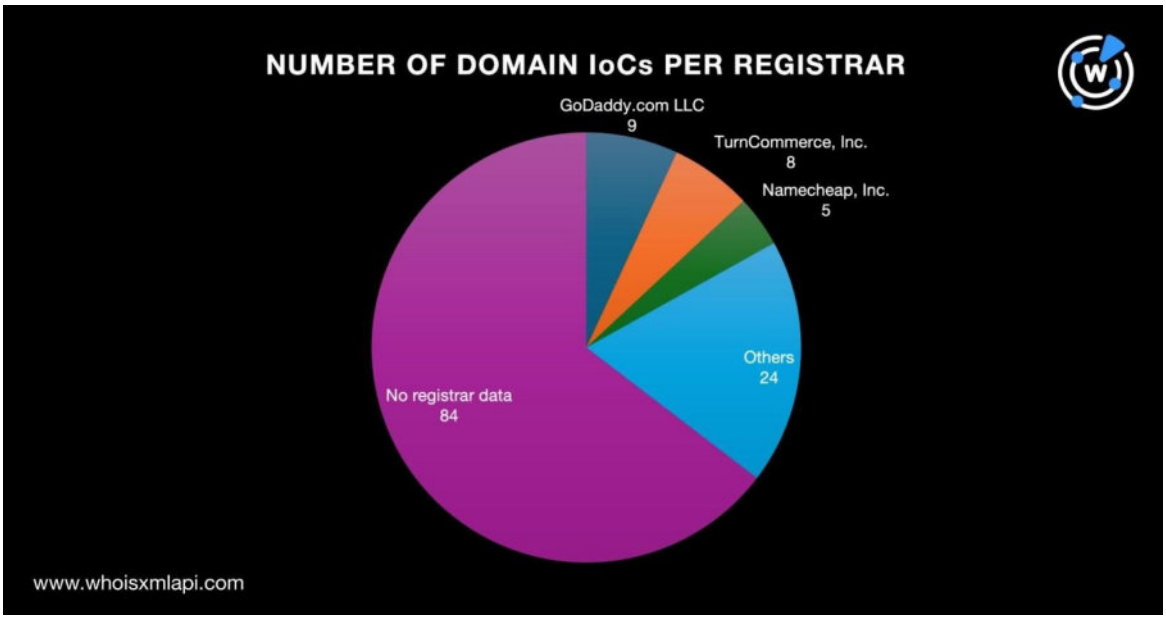
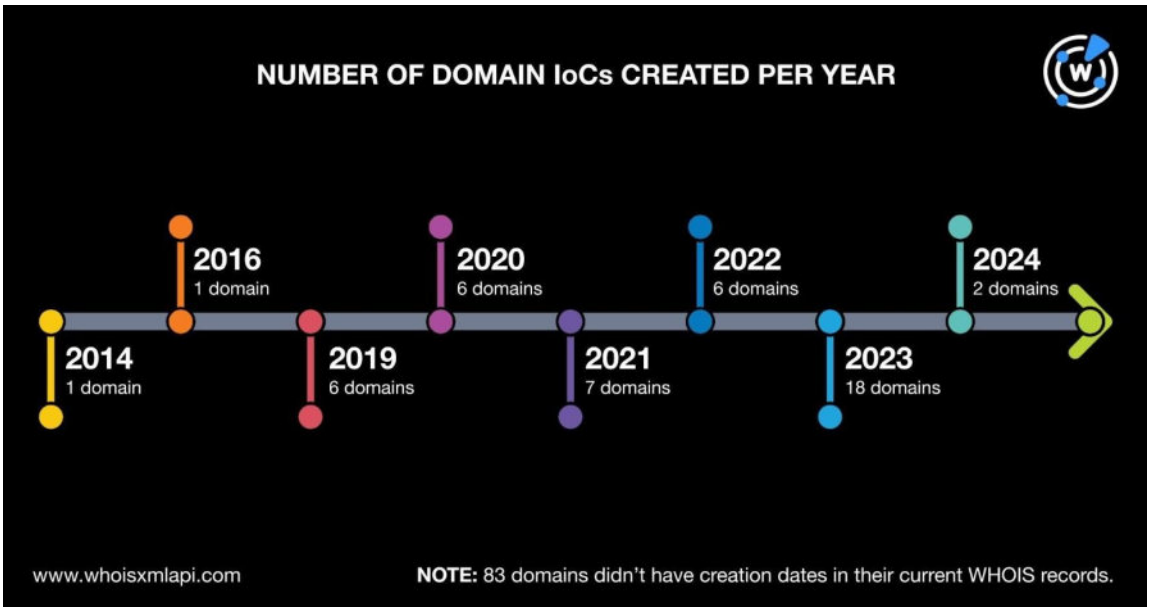
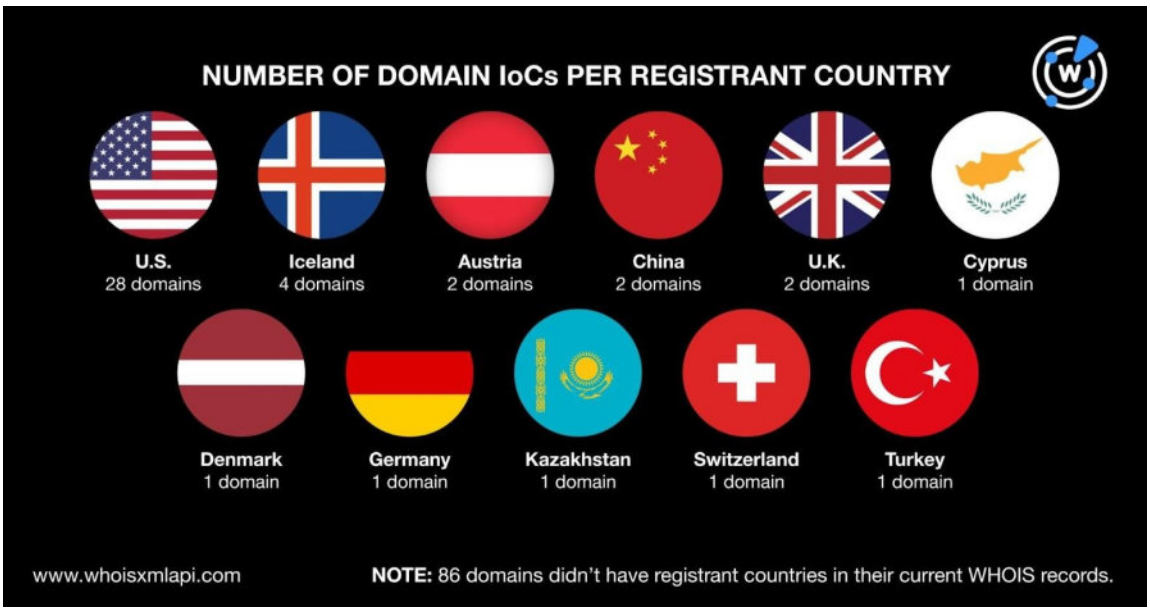
Inc.、Namebeacon.com, Inc.、Network Solutions LLC、REGRU-RU、Sav.com LLC、Squarespace Domains LLC、World4You Internet Services GmbHにそれぞれ1個ずつが管理されていました。なお、84個のドメインIoCについては、現在のWHOISレコードにレジストラのデータがありませんでした。



