2023 Update—How Are the Most-Spoofed Brands Represented in the DNS?

Table of Contents

Executive Report

Even if cyber attack tactics, techniques, and procedures (TTPs) have become increasingly sophisticated over the years, age-old phishing remains the most-used attack vector to this day. In fact, SlashNext detected 255 million phishing attacks over six months in 2022. They detailed their findings in the The State of Phishing Report 2022, which also named some of the most impersonated companies in phishing campaigns.

Building on this list, WhoisXML API researchers sought to uncover, study, and possibly attribute the recently created domains bearing the brand names commonly spoofed in phishing attacks to their owners. Our investigation revealed:

- 12,000+ domains containing the names of the most-impersonated brands and added between 1 January and 5 March 2023
- Only .8% of these cybersquatting domains had WHOIS records that could be publicly attributed to the companies whose names appeared in the domains
- 8,000+ of these properties had active IP resolutions, but only 30 of the IP hosts could be attributed to the spoofed companies
- 6% of the domains were already flagged as malicious

Retrieving Cybersquatting Domains

SlashNext named 18 companies as the most-impersonated global brands. Using Domains & Subdomains Discovery, we found 12,265 domains related to the threat since they contained the brand names registered from 1 January to 5 March 2023. For some companies, we used other targeted text strings to avoid as many false positives as possible.

For example, instead of retrieving all domains containing ***ADP***, we combined it with strings associated with the company, such as ***pay***, ***hr***, ***log***, ***manage***, ***portal***, ***online***, ***employ***, and ***tech***. For Box, we used the company name, alongside ***cloud***, ***support***, ***work***, ***login***, ***account***, and ***signin***.

Furthermore, we only obtained domains that started with the search string for company names that were quite common and began with vowels. The table below shows the search string used for each company and the number of domains we retrieved.

Company Name	Search Strings Used	Number of Domains Found
Adobe	***adobe***	491
ADP	starts with ***adp*** + ***pay***, ***adp*** + ***hr***, ***log***, ***adp*** + ***manage***, ***adp*** + ***portal***, ***adp*** + ***online***, ***adp*** + ***employ***, and ***adp*** + ***tech***	29
Amazon	starts with ***amazon***	2,217
Apple	starts with ***apple***	2,419
Bank of America	***bankofamerica***	141
Box	***box*** + ***cloud***, ***box*** + ***support***, ***box*** + ***work***, ***box*** + ***login***, ***box*** + ***account***, and ***box*** + ***signin***	177
Discord	***discord***	444
DocuSign	***docusign***	24
DropBox	***dropbox***	57
Facebook	***facebook***	429
Google	***google***	1,892
Instagram	***instagram***	584
Microsoft	***microsoft***	852
Netflix	***netflix***	986
PayPal	***paypal***	716
Stripe	***stripe*** + ***pay*** and ***stripe*** + ***process***	10
Wells Fargo	***wellsfargo***	67

