Tracking Down Fake Cryptocurrency Sellers Using DNS Intelligence

Table of Contents

Executive Report

Threat researcher Dancho Danchev recently uncovered 130 domains that seemingly belong to fake cryptocurrency sellers. The WhoisXML API research team sought to find potential connections to the threat by expanding the current list of indicators of compromise (IoCs) using our vast array of DNS intelligence sources.

Our in-depth investigation led to the discovery of:

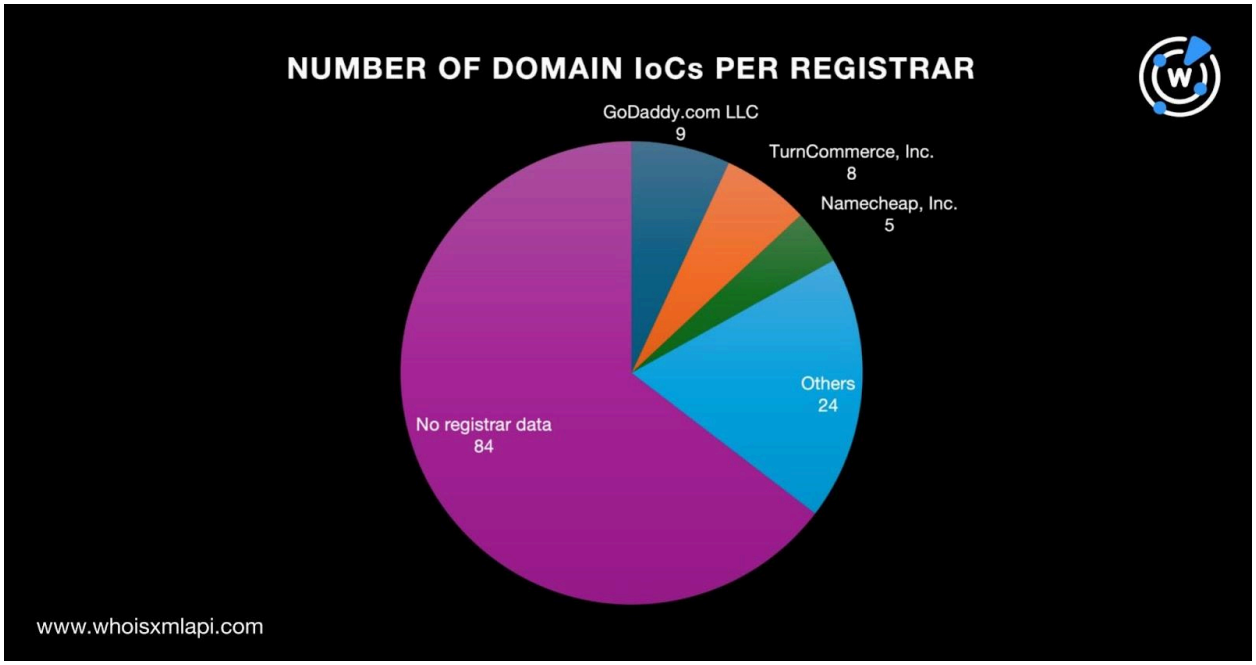
- 522 email-connected domains, 21 of which turned out to be malicious
- 41 IP addresses, 39 of which turned out to be associated with various threats
- 259 IP-connected domains
- 1,947 string-connected domains, 15 of which are already tagged as malicious

