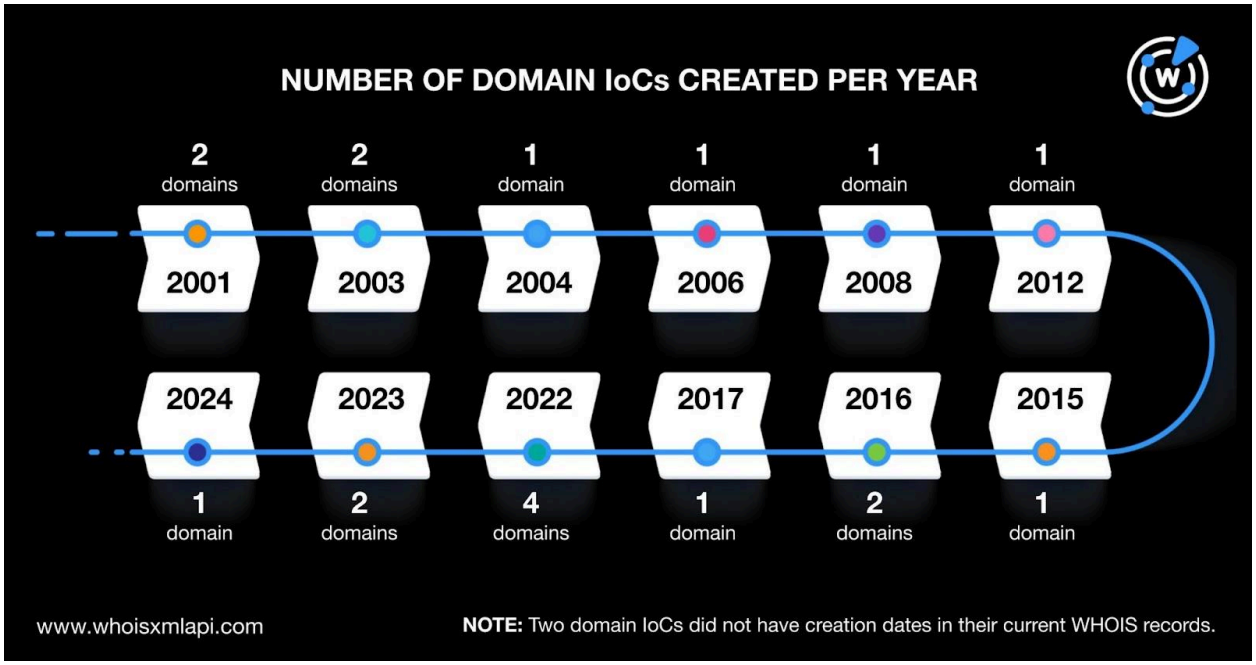
More on the Unfading Sea Haze IoCs

We began our in-depth analysis by subjecting the 21 domains identified as IoCs to a bulk WHOIS lookup, which revealed that:

