Investigating the Proliferation of Deepfake Scams

Table of Contents

Executive Report

While deepfakes may sometimes be perceived as amusing, their potential for harm is significant and far-reaching. One finance worker for a multinational firm, for example, was tricked into paying out US$25 million to a deepfake scammer who pretended to be their company's chief financial officer (CFO) in a video call just this February.

Palo Alto Networks Unit 42 dove deep into various deepfake scams that have plagued users over time and in the process uncovered 416 domain names that played a part in them. The WhoisXML API research team believes there could be more behind the indicators of compromise (IoCs) that have already been made public. Our analysis specifically uncovered:

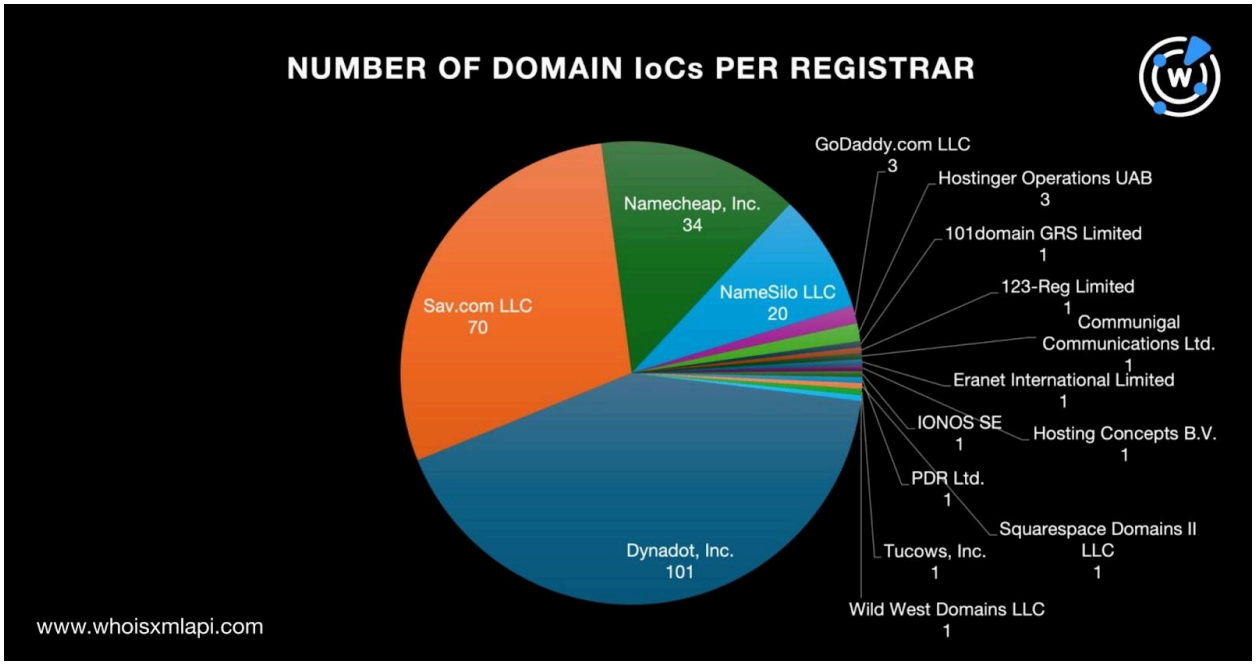
- 1,070 registrant-connected domains
- Six email-connected domains
- 316 IP addresses, 285 of which turned out to be malicious
- 515 IP-connected domains, three of which turned out to be associated with various threats
- 3,056 string-connected domains, 12 of which may have already figured in malicious campaigns