More IoC Facts

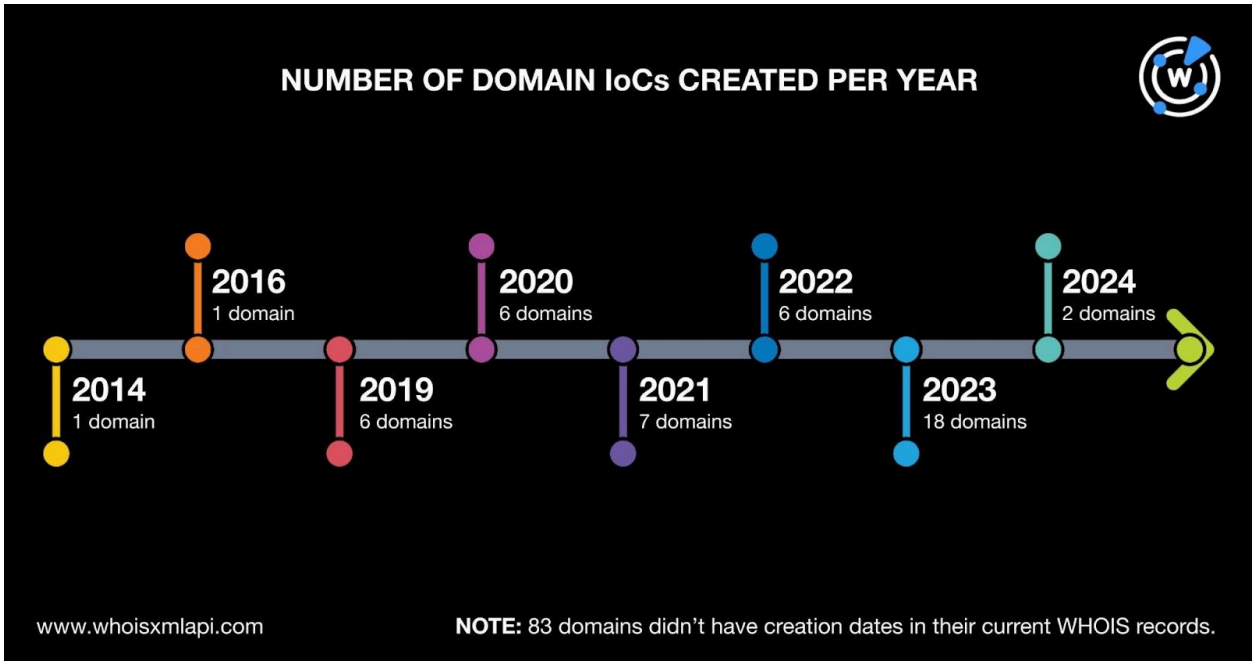
To learn more about the 130 domain names tagged as IoCs, we performed a bulk WHOIS lookup, which revealed that:

- The domain IoCs were distributed among 22 registrars led by GoDaddy.com LLC, which accounted for nine domains. TurnCommerce, Inc. took the second spot with eight domain IoCs. In third place was Namecheap, Inc. with five domain IoCs. Two IoCs each were administered by DropCatch.com LLC, Dynadot LLC, Key-Systems GmbH, NameSilo LLC, and PDR Ltd. Alibaba Cloud Computing Ltd.; Amazon Registrar, Inc.; Automattic, Inc.; CommuniGal Communication Ltd.; CSL Computer Service Langenbach GmbH; Hostinger Operations UAB; http.net Internet GmbH; Name.com, Inc.; Namebeacon.com, Inc.; Network Solutions LLC; REGRU-RU; Sav.com LLC; Squarespace Domains LLC; and World4You Internet Services GmbH accounted for one