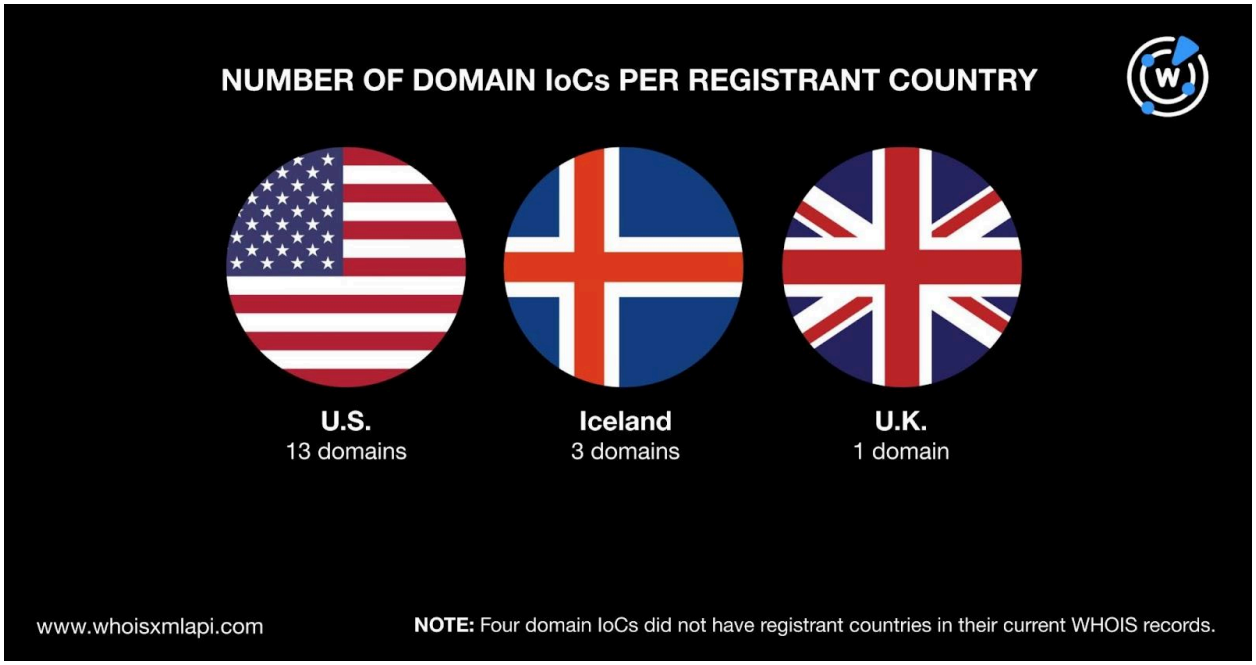
- The domain IoCs were spread across 11 registrars topped by Dynu Systems, Inc.; Gandi SAS; GoDaddy.com LLC; and Namecheap, Inc., which accounted for three domains each. Domain.com LLC; GKG.net, Inc.; Grupo Loading Systems SL; Network Solutions LLC; Porkbun LLC; TLDS LLC; and Vitalwerks Internet Solutions LLC, meanwhile, accounted for one domain IoC each. Finally, two domain IoCs did not have registrars in their current WHOIS records.



- Unfading Sea Haze did not discriminate in terms of domain age, using old and new alike. They were created between 2001 and 2024. Specifically, four domain IoCs were created in 2022; two each in 2001, 2003, 2016, and 2023; and one each in 2004, 2006, 2008, 2012, 2015, 2017, and 2024.