Facts about the IoCs

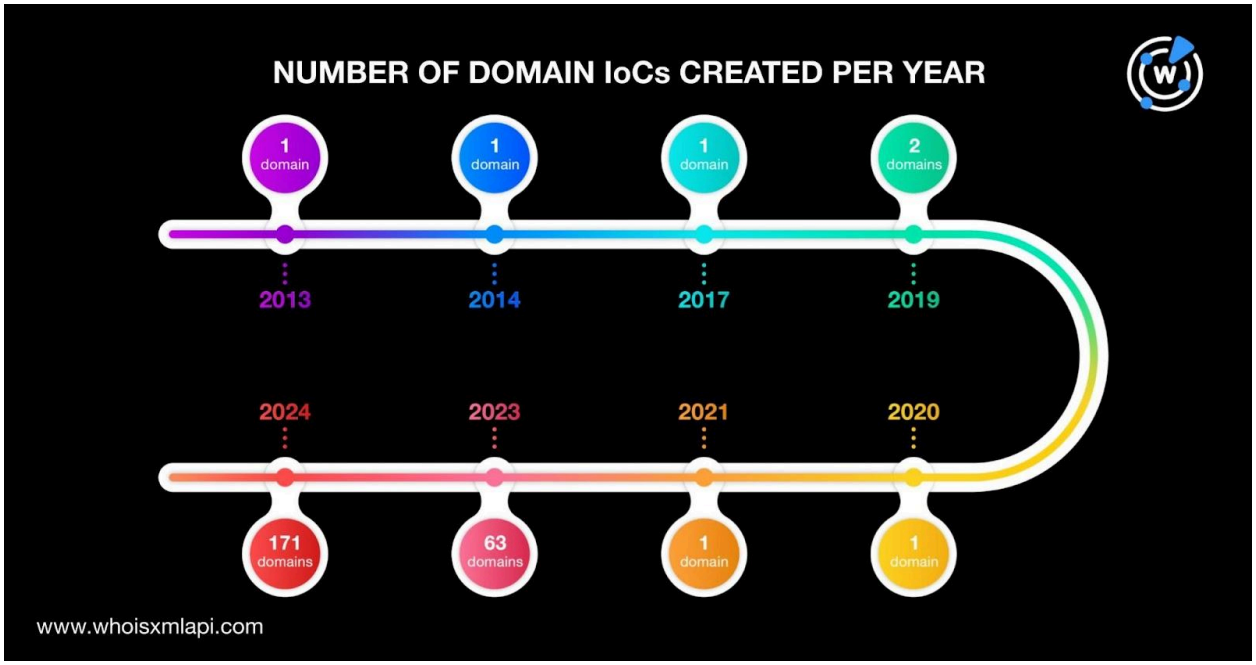
We kicked off the investigation by performing a bulk WHOIS lookup for the domains identified as IoCs, which revealed that only 241 had current WHOIS records. The lookup also yielded other results, namely:

- They were spread across 16 registrars led by Dynadot, Inc., which accounted for 101 domain IoCs. Sav.com LLC came in second place with 70 while Namecheap, Inc. placed third with 34. NameSilo LLC (20 domain IoCs); GoDaddy.com LLC and Hostinger

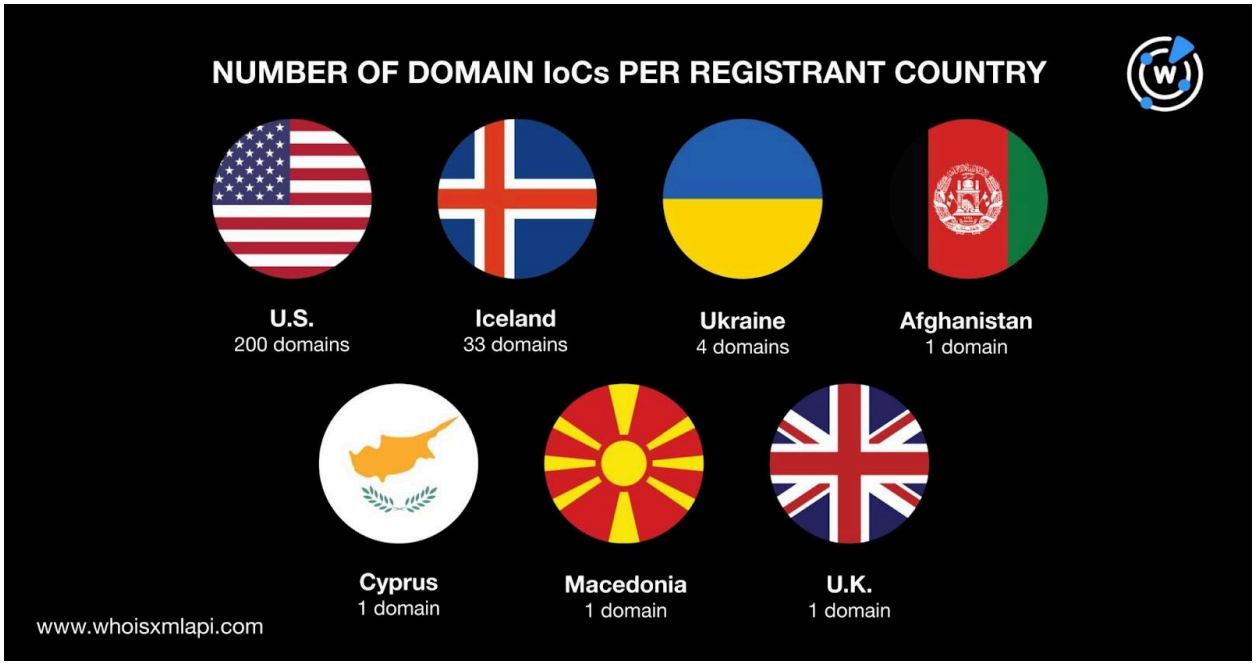
Operations UAB (three domain IoCs each); and 101domain GRS Limited, 123-Reg Limited, Communigal Communications Ltd., Eranet International Limited, Hosting Concepts B.V., IONOS SE, PDR Ltd., Squarespace Domains II LLC, Tucows, Inc., and Wild West Domains LLC (one domain IoC each) completed the list.