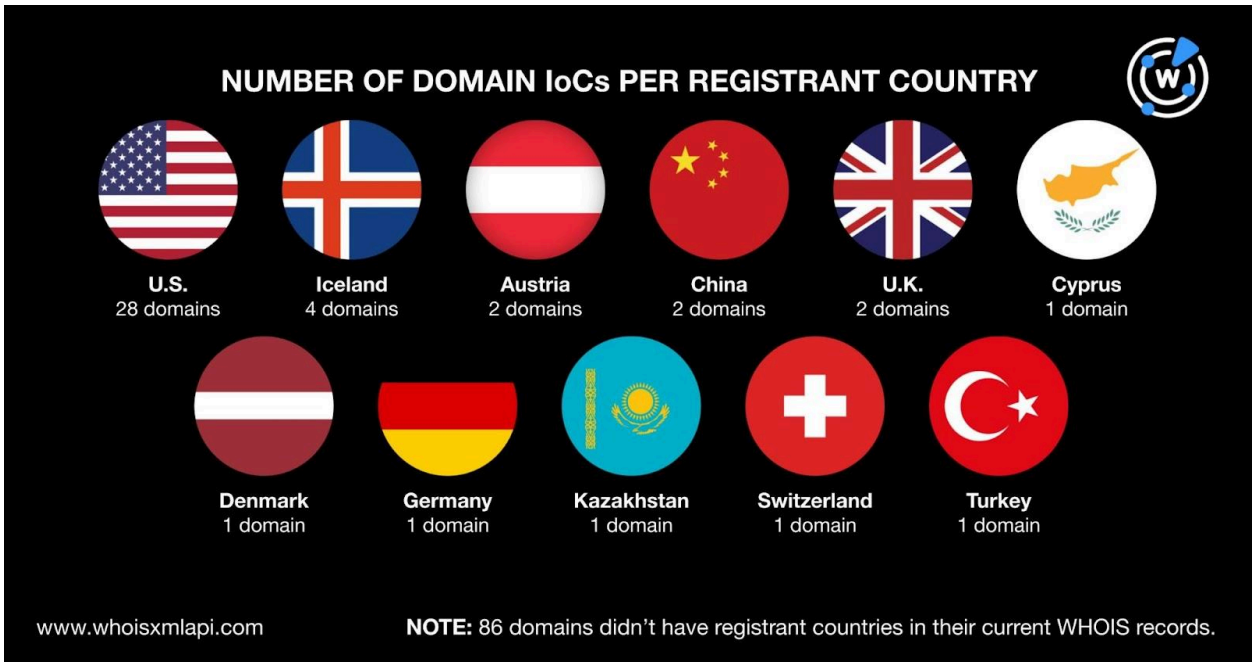
domain IoC each. Finally, 84 domain IoCs did not have registrar data in their current WHOIS records.



- The actors behind the malicious fake cryptocurrency-selling campaigns used both old and new domain names. The oldest domain IoC was created in 2014, while the newest two domains were created in 2024. Eighteen domains were created in 2023; seven in 2021; six each in 2019, 2020, and 2022; two in 2024; and one each in 2014 and 2016. Finally, 83 domain IoCs did not have creation dates in their current WHOIS records.



- The domain IoCs were spread across 11 countries topped by the U.S., which accounted for 28 domains. Four domains were registered in Iceland. Austria, China, and the U.K. accounted for two domain IoCs each. One domain each was registered in Cyprus, Denmark, Germany, Kazakhstan, Switzerland, and Turkey. Finally, 86 domain IoCs did not have registrant countries in their current WHOIS records.



IoC DNS Footprints

To uncover other artifacts potentially connected to the fake cryptocurrency-selling campaigns, we first performed WHOIS History API queries for the 130 domains tagged as IoCs. Their historical WHOIS records contained 336 email addresses after duplicates were removed, 57 of which were public.

We then used the 57 public email addresses as reverse WHOIS API search terms and found 522 email-connected domains after duplicates and the IoCs were filtered out. Twenty-one of the email-connected domains were associated with 1–2 threats according to Threat Intelligence API. Take a look at five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREATS
brainiac[.]net	Phishing Generic
couponmafia[.]com	Phishing Generic
escrow-peer[.]com	Attack Phishing
escrow-trades[.]com	Attack Phishing
escrow-verify[.]com	Attack Phishing

