Unearthing the DNS Roots of the Latest Lotus Blossom Attack

Table of Contents

Executive Report

Cisco Talos recently uncovered multiple Lotus Blossom cyber espionage campaigns targeting government, manufacturing, telecommunications, and media organizations. The group used Sagerunex and other hacking tools after compromising target networks.

The researchers believe Lotus Blossom developed new Sagerunex variants that used a combination of traditional command-and-control (C&C) servers and legitimate third-party cloud services like Dropbox, Twitter, and the Zimbra open-source webmail as C&C tunnels.

Cisco Talos identified several indicators of compromise (IoCs), including 10 domains and 28 IP addresses, which WhoisXML API expanded through a DNS deep dive. Our analysis led to the discovery of:

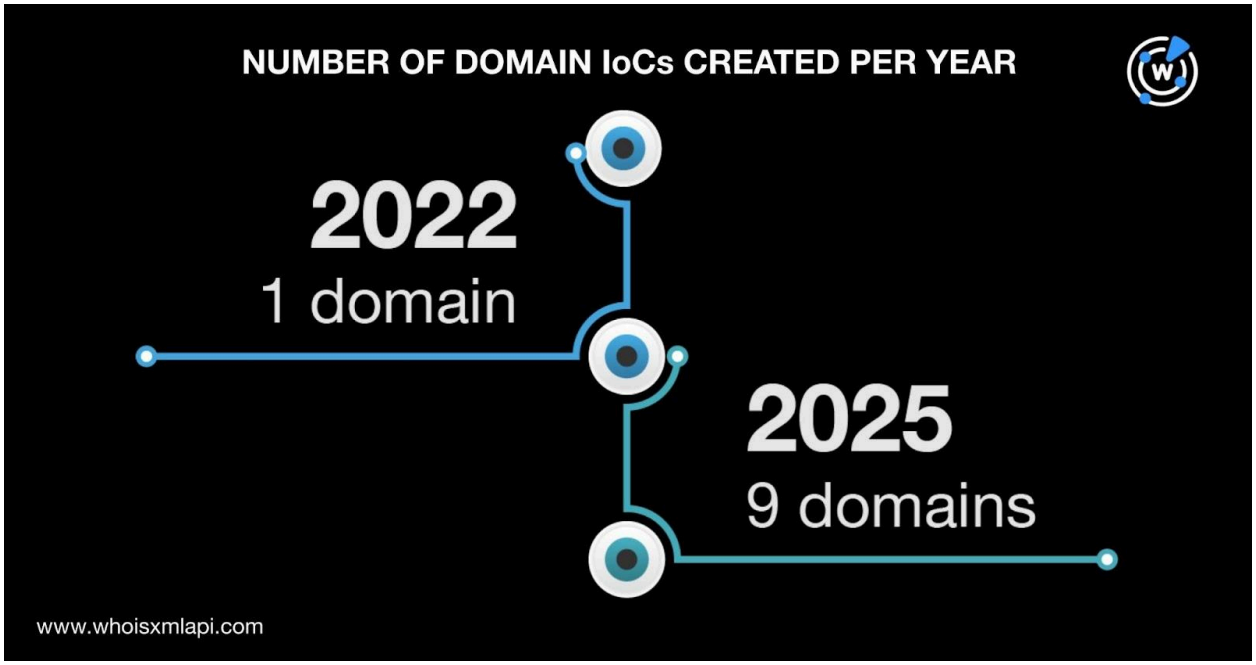
- 90 email-connected domains
- Four additional IP addresses, two of which turned out to be malicious
- 106 IP-connected domains, two of which have already been weaponized for attacks
- 12 string-connected domains