- While a majority of the domain IoCs, 171 to be exact, were created just this year, the oldest was created way back in 2013. Take a look at a timeline that sums up their creation dates below.



- They were registered in seven countries led by the U.S., which accounted for 200 domain IoCs. Iceland took the second spot with 33 domain IoCs while Ukraine placed third with four domain IoCs. Afghanistan, Cyprus, Macedonia, and the U.K. completed the list with one domain IoC each.



- Three domain IoCs also had public registrant details, specifically organization names that can be useful in uncovering registrant-connected domains later on.

The Hunt for Connected Web Properties

We began our search for connected web properties with Reverse WHOIS Search queries for the three public registrant organizations found in the current WHOIS records of the 241 domain IoCs with current WHOIS records on our list. Using the tool's Advanced feature, we looked for exact matches of the registrant organizations in historical WHOIS records. We found 1,070 registrant-connected domains after duplicates and the IoCs were filtered out.

Next, we performed WHOIS History API queries for the 241 domain IoCs, which allowed us to obtain 32 email addresses from their historical WHOIS records after filtering out duplicates. A closer look at them showed that 10 were public email addresses that we then used to look for email-connected domains.

Reverse WHOIS API queries for the 10 public email addresses further showed that one email address could belong to a domainer (given the high number of connected domains), so it was excluded from the final list. The nine public email addresses appeared in the current WHOIS records of six email-connected domains after duplicates, the IoCs, and the registrant-connected domains were filtered out.

