A DNS Deep Dive into the LabHost PhaaS Infrastructure

Table of Contents

Executive Report

The Federal Bureau of Investigation (FBI) shared a warning on 29 April 2025 about the LabHost phishing-as-a-service (PhaaS) campaign that threatened the security of users worldwide, along with a massive list of related indicators of compromise (IoCs). WhoisXML API embarked on an in-depth analysis of the IoCs through a DNS deep dive.

The FBI, in particular, identified 42,515 LabHost PhaaS campaign IoCs. We analyzed 42,401 after excluding duplicates and non-domain entries. To these, we added 1,661 net new typosquatting domains akin to the IoCs on the FBI list. Our investigation of the joint list of 44,062 domains led to these findings and enrichments:

- 18 well-known brands appearing in the net new typosquatting domains, all of which were also found on the FBI list
- 11,009 unique client IP addresses querying 163 domains through a total of 74,617 DNS requests based on Internet Abuse Signal Collective (IASC) DNS traffic data
- 3,319 domains in First Watch Malicious Domains Data Feed with creation dates averaging 419 days prior to the FBI warning date
- 61,727 subdomains with common strings including **www**, **mail**, **webmail**, **cpanel**, **webdisk**, and **smtp**
- 1,346 unique IP resolutions of the 44,062 domains, 1,055 of which were malicious

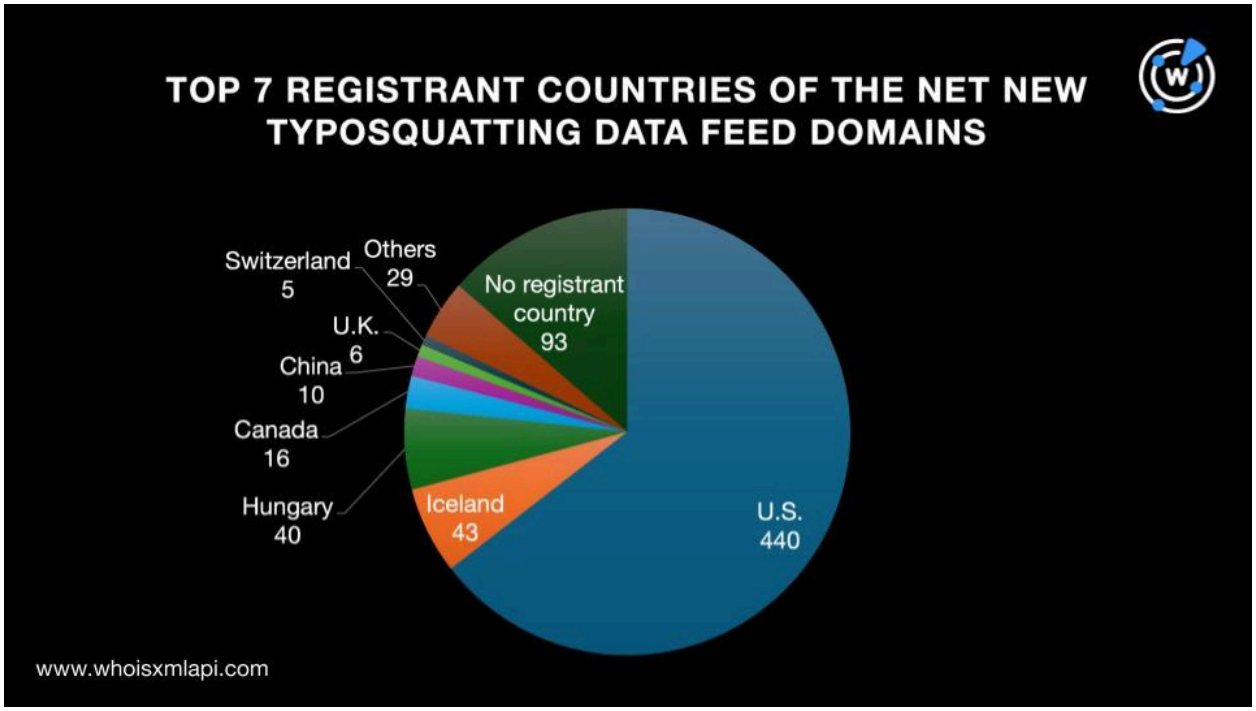
DNS Investigation of the LabHost PhaaS Campaign IoCs

As our first step, we cleaned up the FBI list and were left with 42,401 domains identified as IoCs after excluding duplicates, IP addresses, and non-domains. Then we used our list of domains culled from the FBI list as an input to query all our Typosquatting Data Feed files and found an additional 1,661 connected domains, bringing the total number of domains to 44,062.