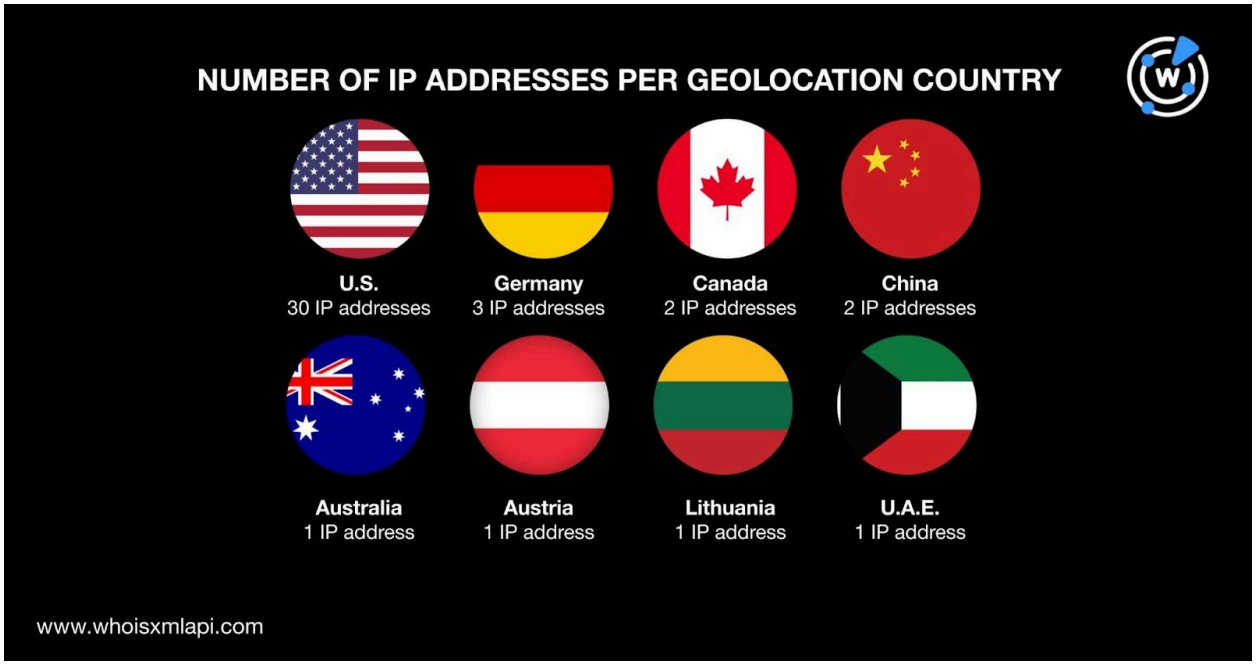
Next, DNS lookups for the 130 domains tagged as IoCs revealed that 91 of them did not actively resolve to any IP address. The remaining 39 domain IoCs, meanwhile, resolved to 41 IP addresses after duplicates were removed. Threat Intelligence Lookup showed that 39 of them were associated with various threats. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
104[.]247[.]81[.]54	Malware
104[.]247[.]81[.]51	Attack Malware
104[.]21[.]63[.]32	Generic Phishing

	Attack
81[.]19[.]154[.]98	Malware Generic Phishing Attack
103[.]224[.]182[.]253	Spam Phishing Generic Malware Command and control (C&C) Attack Suspicious

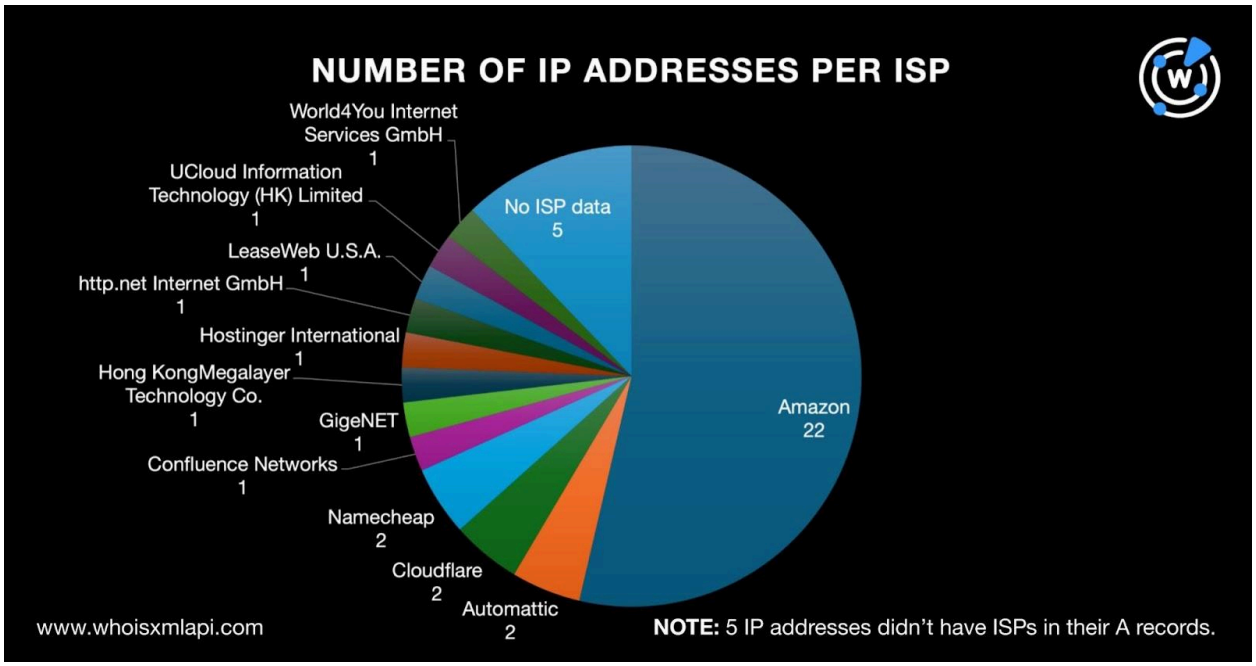
A bulk IP geolocation lookup for the 41 IP addresses showed that:

- They were distributed among eight geolocation countries led by the U.S., which accounted for 30 of the IP addresses. Germany took the second spot with three IP addresses followed by Canada and China with two IP address IoCs each. One IP address each was geolocated in Australia, Austria, Lithuania, and the U.A.E.



- They were also spread across 12 ISPs topped by Amazon, which accounted for 22 IP address IoCs. Automattic, Cloudflare, and Namecheap tied in second place with two IP

IoCs each. One IP address IoC each was administered by Confluence Networks, GigeNET, Hong KongMegalayer Technology Co., Hostinger International, http.net Internet GmbH, LeaseWeb U.S.A., UCloud Information Technology (HK) Limited, and World4You Internet Services GmbH. Finally, five IP addresses did not have ISPs in their A records.



We also subjected the 41 IP addresses to reverse IP lookups and found that only two of them could be dedicated. Altogether, they hosted 259 domains after duplicates, the IoCs, and the email-connected domains were filtered out.

To cover all bases, we looked for domains that started with the same text strings as the IoCs. They only used different topTLD extensions. Eighty-four text strings also appeared in 1,947 string-connected domains. They were:

- **bijora-btc.**
- **bilaxy.**
- **billaxy.**
- **binfox.**
- **bitbitter.**
- **bitcoingate.**
- **bitcoinly.**
- **bitcoinmates.**
- **bitcwallet.**
- **bitexmo.**
- **bitfenix.**
- **bitfinex.**
- **bitreg.**
- **bittorex.**
- **bitumb.**
- **bkex.**
- **blmtrade.**
- **blokcoin.**
- **btc-coin.**
- **chartrade.**
- **coingates.**
- **coinmex.**
- **coinpays.**
- **coinrexo.**
- **coinswallet.**
- **creonix.**
- **cry-coin.**

- **crypto-exchange24.**
- **cryptonex.**
- **cryptonfix.**
- **cryptosafe.**
- **cryptosis.**
- **cryptotis.**
- **cryptotradeltd.**
- **delltrade.**
- **drxtrade.**
- **edustr.**
- **emetero.**
- **exort.**
- **exstrade.**
- **filatrade.**
- **fixxcoin.**
- **gantonshop.**
- **gdax.**
- **goxtrade.**
- **highcoin.**
- **hillstrade.**
- **hiuobi.**
- **hurtrade.**
- **hyptrade.**
- **imetrade.**
- **jiratrade.**
- **kestrade.**
- **ledgerswap.**
- **lloydstrade.**
- **lutidastore.**
- **mybitmax.**
- **owrix.**
- **paxful-trade.**
- **polcrypt.**
- **purplecrypto.**
- **red-shadow.**
- **restrade.**
- **safetytrade.**
- **sfptrade.**
- **spacexcrypt.**
- **ssngroup.**
- **swithcoin.**
- **thebitex.**
- **tidebit.**
- **tihuanaparmo.**
- **tradeberry.**
- **tradekucoin.**
- **tradenc.**
- **traxcoins.**
- **unctrade.**
- **unictrade.**
- **urtrader.**
- **viral.**
- **weextrade.**
- **weonix.**
- **wernox.**
- **worldtrader.**
- **yobit.**

Threat Intelligence API found that 15 of them were associated with various threats. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREATS
coinswallet[.]info	Generic Attack
paxful-trade[.]info	Attack Phishing
paxful-trade[.]link	Attack Phishing
paxful-trade[.]pro	Attack Phishing
yobit[.]press	Malware

—

Our DNS deep dive into the fake cryptocurrency-selling campaigns led to the discovery of 2,769 potentially connected artifacts. Many of them, 75 to be exact, seem to have already been weaponized. As cryptocurrency usage becomes more popular, we are bound to see more threats targeting them, making staying ahead of the curve critical.