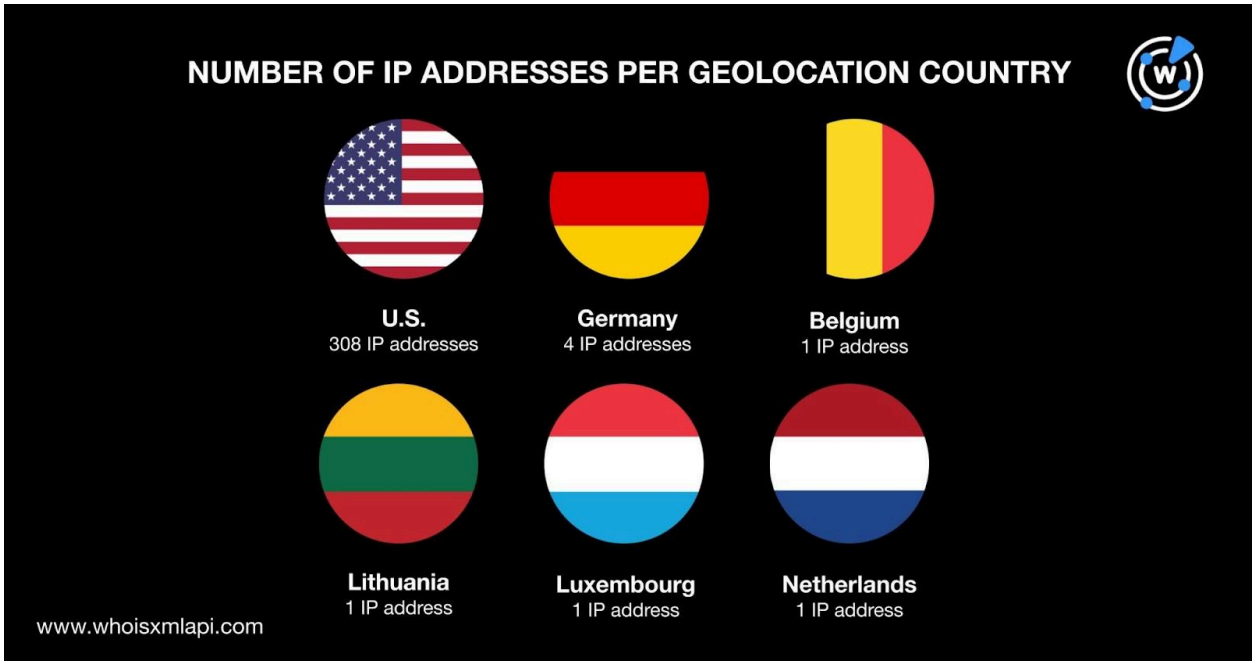
We then conducted DNS lookups for the 241 domain IoCs, which allowed us to determine that they resolved to 316 unique IP addresses. A total of 285 of the 316 IP addresses turned out to be associated with various threats according to Threat Intelligence API. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT TYPES
104[.]21[.]1[.]214	Malware
104[.]21[.]1[.]224	Generic Phishing
104[.]21[.]12[.]192	Generic Malware Phishing
104[.]21[.]15[.]91	Attack Generic Malware Phishing

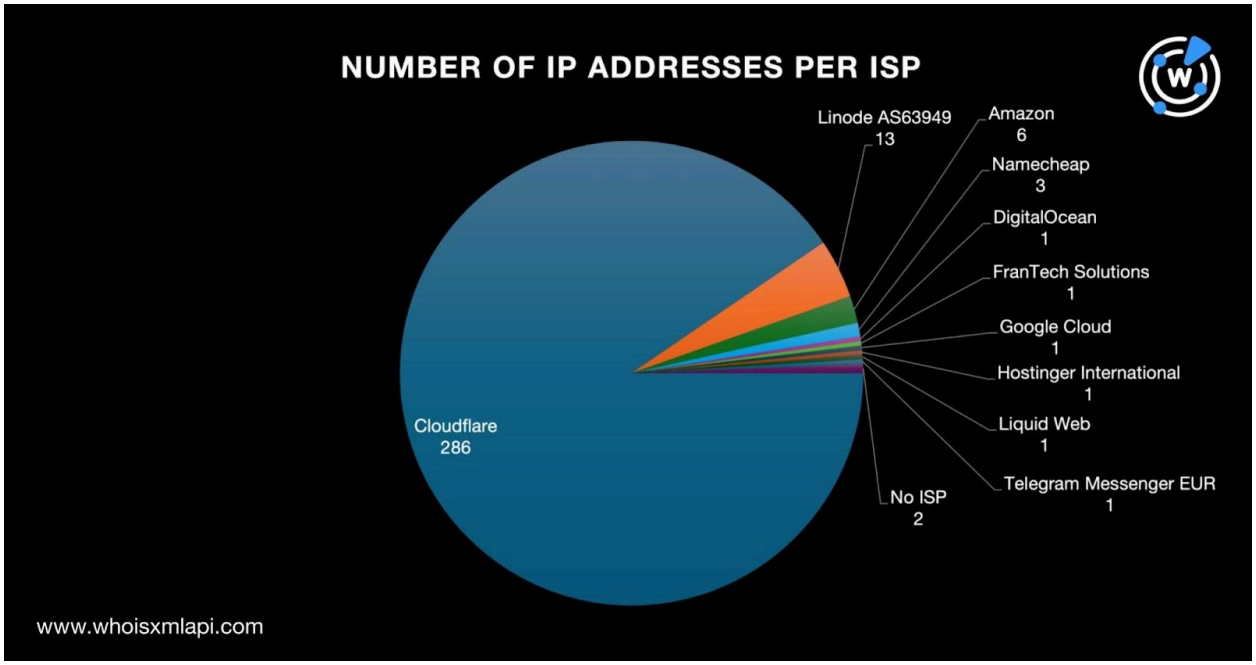
3[.]64[.]163[.]50	Attack Command and control (C&C) Generic Malware Phishing Spam Suspicious