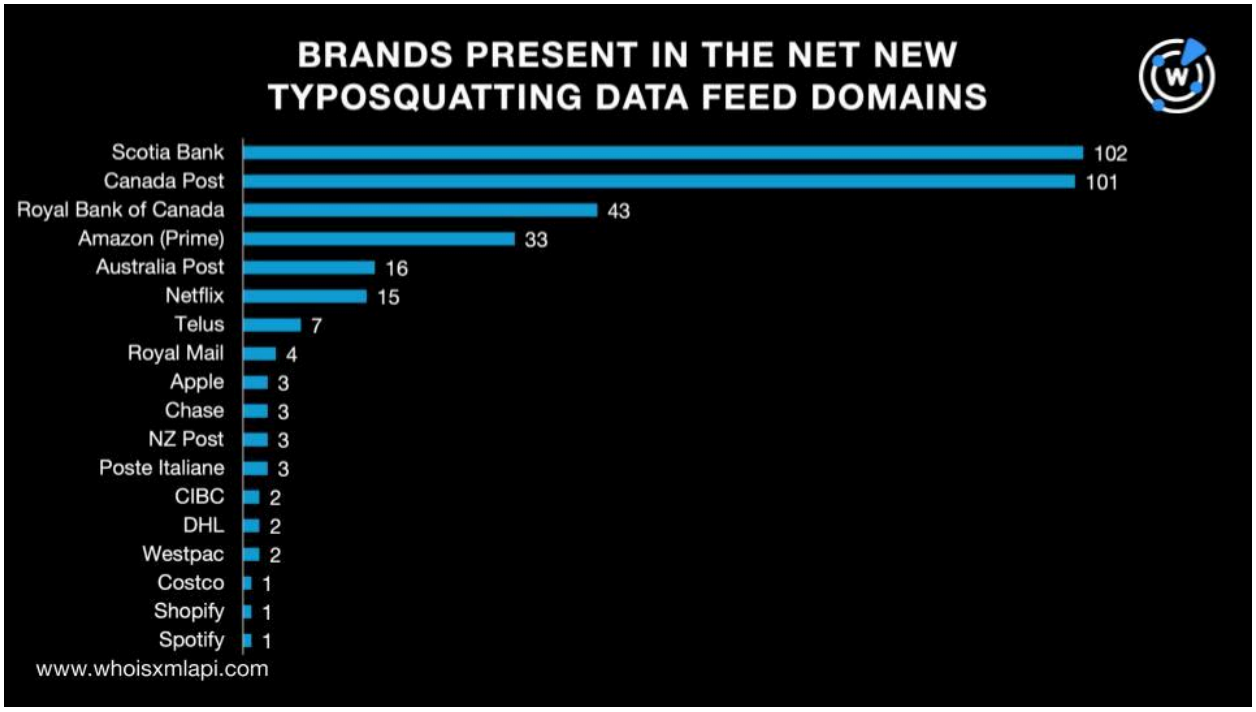
Next, we queried the 1,661 typosquatting domains on Bulk WHOIS API and found that 682 of them had current WHOIS records based on creation dates. The domains were created between 2012 and 2025. Specifically, one domain each was created in 2012 and 2022, 81 in 2023, 458 in 2024, and 141 in 2025.

While three of the 682 domains did not have registrar information on record, the remaining 679 were split among 62 registrars. Dynadot, NameSilo, Porkbun, Namecheap, Domain Science, GoDaddy, Spaceship, Gname.com, PDR, and Tucows comprised the top 10 registrars.

And while 93 of the 682 domains did not have registrant countries on record, the remaining 589 were registered in 27 countries. The U.S., Iceland, Hungary, Canada, China, the U.K., and Switzerland comprised the top 7 registrant countries.