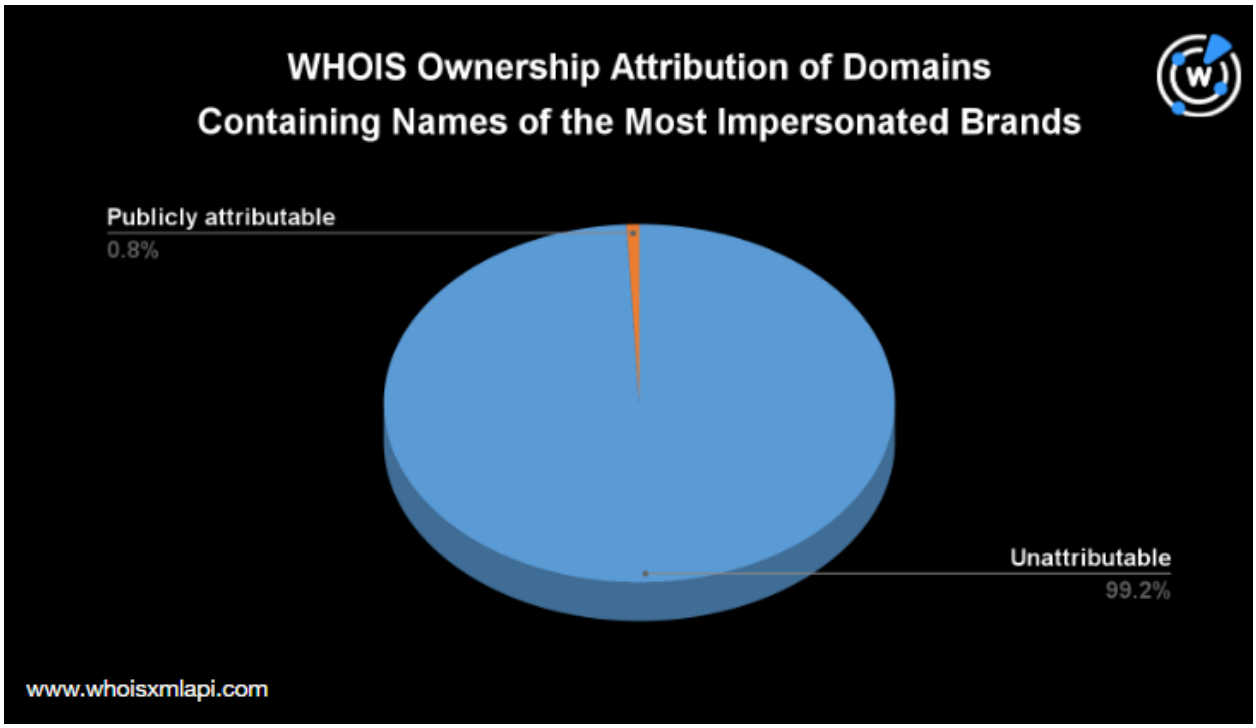
WhatsApp	***whatsapp***	730

WHOIS and IP Host Attribution

Domain attribution effectively distinguishes cybersquatting (and potentially dangerous) domains from a slew of official-looking properties. For this investigation, we analyzed the attribution in two ways—WHOIS ownership and IP address resolution.

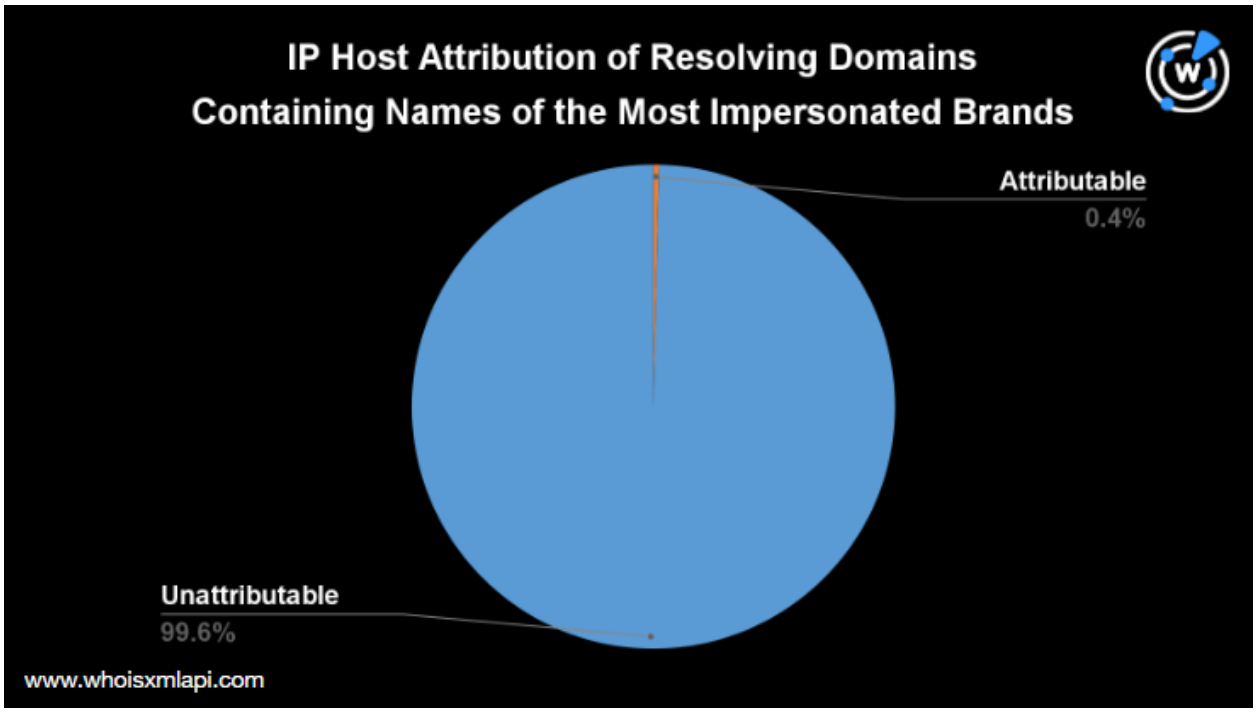
Through Bulk WHOIS API, we determined the registrant organizations of the impersonated companies and the potential cybersquatting domains. All except Discord had public WHOIS records.