To know more about the 316 IP addresses we uncovered, we performed a bulk IP geolocation lookup, which revealed that:

- They were geolocated in six countries led by the U.S., which accounted for 308 IP addresses. Germany took the second spot with four IP addresses. Belgium, Lithuania, Luxembourg, and the Netherlands accounted for one IP address each.



- They were also split across 10 ISPs topped by Cloudflare, which accounted for 286 IP addresses. Linode AS63949 lagged far behind in second place with 13 IP addresses. Amazon took the third spot with six IP addresses followed by Namecheap with three. DigitalOcean, FranTech Solutions, Google Cloud, Hostinger International, Liquid Web, and Telegram Messenger EUR accounted for one IP address each. Two IP addresses did not have ISP information.



We then performed reverse IP lookups for the 316 IP addresses and found that five of them could be dedicated hosts. They hosted 515 IP-connected domains in total after duplicates, the IoCs, and registrant- and email-connected domains were filtered out. Three of them also turned out to be malicious based on Threat Intelligence API checks. An example would be artisticembroid[.]com, which seemingly figured in a phishing campaign.

As our last step, we used Domains & Subdomains Discovery to find domains that started with the same text strings as the 241 domain IoCs. We found out that only 148 of the strings appeared in other domains, namely:

- **ai-usmcapital**
- **ai-usmcollective**
- **ai-usmfence**
- **aifaith**
- **aiprincipal**
- **aireliance**
- **aishield**
- **aiside**
- **aisimple**
- **aitfinoutlay**
- **bit-360**
- **block4aiendeavor**
- **block4aifinancier**
- **block4aiinitiative**
- **block4aimethod**
- **block4aioperation**
- **block4aipatron**
- **block4aiprotection**
- **block4aisafeguarding**
- **block4aischedule**
- **block4aisystem**
- **block4aitask**
- **block4aiwell-being**
- **block4alinitiative**
- **coinaibarrier**
- **coinaibasis**

- coinaiboundary
- coinaichannel
- coinaicommunicate
- coinaieducate
- coinaienclosure
- coinaifence
- coinaifinancier
- coinaiframework
- coinaimedium
- coinaipartition
- coinaiprecaution
- coinaishareholder
- coinaiside
- coinaistage
- coinaiwell-being
- coinalcommunity
- coinalendeavor
- coinalgamble
- coinalinitiative
- coinalinternational
- coinalprecaution
- coinalsafeguarding
- coinalsafetynet
- coinalscheme
- coinalundertaking
- coinaluniversal
- coinalwell-being
- coinangelinvestor
- coinbacker
- coinband
- coinbarrier
- coincapitalist
- coincollective
- coincommunity
- coindependence
- coinfinancier
- coingamble
- coingathering
- coininitiative
- coinpartition
- coinreliance
- coinside
- coinundertaking
- crystalincantation
- d1g1talpoint
- dearetung
- directors.
- easylender
- edenovougobio
- enter-up
- excellentone
- fabulous4onee
- fiirststreeeet
- flowcyber
- flowpulse
- foodtruckit
- fortunatenews
- gfnuw
- ggenniusprrojecct
- globalpolytr
- greenrealm
- groundbreakinginitiative
- growthventure
- growthwall
- grrandventure
- hideoutglownew
- higheststudy
- hotelierjobz
- huerwlleiss-herton
- hugeproject
- iaqa
- inc-co
- individualestablish
- infosysdata
- investcontribution
- investfortification
- investseries
- kevxk
- lartons
- maplegateu-yj