- 悪意ある偽暗号通貨販売キャンペーンの背後にいるアクターは、新旧両方のドメイン名を使用していました。最も古いドメインIoCは2014年に新規登録されていました。他方、最も新しい2つのドメインIoCは2024年に新規登録されたものです。2023年には18個、2021年に7個が、2019年、2020年、2022年にそれぞれ6個、2024年に2個、そして2014年と2016年に1個ずつが新たに登録されていました。残りの83個のドメインIoCについては、現在のWHOISに登録年月日の記録がありませんでした。



- ドメインIoCの登録地は11カ国に分散していました。最も多かったのは米国で、28個が同国で登録されていました。また、アイスランドで4個、オーストリア、中国、英国でそれぞれ2個、キプロス、デンマーク、ドイツ、カザフスタン、スイス、トルコでそれぞれ1個が登録されていました。他方、86個については、現在のWHOISレコードに登録者の国の情報がありませんでした。



DNSに残されたIoCの足跡

偽の暗号通貨販売キャンペーンとの関連が疑われる他のアーティファクトを見つけるため、130個のドメインIoCに対してWHOIS History APIのクエリを実行しました。その結果、ドメインIoCの過去のWHOISレコードには合計336個（重複を除く）のメールアドレスが残っており、そのうち57個は公開されていました。

その57個の公開メールアドレスをキーワードにしてReverse WHOIS APIで検索を実行したところ、それらのメールアドレスを使って登録された533個のドメイン名が検出されました（重複と既存のIoCを除く）。Threat Intelligence APIの結果から、そのうち21個のドメイン名は、1〜2件の脅威に関連していることがわかりました。以下に5つの例を示します：