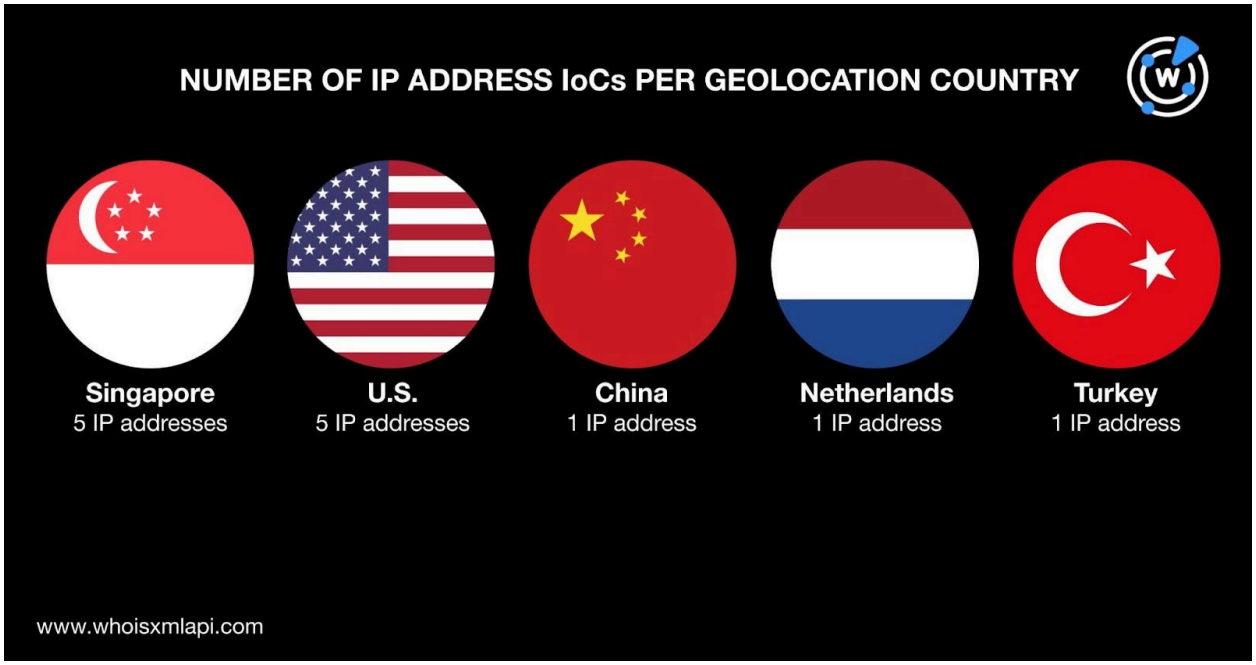


- The U.S. topped the list of registrant countries, accounting for 13 of the domain IoCs. Iceland took the second spot with three domains. One domain IoC was registered in the U.K. Four domains, however, did not have registrant countries in their current WHOIS records.

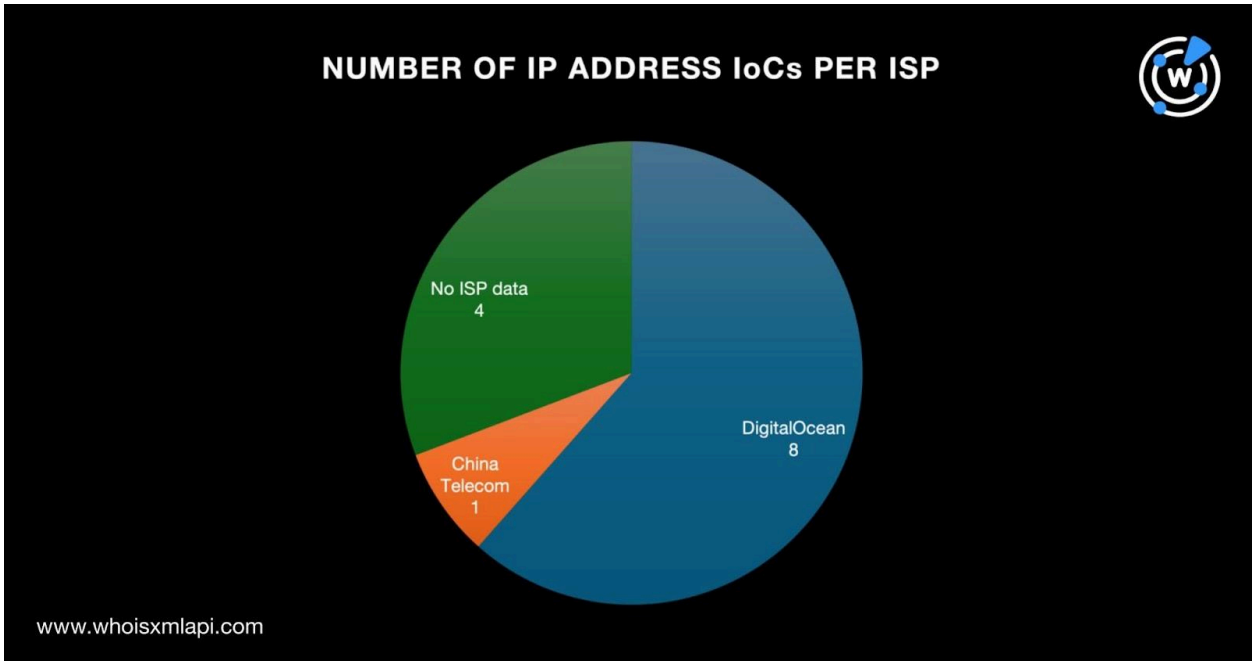


A [bulk IP geolocation lookup] for the 13 IP addresses tagged as IoCs showed that:

- The IP address IoCs originated from five countries led by Singapore and the U.S., which accounted for five IP addresses each. One IP address IoC each was geolocated in China, the Netherlands, and Turkey.