A closer look at the 682 domains revealed that 342 of them contained text strings pertaining to 18 well-known brands even if some were misspelled. The 18 brands possibly being mimicked were Scotia Bank, Canada Post, Royal Bank of Canada, Amazon (including Amazon Prime), Australia Post, Netflix, Telus, Royal Mail, Apple, Chase, NZ Post, Poste Italiane, CIBC, DHL, Westpac, Costco, Shopify, and Spotify. Interestingly, all these brands also appear in the original FBI list.

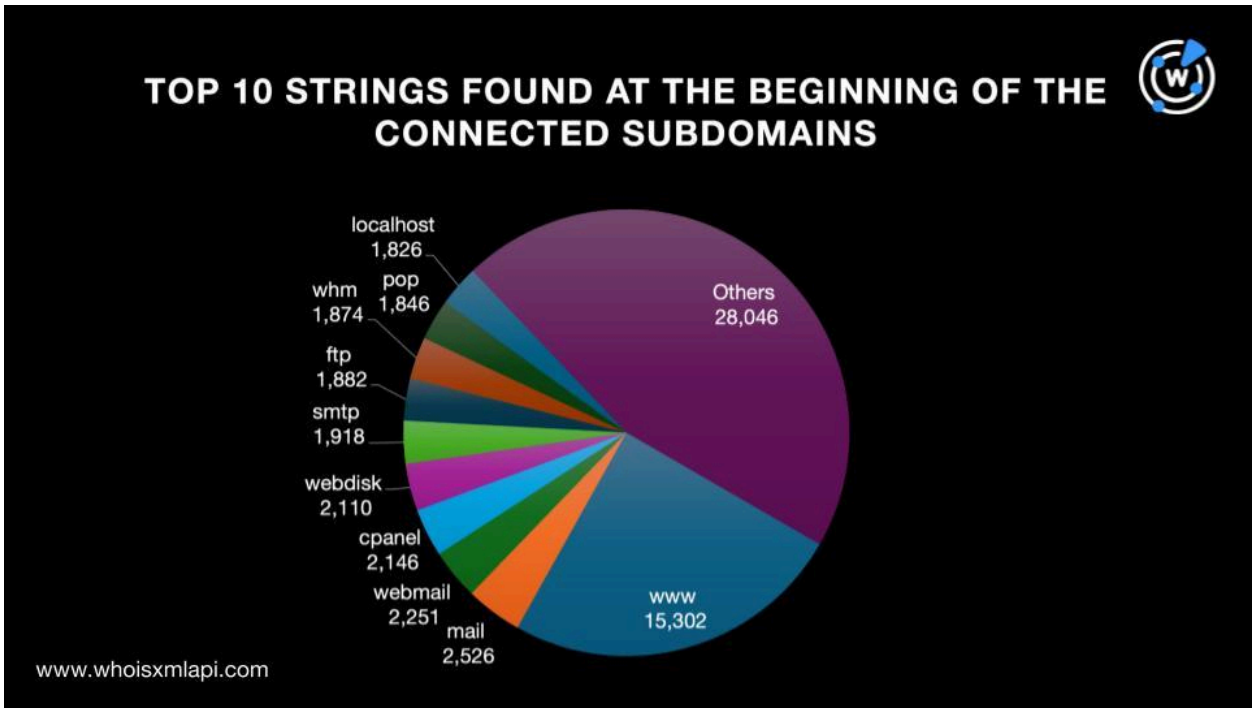


Using sample DNS traffic data our researchers obtained from the IASC, we further analyzed the 44,062 domains. The sample data revealed that 11,009 unique client IP addresses queried 163 distinct domains between 8 April and 9 May 2025, through a total of 74,617 DNS requests.

We then checked the 44,062 domains against First Watch Malicious Domains Data Feed and found that 3,320 were listed. Notably, 3,319 of these domains had creation dates prior to the FBI's warning date. Specifically, their creation dates ranged up to 813 days before the alert was released with an average lead time of 419 days.