Only 97 or less than 1% of the 12,000+ domains in the study could be publicly attributed to the spoofed companies, leaving thousands of cybersquatting domains in the hands of unknown entities.



Our IP resolution analysis yielded a similar outcome. Bulk IP Geolocation API helped us determine that the official domains of the brands in the study resolved to a total of 47 unique IP addresses.

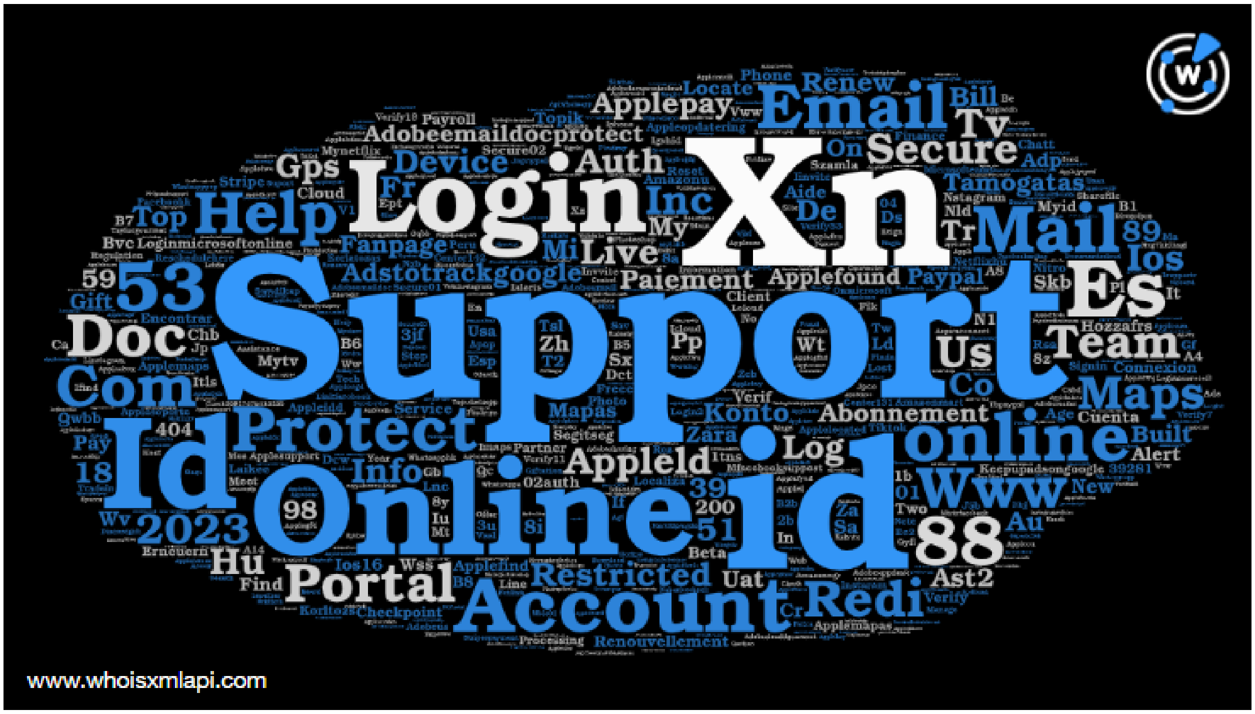
We also found that only about 67% of the recently added cybersquatting domains had active resolutions. However, only 30 (0.4%) of these could be attributed to the companies' IP addresses that hosted their official domains.