- DigitalOcean led the pack of ISPs, accounting for eight of the IP address IoCs. One IP address was administered by China Telecom. Finally, four of the IoCs did not have ISPs in their A records.



Scouring the DNS for More Signs of Unfading Sea Haze

After finding out more about the current list of Unfading Sea Haze IoCs, we sought to look for more potentially connected artifacts.

We started with WHOIS History API queries for the 21 domains identified as IoCs that uncovered 127 email addresses in their historical WHOIS records. Twenty-six of the email addresses were public.

Reverse WHOIS API queries for the 26 public email addresses led to the discovery of 758 email-connected domains after filtering out duplicates and the IoCs. Threat Intelligence Lookup found that one of the email-connected domains—zolafoxtrot[.]com—was associated with malware distribution.

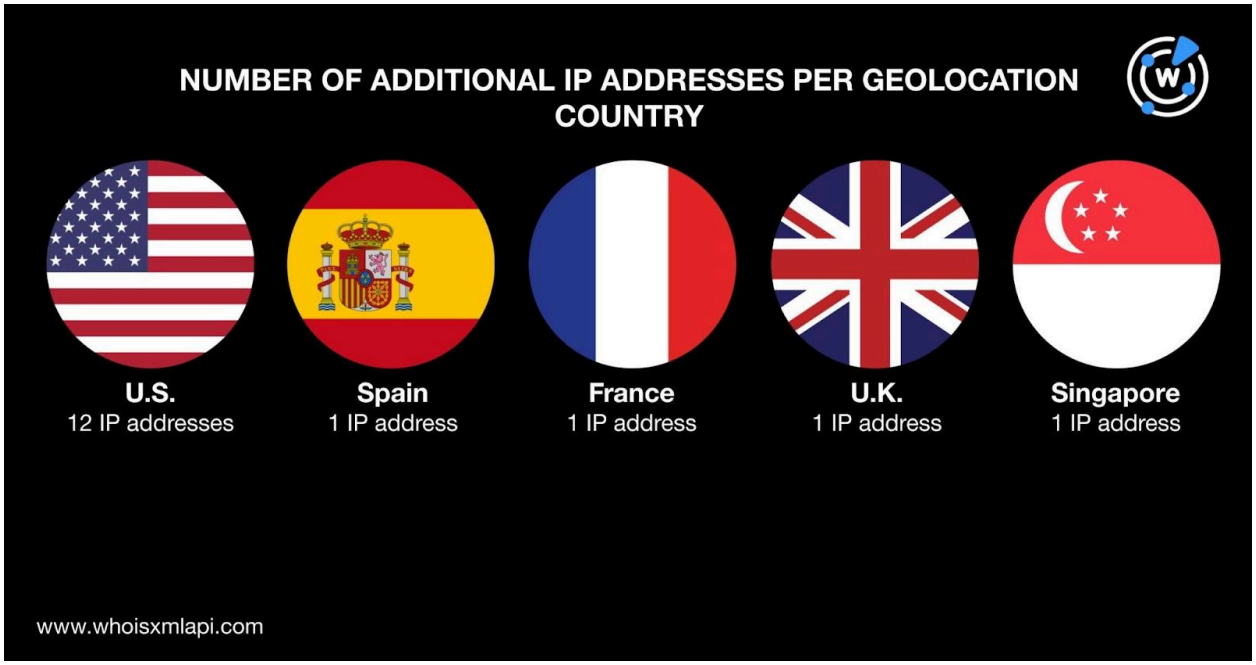
Next, we subjected the 21 domains tagged as IoCs to DNS lookups and found that 17 of them had active IP resolutions. They resolved to 16 IP addresses after we removed the duplicates and IoCs. Threat Intelligence Lookup revealed 11 of the additional IP addresses were associated with various threats. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
199[.]59[.]243[.]225	Attack Command and control (C&C) Generic Malware Phishing Spam Suspicious
3[.]33[.]130[.]190	Attack C&C Generic Malware Phishing Spam Suspicious
15[.]197[.]148[.]33	Attack C&C Generic Malware Phishing