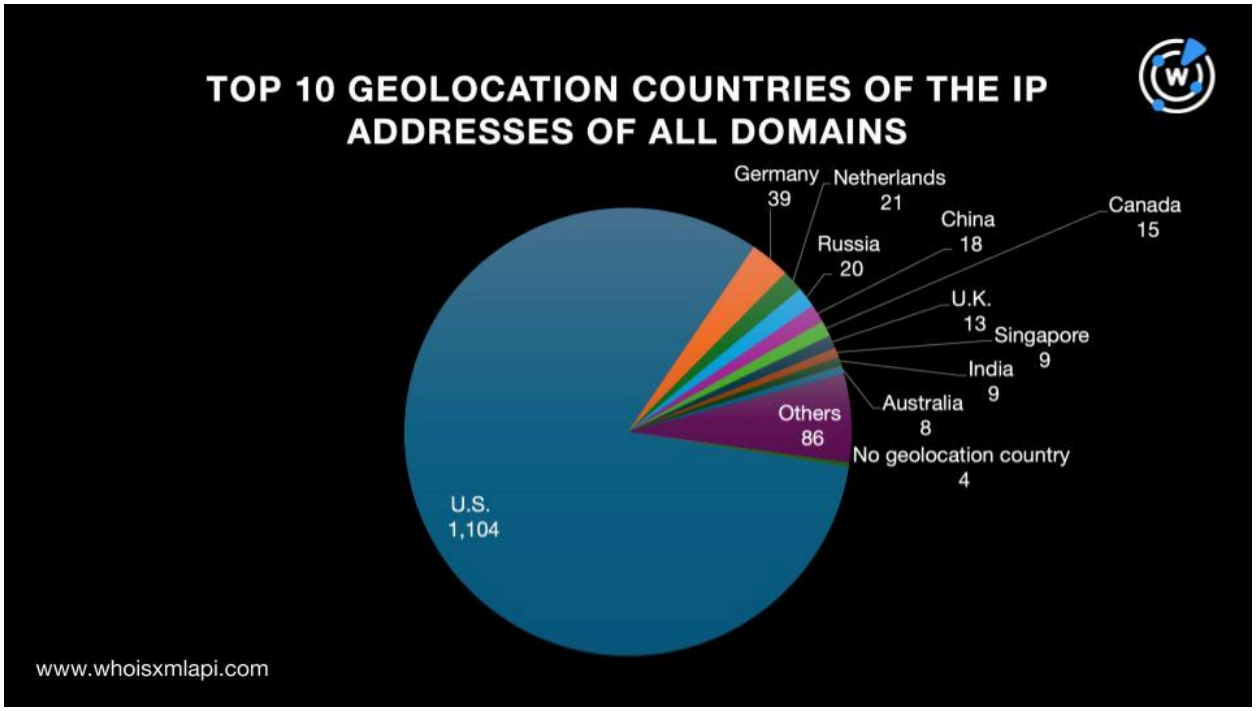
Interestingly, the FBI also reported creation dates for the 42,515 LabHost PhaaS campaign domain IoCs as part of their warning, allowing for a comparison between the FBI's reported dates and those recorded by First Watch. While many of the FBI's dates overlapped with those from First Watch, notable divergences emerged. In fact, First Watch more frequently reported earlier creation dates than the FBI, suggesting possible differences in data sources.

We also queried Subdomains Lookup API and discovered that out of the 44,062 domains, only a minority had a total of 61,727 retrievable subdomains. We further scrutinized the 13,239 unique last-level subdomain values (i.e., leftmost text strings) determined that **www**, **mail**, **webmail**, **cpanel**, **webdisk**, **smtp**, **ftp**, **whm**, **pop**, and **localhost** comprised the top 10.