More on the Lotus Blossom Attack IoCs

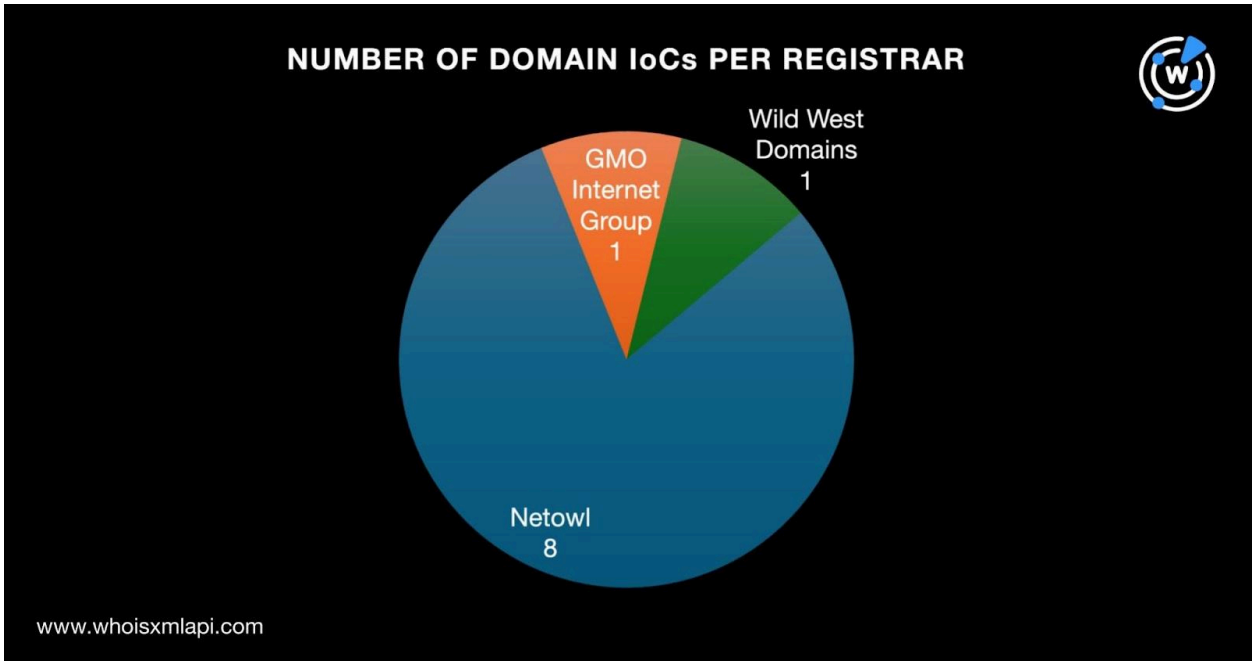
Before we dive into our IoC list expansion, we sought to find more information about the IoCs.

We began by querying the 10 domains identified as IoCs on Bulk WHOIS API and found that all of them had current WHOIS records.

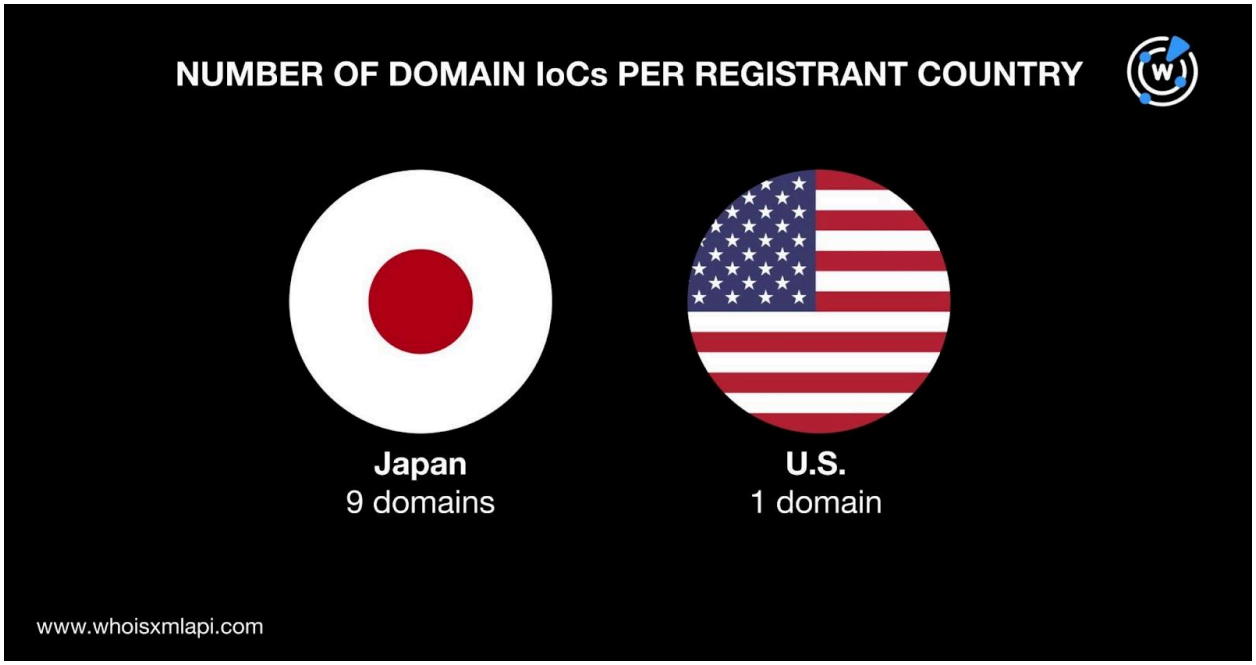
- They were created between 2022 and 2025. Specifically, one was created in 2022 and nine in 2025.