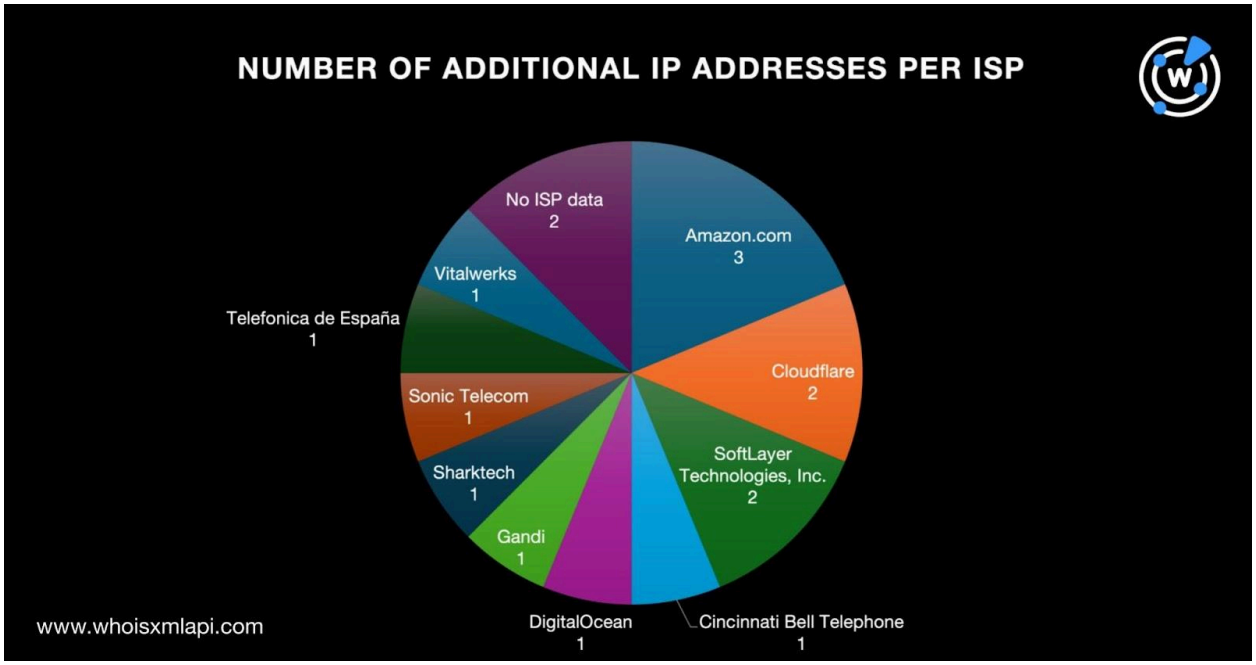
217[.]70[.]184[.]38	Attack C&C Malware Phishing
162[.]216[.]242[.]208	Generic Malware Phishing

A bulk IP geolocation lookup for the 16 additional IP addresses showed that:

- They were spread across five geolocation countries led by the U.S., which accounted for 12 of the additional IP addresses. One IP address each was geolocated in Spain, France, the U.K., and Singapore. Note that 13 additional IP addresses shared the geolocation countries of 10 IP address IoCs.



- Amazon.com topped the list of ISPs, accounting for three of the additional IP addresses. Cloudflare and SoftLayer Technologies, Inc. took the second spot with two IP addresses each. One IP address each was administered by Cincinnati Bell Telephone, DigitalOcean, Gandi, Sharktech, Sonic Telecom, Telefonica de España, and Vitalwerks. Finally, two of the additional IP addresses did not have ISPs on record.



Reverse IP lookups for the 29 IP addresses—13 IoCs and 16 additional IP addresses—revealed that 11 could be dedicated hosts. Altogether, they hosted 272 domains after duplicates, the IoCs, and the email-connected domains were filtered out. Threat Intelligence Lookup showed that 73 of the IP-connected domains were associated with generic threats.