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

Domains Tagged as IoCs

- aftcrypt[.]com
- baystrade[.]com
- bijora-btc[.]com
- bilaxy[.]club
- billaxy[.]com
- binfox[.]ltd
- bitbitter[.]net
- bitcoingate[.]pro
- bitcoinly[.]co[.]uk
- bitcoinmates[.]com
- bitcwallet[.]com
- bitexmo[.]net
- bitfenix[.]xyz
- bitfinex[.]store
- bitmerger[.]com
- bitrade-x[.]com
- bitreg[.]net
- bittenix[.]com
- bitterrexa[.]com
- bittorex[.]net
- bitumb[.]com
- bixetrade[.]com
- bkex[.]us
- blmtrade[.]com
- blokcoin[.]net
- blstacks[.]com
- btc-coin[.]net
- btcbeaxy[.]com
- chartrade[.]com
- coinbascet[.]com
- coinbeaxy[.]com
- coincashup[.]com
- coingates[.]org
- coinmex[.]org
- coinorm[.]com
- coinpays[.]uk
- coinrexo[.]com
- coinswallet[.]space
- cointradego[.]com
- creonix[.]net
- cry-coin[.]net
- crypto-exchange24[.]com

- cryptoborium[.]com
- cryptoelegant[.]com
- cryptohorium[.]com
- cryptolays[.]com
- cryptonex[.]uk
- cryptonfix[.]com
- cryptorwallet[.]com
- cryptosafe[.]ltd
- cryptosis[.]cc
- cryptotis[.]com
- cryptotradego[.]com
- cryptotradeltd[.]com
- cryptoxlogy[.]com
- cryptoxorium[.]com
- cryptozorium[.]com
- crytptbtc[.]com
- delltrade[.]com
- drxtrade[.]com
- edustr[.]com
- emetero[.]com
- exmofit[.]com
- exort[.]org
- exstrade[.]com
- eyetradex[.]com
- filatrade[.]com
- finontrade[.]com
- fixxcoin[.]com
- foxxytrade[.]com
- gantonshop[.]com
- gdax[.]us
- genecryptotrade[.]com
- getcoinbet[.]com
- gexofit[.]com
- goxtrade[.]com
- harydex[.]com
- haxcoins[.]com
- highcoin[.]net
- hillstrade[.]net
- hiuobi[.]com
- hubcoi[.]com
- hurtrade[.]com
- hyptrade[.]com
- imetrade[.]net
- jiratrade[.]com
- kestrade[.]com
- lackeycrypt[.]com
- ledgerswap[.]com
- lloydstrade[.]info
- lutidastore[.]com
- mybitmax[.]com
- newcoins24[.]com
- numercoins[.]com
- onenotet[.]com
- ovextrade[.]com
- owrix[.]com
- padhex[.]com
- paxful-trade[.]com
- polcrypt[.]com
- prudentialex[.]com
- purplecrypto[.]net
- red-shadow[.]ru
- restrade[.]org
- safetytrade[.]net
- sfptrade[.]com
- spacexcrypt[.]com
- ssngroup[.]ltd
- stormpoe[.]com
- swiftcoinbitx[.]com
- swithcoin[.]com
- thebitex[.]com
- tidebit[.]eu
- tihuanaparmo[.]xyz
- tradeberry[.]org
- tradekucoin[.]info
- tradenc[.]com
- traxcoins[.]com
- unctrade[.]com
- unictrade[.]com
- urbshares[.]net
- urtrader[.]com