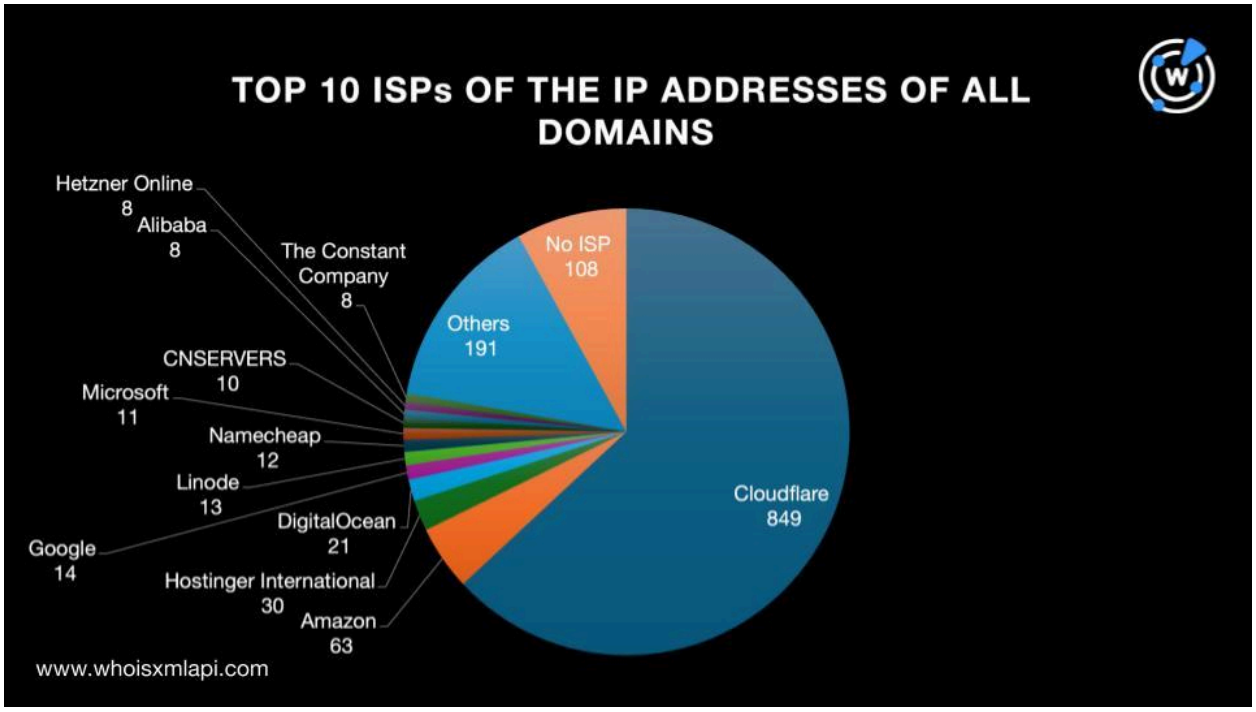


Next, we queried the 44,062 domains from the FBI list and the net new typosquatting domains on DNS Lookup API and found that 1,371 of them had 3,541 active IP resolutions. After filtering out duplicates, we were left with 1,346 unique IP addresses. Also, while 879 were IPv4 addresses, the remaining 467 were IPv6 addresses.

A Bulk IP Geolocation Lookup query for the 1,346 IP addresses, meanwhile, showed that they were split into 41 geolocation countries topped by the U.S., Germany, the Netherlands, Russia, China, Canada, the U.K., Singapore, India, and Australia. Four had no geolocation countries on record.



While 1,238 of the 1,346 IP addresses were administered by 116 ISPs. Note that 108 did not have ISPs on record. The top 10 ISPs were Cloudflare in first place; Amazon in second; Hostinger International in third; DigitalOcean in fourth; Google in fifth; Linode in sixth; Namecheap in seventh; Microsoft in eighth; CNSERVERS in ninth; and Alibaba, Hetzner Online, and The Constant Company in tenth.



Finally, a Threat Intelligence API query for the 1,346 IP addresses revealed that 1,055 of them have already been weaponized for various cyber attacks. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
103[.]224[.]182[.]208	Malware distribution Suspicious activity Phishing Generic threat Attack
20[.]69[.]178[.]82	Malware distribution Attack
2001[:]8d8[:]100f[:]f000[::]200	Malware distribution Phishing Generic threat Suspicious activity C&C
3[.]214[.]92[.]112	Phishing Malware distribution Generic threat Suspicious activity Phishing

	Attack
43[.]246[.]145[.]242	Generic threat

Summing Up Our Findings

Our in-depth DNS investigation into the LabHost PhaaS campaign by analyzing the 42,401 domains the FBI identified as IoCs, enriched by 1,661 net new typosquatting domains akin to the IoCs on the FBI list, allowed us to identify these findings:

- 342 of the net new typosquatting domains contained 18 well-known brand names, all of which also appeared on the FBI list
- 11,009 unique client IP addresses queried 163 domains based on IASC DNS traffic data
- 3,319 domains in First Watch Malicious Domains Data Feed with creation dates averaging 419 days prior to the FBI warning date
- 61,727 subdomains with common strings including **www**, **mail**, **webmail**, **cpanel**, **webdisk**, and **smtp**
- 1,346 unique IP resolutions of the 44,062 domains, 1,055 of which were malicious