Next, we searched for domains that started with the 20 unique text strings found among the 21 domains tagged as IoCs. Only 14 of the strings, however, appeared in 253 other domains after the IoCs and email- and IP-connected domains were taken out, namely:

- **adswt.**
- **blinklab.**
- **d-n-s.**
- **emldn.**
- **fxnxs.**
- **g8z.**
- **giize.**
- **hifiliving.**
- **kozow.**
- **mywire.**
- **ooguy.**
- **redirectme.**
- **simpletra.**
- **twilightparadox.**

It is also interesting to note that the APT group could be cybersquatting on the Bitdefender brand as evidenced by two domain IoCs containing the company's name. While the WHOIS record details of the security provider's legitimate domain bitdefender[.]com have been masked, the IoCs—bitdefenderupdate[.]com and bitdefenderupdate[.]org—may not belong to Bitdefender. For one thing, both domain IoCs were newly created as opposed to bitdefender[.]com, which was created years ago. Also, the legitimate domain was registered in

Cyprus while bitdefenderupdate[.]org was registered in the U.S. The domain IoC bitdefenderupdate[.]com did not have a registrant country in its WHOIS record.

—

Our DNS deep dive into the Unfading Sea Haze attack by expanding a published list of IoCs comprising 21 domain names and 13 IP addresses led to the discovery of 1,299 possibly connected threat artifacts. Among them were 85 digital properties that have already been weaponized for 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

- 0086hdw[.]com
- 0163[.]cm
- 02488[.]org
- 0736px[.]com
- 114pww[.]com
- 11746[.]org
- 161661666[.]com
- 17768[.]net
- 17taowei[.]com
- 1cho[.]net
- 2077[.]co[.]kr
- 2997777[.]net
- 2someplace[.]com
- 3368998[.]com
- 34588[.]info
- 365-bet[.]cm
- 365sweater[.]com
- 4888861[.]com
- 5189999[.]net
- 52bucun[.]com
- 565bet365[.]com
- 583222[.]net
- 6444444[.]net
- 67872[.]org
- 6868[.]com[.]cn
- 6968[.]com[.]cn
- 7287878[.]com
- 7893132[.]com
- 819918[.]org
- 85551[.]info
- 868789[.]info
- 88520[.]info
- 8855888888[.]com
- 886lg[.]com

- 8o4[.]net
- 96637[.]org
- 971122[.]net
- 9888959[.]com
- 999833[.]net
- 9b0[.]net
- abbysaccents[.]net
- actioninbox[.]bid
- actionshop[.]bid
- acyx[.]org
- adasjourney[.]com
- adressenews[.]com
- afreestyleshop[.]com
- aglorei[.]com
- aifa[.]cm
- aifocus[.]us
- aiyuhan[.]com
- alabonne[.]date
- alba02[.]com
- alba03[.]com
- allinclunet[.]com
- allmygoodloan[.]com
- alloinfodeal[.]com
- alloinfoshop[.]com
- allopromodeal[.]com
- allorc[.]com
- alotmorepromo[.]com
- animallnetwork[.]org
- annexeinfo[.]com
- arnaud[.]bid
- arnaud01[.]com
- arnaud02[.]com
- arnaud03[.]com
- arnaud04[.]com
- arnaudhayder[.]com
- arttigcam[.]com
- assopopoliss[.]com
- axadle[.]org
- axcomputerservices[.]com
- b17wingsoffreedom[.]com
- backbpas[.]org
- baeddaeki[.]com
- bargainweb[.]pro
- barquagaming[.]com
- bbin-bbs[.]top
- beiping[.]science
- beiru[.]bid
- benoitanastay[.]com
- bestdeliv[.]info
- bet-365[.]cm
- bhdx168[.]com
- bigdaddysbigd[.]us
- bigyo[.]kr
- bigyo[.]net
- bitcoincash1st[.]com
- bizpromoinfo[.]com
- bjbdjt[.]com
- bjbvw[.]com
- bjtcdw[.]com
- bjtfrc[.]xn--vuq861b
- bjyflcny[.]com
- bl[.]pe[.]kr
- blinklabdigital[.]xyz
- blogchain[.]kr
- bobbynet[.]us
- bobobulu[.]com