ドメインIoCと同じメールアドレスを使用していた悪意あるドメイン名	関連していた脅威
brainiac[.]net	Phishing Generic
couponmafia[.]com	Phishing Generic
escrow-peer[.]com	Attack Phishing
escrow-trades[.]com	Attack Phishing
escrow-verify[.]com	Attack Phishing

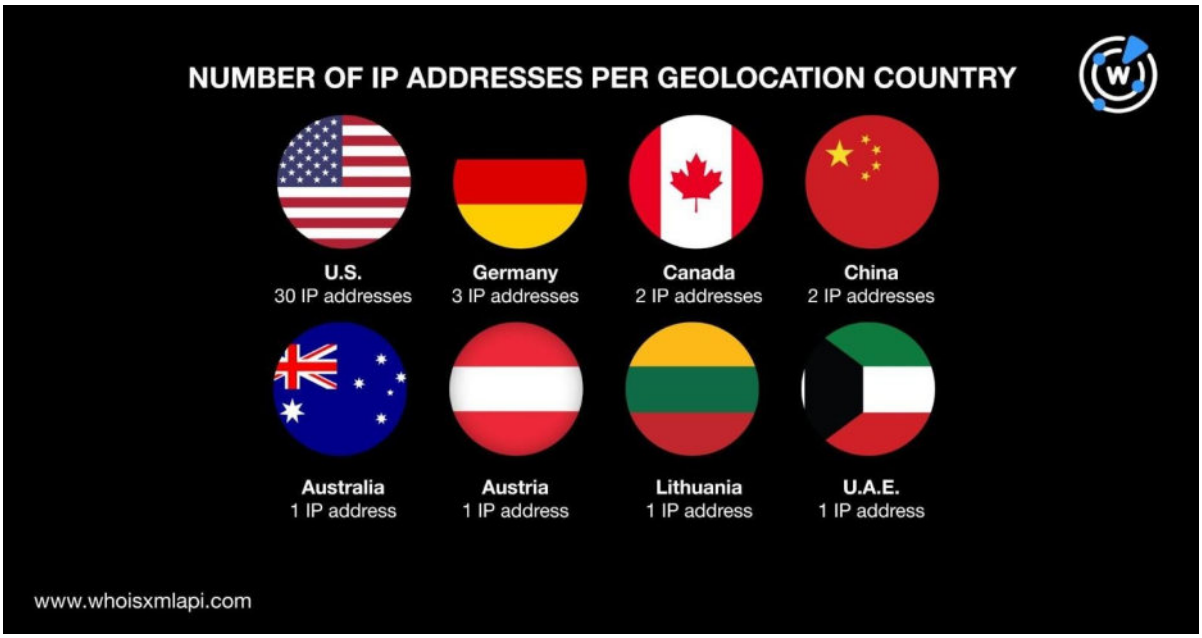
次に、130個のドメインIoCに対してDNS Lookupを実行した結果、91個のドメインIoCは有効なIPアドレスに名前解決しませんでした。他方、残りの39個は41個のIPアドレスに解決しました（重複を除く）。Threat Intelligence Lookupによれば、そのうち39個のIPアドレスは、さまざまな脅威に関与していました。以下に5つの例を示します：

悪意あるIPアドレス	関連していた脅威
104[.]247[.]81[.]54	Malware
104[.]247[.]81[.]51	Attack Malware
104[.]21[.]63[.]32	Generic Phishing Attack