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 New New Typosquatting Domains

- 1transfer[.]store
- 21transfer[.]com
- 2sign-in[.]com
- a-express[.]pics
- aca-post[.]icu
- aca-post[.]online
- bacverified[.]com
- bacverified[.]net
- badaconsulting[.]net
- ca-gst-return[.]com
- cad-etran3940[.]live
- cad-gst-return[.]com
- dabet[.]academy
- dabet[.]accountant
- dabet[.]accountants
- e-alerts[.]live
- e-alerts[.]xyz
- e-flow-toll[.]cloud
- fabet[.]academy
- fabet[.]accountant
- fabet[.]accountants
- g7insurance[.]com
- gccinsurance[.]org
- gccinsurance[.]xyz
- hctransfer[.]com
- hdtransfers[.]pk
- heattransfer[.]net[.]au
- inflationbcab[.]info
- info-rbc2[.]com
- inpostoffice[.]bar
- jbexpress[.]es
- jetzt-bestatigen[.]org
- jetzt-bestatigen[.]xyz
- k-transfer[.]ru
- k-transfer[.]store
- kalttransfer[.]eu
- labexpress[.]online
- leetransfer[.]com
- legalconsulting[.]co
- mactransfers[.]es
- mactransfers[.]eu
- manage-profile[.]click
- nel-fiix-help[.]homes
- nel-fiix-help[.]online
- netbank[.]digital
- onlineabc[.]online
- onlineabc[.]site
- op-mobili-fi-io-in[.]com
- parcel-customs[.]eu
- parcel-customs[.]info
- payback-refunds[.]com
- qc-rbcroyalbank3[.]com
- qc-rbcroyalbank4[.]com
- qc-rbcroyalbank6[.]com
- rbcroyalsecurity[.]info
- reada-consulting[.]co[.]uk
- real-consulting[.]org
- s-oneconsulting[.]com
- sc-logistics[.]com
- scbonline-reset-help[.]space
- td-mobile-secured[.]com
- td-mobile1secured[.]com
- tel1us-int1erac[.]online
- ul-logistics[.]com
- untransfer[.]cl
- update-account01[.]com
- v-logistics[.]co
- veridiance[.]org
- verification-rbc1[.]com
- w-ld[.]cyou
- w-ld[.]one
- w-ld[.]xyz