Determining Domain Usage through Malware Checks and Screenshot Analyses

Given that most domains couldn't be publicly attributed to the impersonated global brands, we sought to find out if some of them had been reported as malicious.

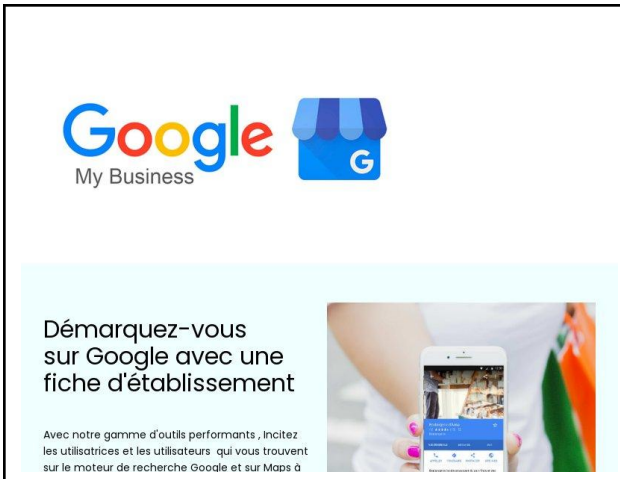
As of 5 March 2023, 6% of the recently added cybersquatting domains were flagged as malicious. Most properties contained strings like ***support***, ***id***, ***online***, ***login***, ***account***, ***email***, and ***help***. The word cloud below shows the common text strings used in the malicious cybersquatting domains.



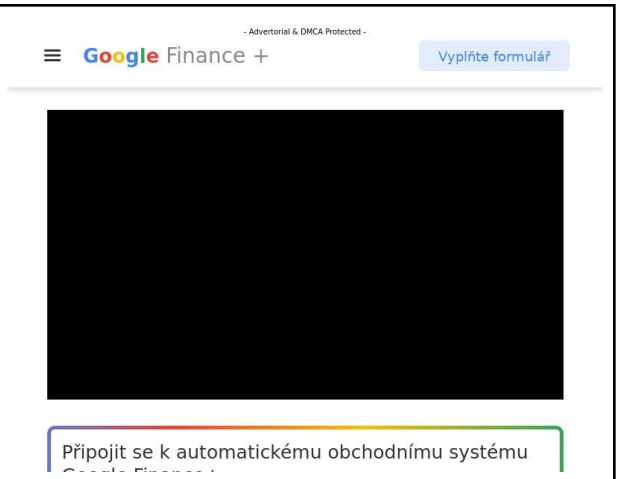
Some of the most notable and recurring string combinations found in the malicious domains were:

- ***adobe-email-doc-protect*** and ***adobemaildocprotect***
- ***appleid***
- ***auth-bankofamerica***
- ***facebook-checkpoint-help-center***
- ***facebook-fanpage-verify***
- ***keepupadsongoogle***
- ***mynetflix***
- ***paypalverifications***
- ***loginmicrosoftonline*** and ***login-microsoftonline***

Screenshot analyses of the malicious properties revealed that some continued to host live websites that were made to look similar to those belonging to the impersonated companies. Below are a few examples.