- **metawings**
- **milfarka**
- **naatuureeffocus**
- **newglowhideout**
- **originalquantum**
- **outlayquantum**
- **passionquantum**
- **peerfeectwall**
- **pro-fitters**
- **promisingendeavor**
- **qatuk**
- **quantum-ai**
- **quantumai.**
- **quantumal**
- **redwoodrest**
- **registration-form**
- **riseanalyze**
- **rockriddle**
- **sacvenih**
- **safegroup**
- **spacemome**
- **sskkilfulinnvestoor**
- **subsidystart**
- **superstarone**
- **swapfavour**
- **systemaibarricade**
- **systemaibasis**
- **systemaigroundwork**
- **systemainegotiator**
- **techmerge-ai**
- **testdomaintest**
- **theebeestbrookeer**
- **thequantumai**
- **unityventurehub**
- **untamedal**
- **wizardstar-sred**
- **wizardstar-sree**
- **wizardstar-srej**
- **wizardstar-sren**
- **wizardstar-srey**
- **wztnb**
- **xtradgpt**

Altogether, we uncovered 3,056 string-connected domains after duplicates; the IoCs; and the registrant-, email-, and IP-connected domains were filtered out. Twelve of them turned out to be associated with various threats according to Threat Intelligence API. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT TYPE
bit-360-ai[.]com	Generic Phishing
coincollective[.]net	Attack
dearetung[.]sbs	Generic Phishing
iaqajiaauwvlptner[.]org	C&C
quantum-ai-trading[.]com	Phishing

—

Our in-depth IoC list expansion analysis for the 416 deepfake scam domains led to the discovery of 4,963 connected web properties comprising 1,070 registrant-connected domains, six email-connected domains, 316 IP addresses, 515 IP-connected domains, and 3,056 string-connected domains. Three hundred of these connected artifacts have also already been used in various malicious campaigns.

As evidenced by the large pool of web properties connected to the threat, it seems the role of deepfakes in malicious campaigns is prominent.

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 Registrant-Connected Domains

- ablesizefacefade[.]click
- abletodaysnackcanyon[.]com
- aboutdonorhellosaddle[.]click
- aboveblossomcolor[.]click
- abovefabrictragic[.]click
- abovegospelincreasesoul[.]click
- abovemistakeindexforum[.]online
- abovereasonmodify[.]click
- absorbgungovernpayment[.]online
- abstractskatepursereason[.]click
- absurdpersonbeautybrush[.]online
- accessgluepuritydice[.]click
- accesslanguagealtermaze[.]click
- accidentgorillakite[.]click
- accountcodepeanutauction[.]online
- achievepioneersettle[.]click
- acousticgatemediaarrive[.]click
- acousticgingerdismissdisplay[.]online
- acrossmajorradargold[.]com
- actionlegtrumpet[.]click
- actualapplerookieassault[.]click
- adaptdeerpeppersurvey[.]click
- addmusthaveoppkit[.]click
- addmusthaveoppkit[.]online
- addmusthaveoppprofit[.]click
- addmusthaveoppprofit[.]online
- addmusthaveoppsalary[.]click
- addmusthaveoppsalary[.]online
- addresstransfercritickit[.]click
- adjustseniorpopularsea[.]click
- adjusttopiclazy[.]click