- They were split among three registrars led by Netowl, which administered eight domains. GMO Internet Group and Wild West Domains accounted for one domain each.



- They were registered in two countries topped by Japan, which accounted for nine domains. One domain was registered in the U.S.

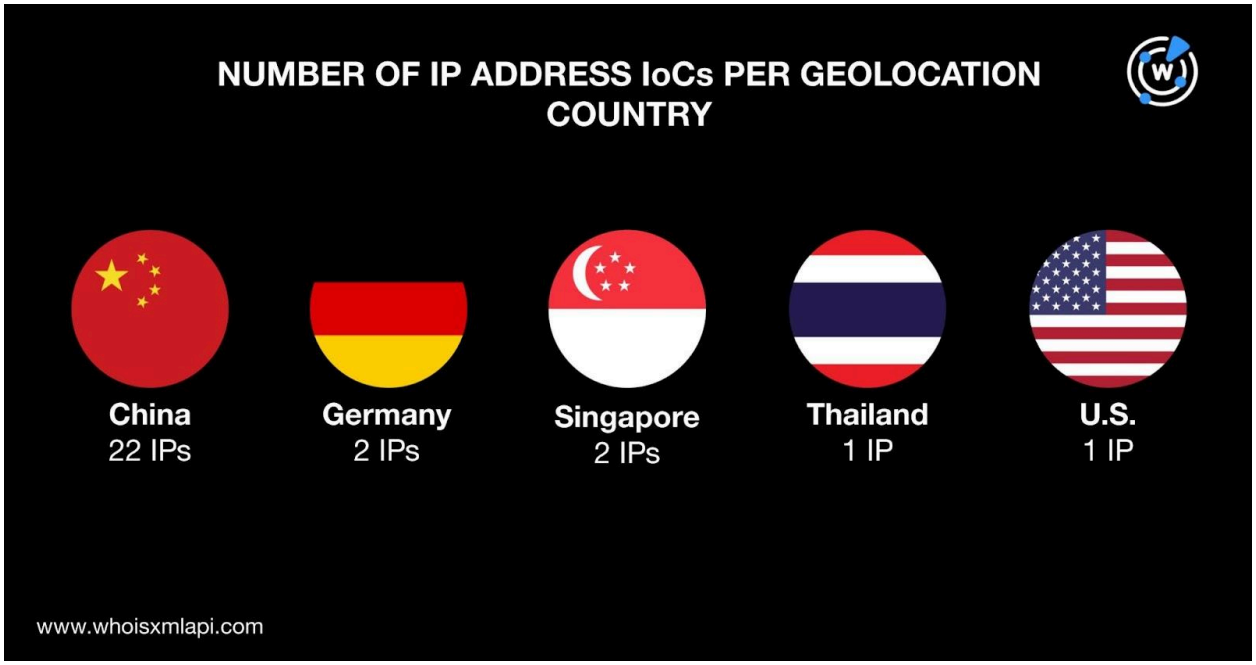


We also queried the 10 domains identified as IoCs on DNS Chronicle API and found that nine had 127 historical domain-to-IP resolutions. The domain doyourbestyet[.]com had five resolutions since 4 October 2019—the oldest resolution date among the IoCs. Interestingly, though, based on its current WHOIS record, it was created on 28 February 2025, which could mean it was recently reregistered. Take a look at detailed results for three other domains below.