- xn--obile-el1b[.]com
- xn--scotiahnk-676d[.]com
- xn--scotiaknk-676d[.]com

Sample Subdomains of the Domains on the FBI List

- 0-apastylecentral[.]apa[.]org[.]library[.]newdomain[.]com
- 0-c-involved[.]r[.]t[.]netflixx[.]info
- 0-checkpoint[.]riag[.]com[.]umiss[.]lib[.]newdomain[.]com
- a--m[.]newdomain[.]com
- a-dw12[.]playgami[.]adev[.]netflixx[.]info
- a-h-mirtalebipour[.]newdomain[.]com
- b[.]a1ds14[.]netflixx[.]info
- b[.]i76-hptsdopl-scat[.]netflixx[.]info
- b[.]netflixx[.]info
- c-n7k-n04-01[.]rz[.]interacet[.]com
- c[.]mx[.]e[.]netflixx[.]info
- c[.]rbs-supportdigital[.]com
- d[.]onlineupdatecibcunlock[.]xyz
- d[.]p90juio[.]xyz
- d[.]pay-coniq[.]xyz
- emails[.]netflixx[.]info
- emailverificationapi[.]netflixx[.]info
- emannueloc[.]newdomain[.]com
- f40bc86d-ca67-4ae6-9ee9-d9d1466feb1b[.]fabet[.]broker
- f4d960a7-07d0-4efd-b47c-47af26cac309[.]random[.]authsecuredcraportal[.]com
- f4d960a7-07d0-4efd-b47c-47af26cac309[.]random[.]e-transf[.]online
- gdnuymvr[.]atb-login[.]com
- gdv[.]newdomain[.]com
- gdysr[.]reg-gq[.]com
- hideiphideip[.]1e[.]apicpoc-dev[.]aws[.]canadapost-postescanada[.]ca
- hidemyass[.]newdomain[.]com
- hifzstaging[.]newdomain[.]com
- icodesgs-master[.]coop[.]sddc[.]newdomain[.]com
- icomzapp[.]debet[.]vision
- ics-001[.]pplsira[.]cair[.]web994[.]netflixx[.]info
- j5sqgrocb20asau13wqyzym8n[.]optimalpaymanagement[.]info
- j60[.]newdomain[.]com
- j61[.]cceng[.]netflixx[.]info
- kayakaddon[.]netflixx[.]info
- kayakalipmetal[.]netflixx[.]info
- kayakalpnaturopathy[.]netflixx[.]info
- laksa19[.]netflixx[.]info
- lalafo[.]paym[.]one
- lallardesantos[.]newdomain[.]com
- m[.]boa24-7onl1ne[.]com
- m[.]ca-express-delivery[.]com
- m[.]ca-express-support[.]com
- natursekt[.]newdomain[.]com
- naushad[.]newdomain[.]com
- nauticajavierberga[.]newdomain[.]com
- office[.]authorize-securedeposit[.]info
- office[.]clientcardsupport[.]info
- office[.]crapay[.]com
- pay[.]pay[.]pay[.]kwid9[.]et-interac-ca-telus-refund-ca72g72h[.]xyz
- pay[.]pay[.]pay[.]kwid9[.]et1-interc-transfer-wireless[.]xyz
- pay[.]pay[.]sber[.]cdek[.]pochta[.]fedex-global-assistance-id80002837[.]com
- qa[.]ci[.]dabet[.]supplies

- qa[.]ci[.]debet[.]actor
- qa[.]ci[.]debet[.]builders
- r13[.]communications[.]canadapost-postescanada[.]ca
- r14[.]notifications[.]canadapost-postescanada[.]ca
- r171[.]notifications[.]canadapost-postescanada[.]ca
- sandbox[.]clientcardsecure[.]com
- sandbox[.]dabet[.]actor
- sandbox[.]dabet[.]coupons
- teleport[.]pre[.]netflixx[.]info
- teller-template[.]newdomain[.]com
- telus-mobility[.]interact[.]gold
- uat[.]policycheck[.]newdomain[.]com
- uat[.]superset[.]exclusivememberships[.]club
- uat[.]superset[.]w9bet[.]click
- venurakahawala[.]newdomain[.]com
- venwstu[.]getconsulting[.]org
- ver[.]book-itnow[.]com
- web[.]fabet[.]support
- web[.]fabet[.]systems
- web[.]joinredeliveryonlineca[.]info
- xn--p39ap6b0zcnvrrxcrri[.]comssl[.]crapay[.]com
- xn--wtqs2dm0o[.]newdomain[.]com
- xn1wp[.]crtcinfoadmingroup[.]info
- yahoo-beauties[.]netflixx[.]info
- yahoo-broadcast[.]netflixx[.]info
- yahoo-cell[.]netflixx[.]info
- zveayjw[.]reg-gq[.]com
- zvtglgzpzyv[.]transfer-return[.]com
- zw[.]netflixx[.]info

Sample IP Addresses Corresponding to the Domains on the FBI List

- 138[.]124[.]184[.]14
- 20[.]69[.]157[.]201
- 38[.]180[.]8[.]122
- 149[.]248[.]19[.]20
- 91[.]195[.]240[.]12
- 216[.]245[.]197[.]41
- 52[.]223[.]13[.]41
- 0[.]0[.]0[.]0
- 103[.]224[.]212[.]200
- 172[.]247[.]173[.]173
- 172[.]247[.]173[.]148
- 172[.]247[.]173[.]141
- 172[.]247[.]173[.]204
- 172[.]247[.]173[.]165
- 8[.]218[.]242[.]28
- 15[.]197[.]172[.]60
- 104[.]21[.]16[.]16
- 172[.]67[.]209[.]197
- 2606:4700:3033::ac43:d1c5
- 2606:4700:3036::6815:1010
- 20[.]211[.]64[.]19
- 74[.]119[.]193[.]118
- 74[.]119[.]239[.]234
- 173[.]223[.]234[.]61