- advancedesigndayfuel[.]click
- afraidexpandribspoil[.]online
- againtellbulletfloor[.]click
- airportrailfamily[.]click
- alarmgiantbroom[.]click
- albumcheeseplateacoustic[.]click
- alcoholfarmtrulyvague[.]click
- aliencouchneitherexclude[.]click
- alleyafraidcover[.]click
- allforgiveaways[.]net
- allowleavebodywoman[.]click
- allowstylehundredcousin[.]online
- allowyouthpicnicpanic[.]click
- alterbrushcomfortmodify[.]click
- amazingnoticevillagereflect[.]click
- amountwisdomvisagate[.]click
- amusedmultiplyprint[.]click
- anklemergerailhover[.]click
- announceoffercurrentcasino[.]click
- annualchairmailrecycle[.]com
- answerkangarooclipphoto[.]click
- antiquehomecopperscale[.]click
- anxietyexchangeduck[.]click
- anysheriffgain[.]click
- appearawfulflaggreat[.]com
- applecandyworth[.]click
- applepigladderolympic[.]click
- approvenephewintocatalog[.]click
- arcticfoxrangefatal[.]click
- areadrumrarebrown[.]click
- areamessagetravelmaple[.]com
- areanuclearclosecrystal[.]click
- armoruniversekisstoward[.]online
- armysiegeleft[.]click
- arrivepreferachieve[.]click
- arrowcouplebeachswing[.]online
- arrowpatterndivert[.]click
- artistmangorouteculture[.]click
- artworkthatapproveevidence[.]online
- askabaqeoazq[.]online
- askloopkiwidrastic[.]click
- aspectcamphubwreck[.]click
- aspectvelvetpoleinsane[.]click
- assaulthobbyorientdoctor[.]com
- attendlavacheesesketch[.]click
- augustorientdustmerge[.]click
- authortorchballmoment[.]click
- autumnphonepraise[.]click
- awaredramaimpactdirt[.]click
- awaremediauseful[.]click
- awaytuitionjewelcushion[.]online
- awfulcomicunhappylove[.]click
- bachelorswingheadliberty[.]click
- badgecactusrazor[.]click
- balanceglidetroubledespair[.]click
- bamboomobiletrophystock[.]click
- bamboopotatowishhungry[.]click
- bananaorderinputsustain[.]click
- bardeputyinflictstruggle[.]click
- barrelfalseconvincesword[.]click
- battleguitarnoticeabandon[.]com
- beachbadgerack[.]click
- beachcoconutcropoven[.]click
- beachincludeturtleedit[.]click
- beanbottomblackclever[.]click
- becauseluggagecheckfiscal[.]click
- becomeflightcompanyepisode[.]click
- beefaspectstairscram[.]click
- beefdebrisalphahammer[.]click

Sample Email-Connected Domains

- bestbreed[.]cn
- bestbreed[.]com[.]cn

- megafire[.]cn

Sample IP Addresses

- 104[.]21[.]0[.]106
- 104[.]21[.]0[.]125
- 104[.]21[.]1[.]214
- 104[.]21[.]1[.]224
- 104[.]21[.]1[.]77
- 104[.]21[.]11[.]100
- 104[.]21[.]11[.]87
- 104[.]21[.]12[.]192
- 104[.]21[.]13[.]52
- 104[.]21[.]14[.]42
- 104[.]21[.]15[.]248
- 104[.]21[.]15[.]91
- 104[.]21[.]16[.]145
- 104[.]21[.]16[.]173
- 104[.]21[.]16[.]60
- 104[.]21[.]16[.]67
- 104[.]21[.]17[.]207
- 104[.]21[.]17[.]29
- 104[.]21[.]17[.]92
- 104[.]21[.]18[.]15
- 104[.]21[.]18[.]181
- 104[.]21[.]18[.]188
- 104[.]21[.]18[.]236
- 104[.]21[.]2[.]177
- 104[.]21[.]2[.]240
- 104[.]21[.]2[.]40
- 104[.]21[.]21[.]137
- 104[.]21[.]21[.]31
- 104[.]21[.]21[.]54
- 104[.]21[.]23[.]100
- 104[.]21[.]23[.]162
- 104[.]21[.]23[.]164
- 104[.]21[.]23[.]58
- 104[.]21[.]23[.]90
- 104[.]21[.]24[.]6
- 104[.]21[.]25[.]168
- 104[.]21[.]26[.]253
- 104[.]21[.]26[.]37
- 104[.]21[.]27[.]15
- 104[.]21[.]29[.]153
- 104[.]21[.]29[.]236
- 104[.]21[.]29[.]246
- 104[.]21[.]3[.]146
- 104[.]21[.]30[.]34
- 104[.]21[.]31[.]130
- 104[.]21[.]32[.]131
- 104[.]21[.]32[.]3
- 104[.]21[.]33[.]175
- 104[.]21[.]33[.]49
- 104[.]21[.]34[.]116

Sample IP-Connected Domains

- 1000alternative[.]com
- 24byte[.]com
- a[.]telegra[.]ph
- aabidaqtradingltd[.]com
- abhijeetdesign[.]com
- adangimenez[.]com
- admin[.]telegra[.]ph
- adpcgov[.]com
- aescorpllc[.]com
- africannavigatorsafaris[.]com
- agricorex[.]com
- agrorural[.]mx
- airbacky[.]shop
- aktiifbk[.]com
- ambplc[.]org
- annatob[.]com
- api[.]telegra[.]ph
- app[.]telegra[.]ph