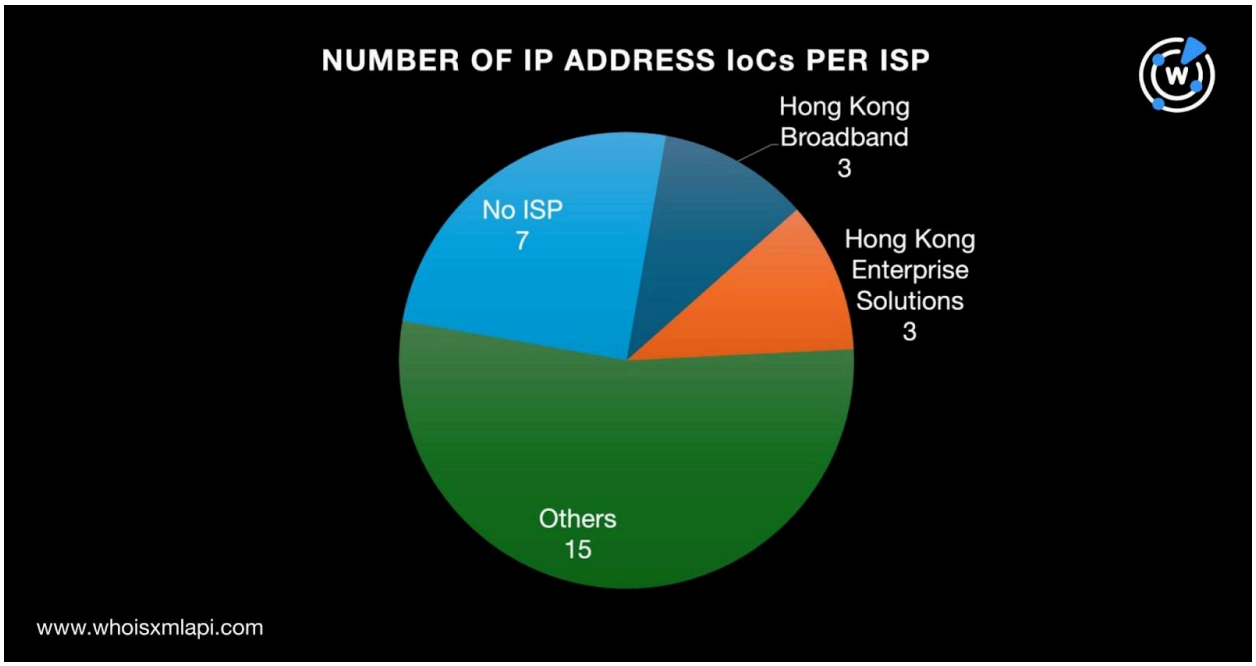
DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE
acdserv[.]com	86	18 February 2020
davoport[.]org	4	28 February 2025
sensor-data[.]online	1	8 March 2025

Next, we queried the 28 IP addresses identified as IoCs on Bulk IP Geolocation Lookup and found that:

- They were geolocated in five countries led by China, which accounted for 22 IP addresses. Two IP addresses each originated from Germany and Singapore. Finally, one IP address each was geolocated in Thailand and the U.S.



- Only 21 of them had ISPs on record. Hong Kong Broadband and Hong Kong Enterprise Solutions topped the list of ISPs with three IP addresses each. Cloudie, Dimension Network, Huawei Cloud, The Constant Company, and Zenlayer administered two IP addresses each. One IP address each was administered by DXTL, EDGENAP, KLAYER, Lucidacloud, and XNNET. Finally, seven IP addresses did not have ISP information.