- viral[.]kz
- waxcoins[.]com
- weextrade[.]com
- weonix[.]net
- wernox[.]net
- worldtrader[.]org
- yalescoin[.]com
- yobit[.]website

Sample Email-Connected Domains

- 1pojfr[.]us
- 360vrphoto[.]com
- 360vrtourguide[.]com
- 7oo7[.]com
- a1roofing[.]us
- abnormal[.]net
- activitycrate[.]com
- addyexpress[.]com
- aerodrawing[.]com
- affirm-paxful[.]com
- agoraop[.]us
- airdunk[.]net
- allhaul[.]us
- alphamvp[.]com
- amazoon[.]us
- amazula[.]com
- anestri[.]com
- animatorvideos[.]com
- antexcoin[.]com
- anyshoponline[.]com
- apollodesign[.]us
- apollomade[.]us
- apollomfg[.]us
- artofgrowth[.]com
- artoscoin[.]com
- atomichash[.]com
- auctioning[.]company
- automateemails[.]com
- bainance[.]us
- bbwsexvideos[.]us
- belledom[.]com
- benocoin[.]com
- bibbio[.]com
- bidcash[.]com
- bilslight[.]com
- binatyx[.]com
- binecoin[.]com
- binodium[.]com
- bit-coin-wallet[.]biz
- bit-coin-wallet[.]us
- bitardos[.]com
- bitcextra[.]com
- bitcflash[.]com
- bitclop[.]com
- bitcluxe[.]com
- bitcmulti[.]com
- bitcoin-applications[.]com
- bitcoindiv[.]com
- bitcoinembassyindia[.]com
- bitcoinendorse[.]com
- bitcoinenergize[.]com
- bitcoinexchangeprice[.]com
- bitcoinfinder[.]com
- bitcoingfs[.]com
- bitcoinhistoric[.]com
- bitcoinhistorical[.]com
- bitcoinidentify[.]com
- bitcoinmone[.]com
- bitcoinnarc[.]com
- bitcoinops[.]com
- bitcoinppv[.]com
- bitcoinpricingchart[.]com
- bitcoinreply[.]com
- bitcoinshippers[.]com
- bitcoinsocialnetwork[.]com
- bitcoinspaceship[.]com

- bitcointly[.]com
- bitcoinunify[.]com
- bitcoinxchangerates[.]com
- bitcoinyx[.]com
- bitcplace[.]com
- bitcprice[.]com
- bitcraf[.]com
- bitcreon[.]com
- bitcrion[.]com
- bitcrise[.]com
- biteonyx[.]com
- biterios[.]com
- bitfincoinex[.]com
- bitgamb[.]com
- bitgeco[.]com
- bitguru24[.]com
- bitlios[.]com
- bitlumin[.]com
- bitlunix[.]com
- bitmaro[.]com
- bitnexed[.]com
- bitocoinex[.]com
- bitprofex[.]com
- bitrezol[.]com
- bitrols[.]com
- bitsavex[.]com
- bitsclap[.]com
- bitsfame[.]com
- bitsfino[.]com
- bitslipto[.]com
- bitsnaco[.]com
- bitsnefix[.]com
- bitstiger[.]com
- bitsultra[.]com

Sample IP Addresses

- 103[.]224[.]182[.]253
- 104[.]21[.]63[.]32
- 104[.]247[.]81[.]51
- 104[.]247[.]81[.]54
- 13[.]248[.]169[.]48
- 13[.]248[.]213[.]45
- 13[.]56[.]33[.]8
- 15[.]197[.]148[.]33
- 154[.]39[.]176[.]142
- 162[.]255[.]119[.]22
- 172[.]67[.]142[.]173
- 192[.]0[.]78[.]24
- 192[.]0[.]78[.]25
- 192[.]64[.]119[.]138
- 198[.]49[.]23[.]145
- 199[.]59[.]243[.]225
- 208[.]91[.]197[.]27
- 213[.]160[.]71[.]210
- 23[.]82[.]12[.]29
- 3[.]130[.]204[.]160