- applyforseo[.]com
- appsocode[.]com
- ardp-gh[.]org
- artembroid[.]com
- artiodactyla[.]net
- artisticembroid[.]com
- autoconfig[.]telegra[.]ph
- autodiscover[.]africannavigatorsafaris[.]com
- autodiscover[.]artiodactyla[.]net
- autodiscover[.]belleloodesigns[.]com
- autodiscover[.]david-boreanaz[.]com
- autodiscover[.]elliebyrddallas[.]com
- autodiscover[.]karriphillips[.]com
- autodiscover[.]needsonclick[.]com
- autodiscover[.]rdgcarpentry[.]co[.]uk
- autodiscover[.]septmax[.]com
- autodiscover[.]telegra[.]ph
- autodiscover[.]tracking[.]septmax[.]com
- axonsystems[.]ai
- ayelmari[.]com
- b[.]telegra[.]ph
- b2pools[.]com
- babyfifi[.]com
- bbs[.]telegra[.]ph
- beauld[.]com
- belinacourier[.]com
- belleloodesigns[.]com
- beta[.]telegra[.]ph
- betterasyouage[.]com
- bienesraiceslisum[.]com
- biotouchcardio[.]com
- biotouchmedical[.]com

Sample String-Connected Domains

- ai-usmcapitalist[.]shop
- ai-usmcollective[.]shop
- ai-usmfence[.]shop
- aifaith[.]church
- aifaith[.]com
- aifaith[.]faith
- aifaith[.]gi
- aifaith[.]live
- aifaith[.]net
- aifaith[.]online
- aifaith[.]org
- aifaith[.]top
- aifaithai[.]com
- aifaithbots[.]com
- aifaithcommunity[.]org
- aifaitherapy[.]com
- aifaitherfu[.]de
- aifaithwear[.]com
- aifaithwear[.]org
- aifaithworks[.]com
- aifaithworks[.]net
- aifaithworks[.]org
- aiprincipal[.]cn
- aiprincipal[.]com
- aiprincipal[.]io
- aiprincipal[.]net
- aiprincipals[.]com
- aireliance[.]co
- aireliance[.]com
- aireliance[.]shop
- aishield[.]agency
- aishield[.]app
- aishield[.]au
- aishield[.]ca
- aishield[.]cloud
- aishield[.]cn
- aishield[.]co
- aishield[.]co[.]uk
- aishield[.]com
- aishield[.]com[.]au

- aishield[.]com[.]cn
- aishield[.]com[.]tw
- aishield[.]de
- aishield[.]email
- aishield[.]eu
- aishield[.]in
- aishield[.]info
- aishield[.]io
- aishield[.]live
- aishield[.]me
- aishield[.]net
- aishield[.]nl
- aishield[.]online
- aishield[.]org
- aishield[.]press
- aishield[.]pro
- aishield[.]ru
- aishield[.]store
- aishield[.]tech
- aishield[.]top
- aishield[.]us
- aishield[.]world
- aishield[.]xyz
- aishield360[.]com
- aishieldcanada[.]org
- aishielded[.]com
- aishielder[.]com
- aishieldforces[.]com
- aishieldglobal[.]com
- aishielding[.]com
- aishieldllc[.]com
- aishieldme[.]com
- aishieldmobile[.]com
- aishieldpro[.]com
- aishieldrs[.]com
- aishields[.]au
- aishields[.]com
- aishields[.]com[.]au
- aishields[.]org
- aishields[.]tech
- aishieldsecurity[.]com
- aishieldspam[.]com
- aishieldtech[.]com
- aishieldusa[.]com
- aishieldx[.]com
- aishieldz[.]com
- aiside[.]ai
- aiside[.]bar
- aiside[.]biz
- aiside[.]cn
- aiside[.]co
- aiside[.]com
- aiside[.]com[.]cn
- aiside[.]cool
- aiside[.]me
- aiside[.]net
- aiside[.]org
- aiside[.]pe
- aiside[.]pw
- aiside[.]ru