We also queried the 28 IP addresses identified as IoCs on DNS Chronicle API and found that 16 had 778 historical IP-to-domain resolutions over time. The IP address 160[.]124[.]251[.]105 had 223 resolutions starting on 10 October 2019—the oldest resolution date among the IoCs. Take a look at detailed results for five other IP addresses below.

IP ADDRESS IoC	NUMBER OF DOMAIN RESOLUTIONS	FIRST RESOLUTION DATE
103[.]213[.]245[.]95	2	14 June 2024
103[.]74[.]192[.]105	16	26 November 2019
122[.]10[.]91[.]36	36	22 April 2020
43[.]252[.]161[.]22	162	17 August 2022
45[.]32[.]127[.]212	25	17 September 2021

On to the IoC List Expansion

To kick off our expansion analysis, we queried the 10 domains identified as IoCs on WHOIS History API and found that they all had email addresses in their historical WHOIS records. We uncovered 14 email addresses in all. Further scrutiny revealed that six were public email addresses.

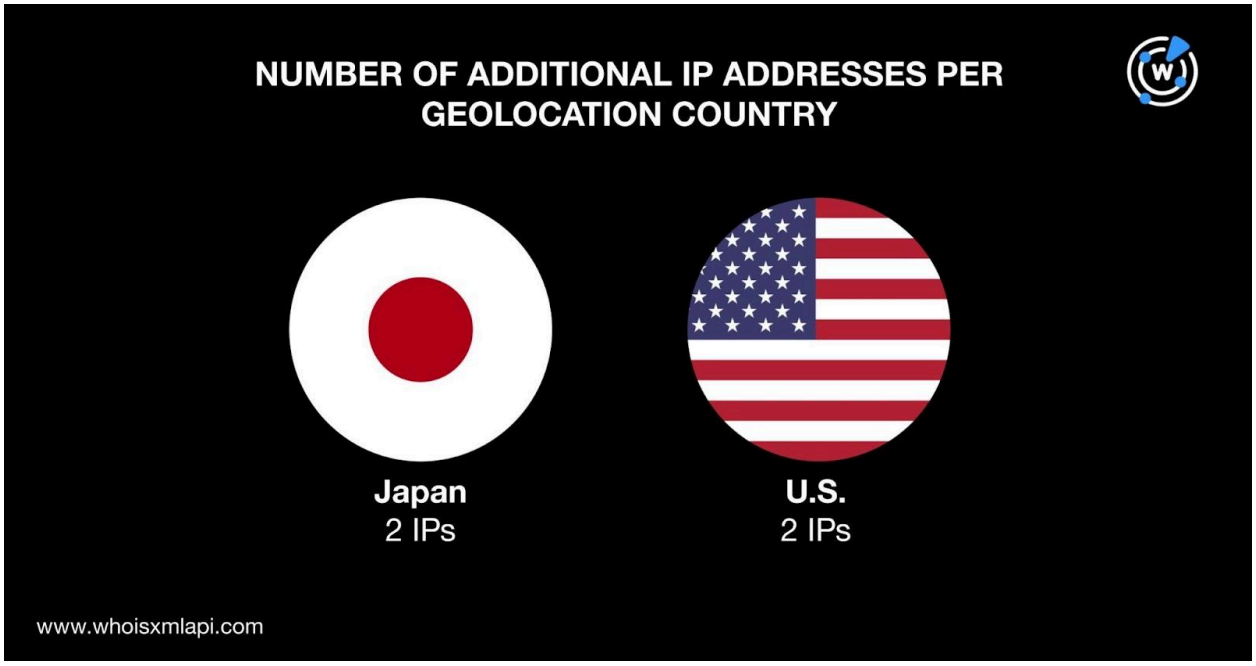
We queried the six public email addresses on Reverse WHOIS API and found that while none of them appeared in the current WHOIS records of other domains, all of them appeared in the historical WHOIS records of several. However, one domain could belong to a domainer. In sum, five public email addresses appeared in the current records of 90 domains after duplicates and those already identified as IoCs were filtered out.

Next, we queried the 10 domains identified as IoCs on DNS Lookup API and found that they resolved to four IP addresses after duplicates and those already tagged as IoCs were filtered out.