Sample Additional IP Addresses

- 104[.]21[.]5[.]227
- 15[.]197[.]148[.]33
- 158[.]247[.]7[.]206
- 162[.]216[.]242[.]208
- 167[.]99[.]76[.]75
- 169[.]47[.]130[.]72
- 169[.]47[.]130[.]85
- 172[.]67[.]133[.]240

- 192[.]184[.]140[.]47

Sample IP-Connected Domains

- 3utilities[.]com
- 9lives[.]ar
- 9lives[.]com[.]ar
- 9livesdelicias[.]com[.]ar
- acarte[.]cloud
- access[.]ly
- adegi[.]me
- aminomax[.]ar
- aminomax[.]com[.]ar
- angelcamddns[.]com
- apollorlando[.]com
- apr911[.]net
- bamatheatre[.]com
- belisa[.]rocks
- biztoe[.]com
- blogsyte[.]com
- blorks[.]com
- bounceme[.]net
- brasilia[.]me
- cable-modem[.]org
- cariamici[.]com[.]ar
- carnerodelmal[.]com
- caroamici[.]cl
- caroamici[.]com[.]ar
- carouselnoir[.]com
- casaruralanida[.]es
- catapult[.]ar
- catapult[.]com[.]ar
- catdevnull[.]org
- cglcontracting[.]com
- chandmani[.]com
- chatdi[.]vn
- cheffatass[.]com
- chickenkiller[.]com
- christsupremaci[.]st
- ciscofreak[.]com
- coffee[.]ac[.]kr
- collegefan[.]org
- couchpotatofries[.]org
- damnserver[.]com
- darkbazaar[.]com
- ddns[.]me
- ddns[.]net
- ddnsking[.]com
- der-stuermer[.]com
- desdeelvestidor[.]com
- destetеprecoz[.]com[.]ar
- ditchyourip[.]com
- djmacattack[.]com
- dnsfor[.]me

Sample Malicious IP-Connected Domains

- blogsyte[.]com
- bounceme[.]net
- brasilia[.]me
- cable-modem[.]org
- ciscofreak[.]com
- collegefan[.]org
- couchpotatofries[.]org
- damnserver[.]com
- ddns[.]me
- ddns[.]net
- ddnsking[.]com
- ditchyourip[.]com
- dnsfor[.]me
- dnsiskinky[.]com
- dvrcam[.]info
- dynns[.]com
- eating-organic[.]net
- fantasyleague[.]cc

- geekgalaxy[.]com

- geekgalaxy[.]com

Sample String-Connected Domains

- adswt[.]club
- adswt[.]info
- adswt[.]xyz
- blinklab[.]app
- blinklab[.]ca
- blinklab[.]cn
- blinklab[.]co
- blinklab[.]co[.]jp
- blinklab[.]co[.]kr
- blinklab[.]co[.]uk
- blinklab[.]com[.]br
- blinklab[.]de
- blinklab[.]eu
- blinklab[.]hk
- blinklab[.]info
- blinklab[.]insure
- blinklab[.]it
- blinklab[.]me
- blinklab[.]net
- blinklab[.]nl
- blinklab[.]org
- blinklab[.]ph
- blinklab[.]sg
- blinklab[.]ws
- blinklab[.]xyz

- d-n-s[.]at
- d-n-s[.]be
- d-n-s[.]biz
- d-n-s[.]ca
- d-n-s[.]ch
- d-n-s[.]cloud
- d-n-s[.]cn
- d-n-s[.]co
- d-n-s[.]co[.]jp
- d-n-s[.]co[.]uk
- d-n-s[.]co[.]za
- d-n-s[.]com
- d-n-s[.]com[.]cn
- d-n-s[.]com[.]ua
- d-n-s[.]de
- d-n-s[.]dk
- d-n-s[.]eu
- d-n-s[.]fr
- d-n-s[.]fun
- d-n-s[.]host
- d-n-s[.]hosting
- d-n-s[.]hu
- d-n-s[.]info
- d-n-s[.]ir
- d-n-s[.]it