Sample IP-Connected Domains

- 24hfx[.]com
- 360ant[.]com
- 360jav[.]com
- 365yin[.]com
- 38989cc[.]cn
- 3mchain[.]com
- 51trading[.]com
- 52oil[.]com
- 636526[.]com
- 6955a[.]cn
- 997358[.]com
- aaaname[.]com
- aaluck[.]com
- aicrosschain[.]com
- aliisp[.]com
- alijf[.]com

- alimw[.]com
- alipoc[.]com
- alipz[.]com
- aliqy[.]com
- alisms[.]com
- alissl[.]com
- aliyingyong[.]com
- ammswap[.]com
- amzf[.]cn
- bameibao[.]com
- bcw6[.]net
- bfdax[.]com
- binarydex[.]com
- biz777[.]com
- bocai[.]plus
- btdapp[.]com
- btmax[.]com
- bttswap[.]com
- buyxau[.]com
- canjun[.]cn
- capfax[.]com
- cdndex[.]com
- cdschain[.]com
- chamcc[.]com
- chebaijin[.]com
- chengduishang[.]com
- cmbchain[.]com
- cmx123[.]com
- coin580[.]com
- crosschain[.]im
- crosschain[.]plus
- crosschainplus[.]com
- cryptotradeltd[.]com
- cupswap[.]com

Sample String-Connected Domains

- bijora-btc[.]net
- bijora-btc[.]org
- bilaxy[.]app
- bilaxy[.]biz
- bilaxy[.]cc
- bilaxy[.]ch
- bilaxy[.]cloud
- bilaxy[.]co
- bilaxy[.]co[.]uk
- bilaxy[.]com
- bilaxy[.]com[.]au
- bilaxy[.]com[.]tr
- bilaxy[.]cool
- bilaxy[.]de
- bilaxy[.]digital
- bilaxy[.]eu
- bilaxy[.]exchange
- bilaxy[.]fit
- bilaxy[.]fr
- bilaxy[.]fun
- bilaxy[.]fyi
- bilaxy[.]host
- bilaxy[.]info
- bilaxy[.]io
- bilaxy[.]ir
- bilaxy[.]it
- bilaxy[.]kred
- bilaxy[.]life
- bilaxy[.]live
- bilaxy[.]ltd
- bilaxy[.]luxe
- bilaxy[.]net
- bilaxy[.]network
- bilaxy[.]news
- bilaxy[.]nl
- bilaxy[.]one
- bilaxy[.]online
- bilaxy[.]org
- bilaxy[.]pl
- bilaxy[.]plus

- bilaxy[.]pro
- bilaxy[.]ru
- bilaxy[.]shop
- bilaxy[.]site
- bilaxy[.]social
- bilaxy[.]space
- bilaxy[.]store
- bilaxy[.]tech
- bilaxy[.]today
- bilaxy[.]top
- bilaxy[.]trade
- bilaxy[.]tv
- bilaxy[.]uno
- bilaxy[.]us
- bilaxy[.]vip
- bilaxy[.]website
- bilaxy[.]world
- bilaxy[.]xyz
- billaxy[.]net
- binfox[.]bar
- binfox[.]cn
- binfox[.]com
- binfox[.]de
- binfox[.]net
- binfox[.]online
- binfox[.]uy
- binfox[.]ws
- binfox[.]xn--io0a7i[.]cn
- bitbitter[.]com
- bitbitter[.]eu
- bitbitter[.]tk
- bitcoingate[.]biz
- bitcoingate[.]ca
- bitcoingate[.]ch
- bitcoingate[.]club
- bitcoingate[.]com
- bitcoingate[.]com[.]au
- bitcoingate[.]cz
- bitcoingate[.]eu
- bitcoingate[.]net
- bitcoingate[.]org
- bitcoingate[.]pl
- bitcoingate[.]shop
- bitcoingate[.]sk
- bitcoinly[.]app
- bitcoinly[.]blog
- bitcoinly[.]ch
- bitcoinly[.]club
- bitcoinly[.]co
- bitcoinly[.]co[.]in
- bitcoinly[.]com
- bitcoinly[.]de
- bitcoinly[.]dev
- bitcoinly[.]digital
- bitcoinly[.]eu
- bitcoinly[.]fr
- bitcoinly[.]ga
- bitcoinly[.]in
- bitcoinly[.]info
- bitcoinly[.]io