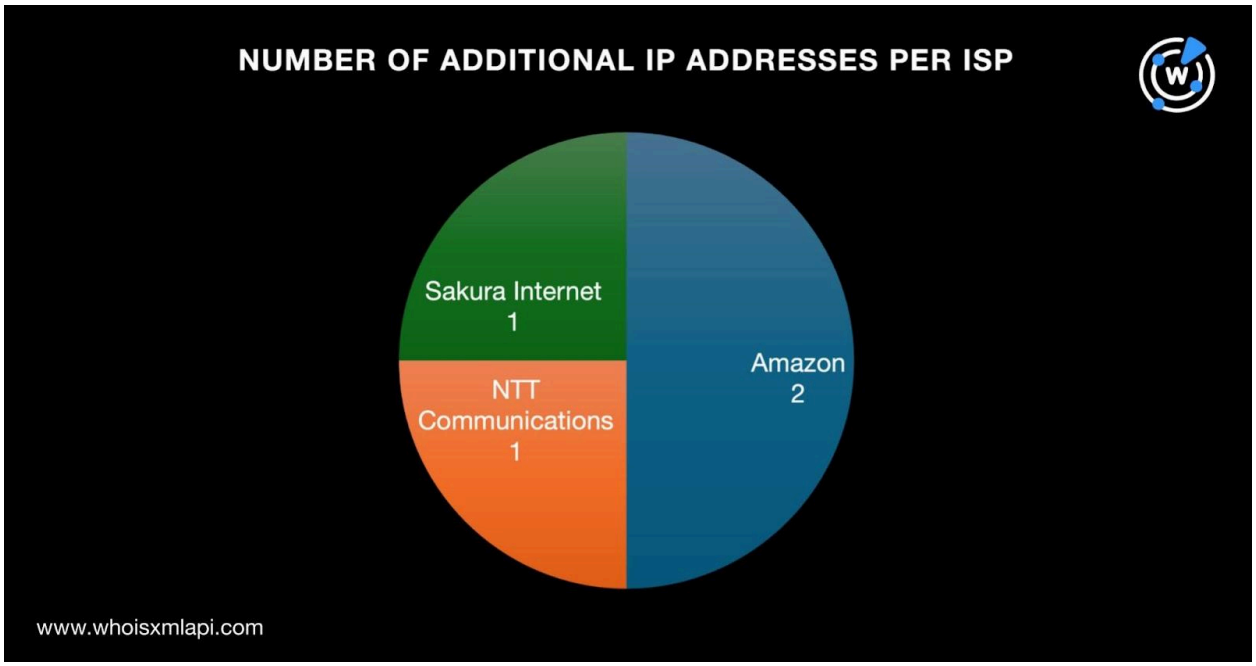
A Threat Intelligence API query for the four additional IP addresses showed that two have already been tagged as malicious. An example would be 160[.]16[.]200[.]77, which was associated with generic threats and malware distribution.

A Bulk IP Geolocation Lookup query for the four additional IP addresses, meanwhile, showed that:

- They were geolocated in two countries—two each in Japan and the U.S. These were consistent with the domain IoCs registrant countries.



- They were split among three ISPs led by Amazon, which administered two IP addresses. NTT Communications and Sakura Internet managed one IP address each.



Now, given the 28 IP addresses identified as IoCs and the four additional ones we uncovered, we had 32 IP addresses for further analysis. A Reverse IP API query for the 32 IP addresses showed that seven had current IP-to-domain resolutions. Further scrutiny of the seven IP addresses revealed that four could be dedicated hosts. Altogether, the four possibly dedicated IP addresses hosted 106 domains after duplicates, those already tagged as IoCs, and the email-connected domains were filtered out.

A Threat Intelligence API query for the 106 IP-connected domains showed that two have already been tagged as malicious. An example would be adv138mail[.]com, which was associated with malware distribution.

As the final step, we sought to uncover other domains that started with the same 10 unique text strings as the 10 domains identified as IoCs using Domains & Subdomains Discovery. We found connections for these three strings:

- cebucafe.
- davaotour.
- sensor-data.