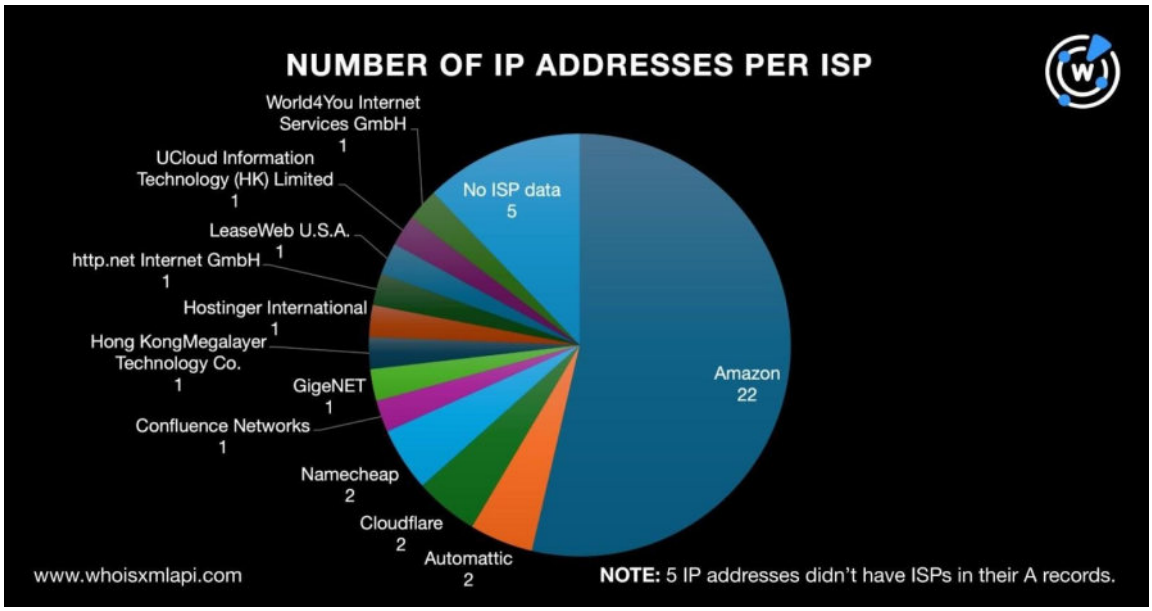
81[.]19[.]154[.]98	Malware Generic Phishing Attack
103[.]224[.]182[.]253	Spam Phishing Generic Malware Command and control (C&C) Attack Suspicious

また、ドメインIoCが解決した41個のIPアドレス（以下「IPアドレスIoC」）についてBulk IP Geolocation Lookupを実行した結果、以下のことが判明しました：

- 41個のジオロケーションは8カ国に分散していました。最も多かったのは米国で、30個が地理的に位置していました。次に多かったのはドイツで、3個ありました。さらに、2個がそれぞれカナダと中国を指していました。その他、オーストラリア、オーストリア、リトアニアおよびUAEに1個ずつありました。



- 最も多くのIPアドレスIoCを管理していたISPはAmazonで、22個にのぼりました。また、Automattic、Cloudflare、Namecheapがそれぞれ2個、 Confluence Networks 、GigeNET、Hong KongMegalayer Technology Co.、Hostinger International、http.net Internet GmbH、LeaseWeb U.S.A.、UCloud Information Technology (HK) LimitedおよびWorld4You Internet Services GmbHがそれぞれ1個の管理ISPになっていました。さらに、Aレコードを見たところ、5個については管理ISPがありませんでした。



41個のIPアドレスIoCを[Reverse IP Lookup]にかけたところ、専用と思われるアドレスが2個ありました。そして、それらは合計259個のドメイン名（重複、既存IoCおよびドメインIoCと同じメールアドレスを使用していたドメイン名を除く）をホストしていました。

最後に、IoCと同じ文字列で始まるドメイン名を探しました。すなわち、第2レベルドメインの文字列がドメインIoCと同じ単語で始まっており、TLDはさまざまに異なるドメイン名です。分析の結果、以下の84種類の文字列が、1,947個のドメイン名の第2レベルに共通して含まれていることがわかりました：

- **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.

そして、Threat Intelligence APIにより、そのうちの15個のドメイン名がさまざまな脅威と関連していることが判明しました。5つの例を以下に示します：

共通の文字列を含む悪意あるドメイン名	関連していた脅威
coinswallet[.]info	Generic Attack
paxful-trade[.]info	Attack Phishing
paxful-trade[.]link	Attack Phishing
paxful-trade[.]pro	Attack Phishing
yobit[.]press	Malware

—

今回当社が行ったDNSの徹底調査により、偽の暗号通貨販売キャンペーンに関与した疑いのあるアーティファクトが合計2,769個発見されました。そのうち75個は、すでに悪用されているようです。暗号通貨の普及につれ、今後暗号通貨を標的とした脅威はさらに増えることが予想されます。先手を打って対策を講じることが必要です。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトの例

ドメインIoC

- 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

ドメインIoCと同じメールアドレスを使用していたドメイン名の例

- 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

ドメインIoCが名前解決したIPアドレスの例

- 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

ドメインIoCが解決するIPアドレスにホストされていたドメイン名の例

- 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

ドメインIoCと同じ文字列を含むドメイン名の例

- 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