Specifically, we unearthed 12 string-connected domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

—

Our DNS deep dive into the latest Lotus Blossom attack that leveraged Sagerunex and other hacking tools led to the discovery of 212 potentially connected artifacts. We specifically unearthed 90 email-connected domains, four additional IP addresses, 106 IP-connected domains, and 12 string-connected domains. Our findings also revealed that four of the artifacts—two domains and two IP addresses—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

- 78mpk[.]com
- 8080cpcp[.]com
- acerlaptopshop[.]com
- agustinpalace[.]org
- airforcessport[.]com
- baike[.]so
- betbetmania[.]com
- bly058[.]com
- cabucafe[.]com
- coosunglass[.]com
- dainstock[.]com
- djyle[.]com
- dke23[.]com
- eelectronicswhosale[.]com
- efrenperalta[.]org
- eoutdoorstores[.]com
- freegiftclubs[.]com
- frslshop[.]com
- gahlsh[.]com
- go851[.]com
- gold1114[.]com
- haobo16888[.]com
- hdpowertools[.]com
- hksunglass[.]com
- jctomys[.]com
- kax88[.]com
- lalalamusic[.]net
- lead-stock[.]com
- like-football[.]net
- marioking338[.]com
- marioking339[.]com
- marioking400[.]com
- nftopstores[.]com
- niceoutsports[.]com
- nikeshoe[.]tw
- ontomyshops[.]com
- philoea[.]org
- philtrace[.]net
- piccsunglass[.]com
- qqsunglass[.]com
- ray-stock[.]com
- rowerexpert[.]com
- roweronsale[.]com
- sabanb[.]com
- sae-bank[.]com
- saebank[.]com
- telegram-gram[.]com
- timezonecorp[.]com
- tomioutlet[.]com
- ubestmallss[.]com
- uclasicshop[.]com
- uclasicstore[.]com
- vovworld[.]org
- wanxi[.]mobi
- ws727[.]com
- xinhaopingbiqi[.]net
- xn--h9ja5g311ltda457ae4zjmfcqbh60btwyjf5cg7r[.]com
- yaddal2[.]tv
- yk1004[.]com
- ziondoor[.]com

Sample Additional IP Addresses

- 100[.]24[.]208[.]97
- 35[.]172[.]94[.]1

Sample IP-Connected Domains

- a[.]sinkhole[.]yourtrap[.]com
- adv138mail[.]com
- angry-mendel[.]103-213-245-95[.]plesk[.]page
- beidouqc[.]net
- btblt[.]com
- cpanel[.]adv138mail[.]com
- cpanel[.]faxzfwxgwlxrey[.]com
- cpanel[.]gfhzsgcqyve[.]com
- faxzfwxgwlxrey[.]com
- ftp[.]adv138mail[.]com
- ftp[.]faxzfwxgwlxrey[.]com
- gfhzsgcqyve[.]com
- localhost[.]adv138mail[.]com
- localhost[.]faxzfwxgwlxrey[.]com
- localhost[.]gfhzsgcqyve[.]com
- mail[.]adv138mail[.]com
- mail[.]faxzfwxgwlxrey[.]com
- mail[.]gfhzsgcqyve[.]com
- ouyicc[.]cc
- pop[.]adv138mail[.]com
- pop[.]faxzfwxgwlxrey[.]com
- pop[.]gfhzsgcqyve[.]com
- sinkhole[.]dynu[.]net
- smtp[.]adv138mail[.]com
- smtp[.]faxzfwxgwlxrey[.]com
- tifunckvmnzsz[.]com
- tkkbk[.]com
- tkztgl[.]cn
- unblvasxecfc[.]com
- webdisk[.]adv138mail[.]com
- webdisk[.]faxzfwxgwlxrey[.]com
- webdisk[.]gfhzsgcqyve[.]com
- yszr[.]cn

Sample String-Connected Domains

- cebucafe[.]com
- cebucafe[.]xyz
- davaotour[.]com
- sensor-data[.]cloud
- sensor-data[.]com
- sensor-data[.]de