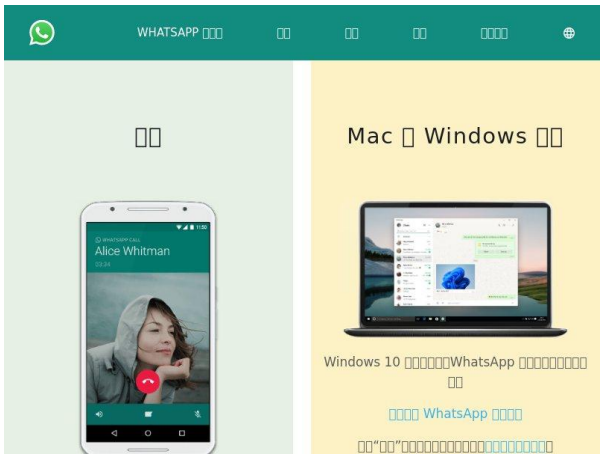


Screenshot of ads-analyticsgoogle[.]com

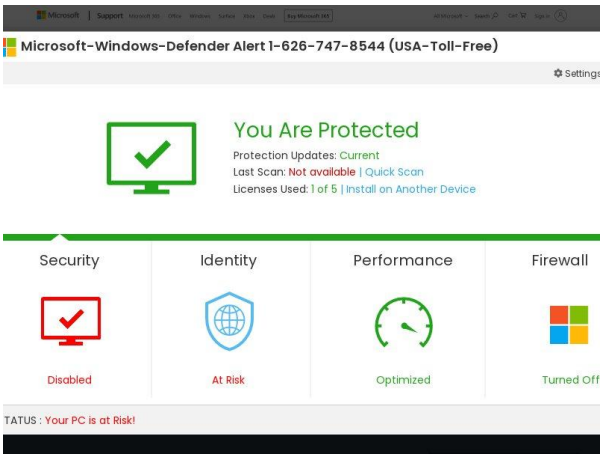


Screenshot of google-finance[.]plus

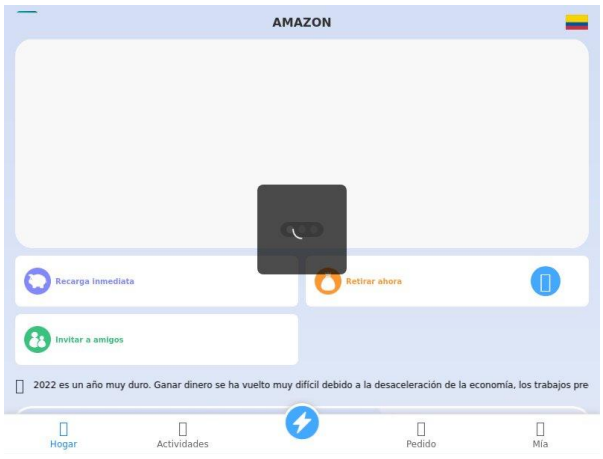
Screenshot of apple-id50colombia[.]live, apple-1tns[.]info and apple-device[.]top



Screenshot of whatsapps-zh[.]com



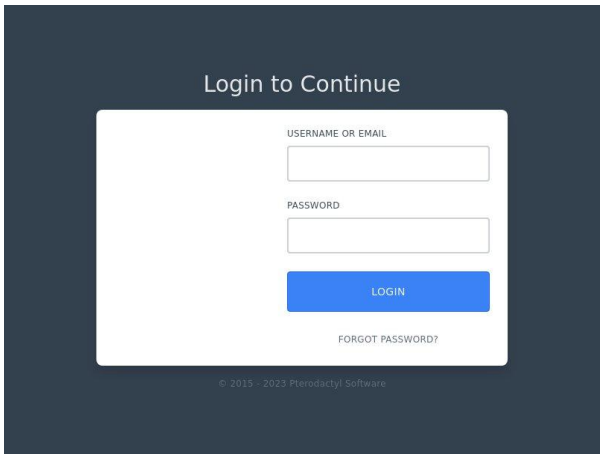
Screenshot of amazonpaymentservices[.]tk



Screenshot of amazonagtcc[.]net

Other malicious domains hosted sites that asked users to provide their login details.

Screenshot of netflix-activation[.]info



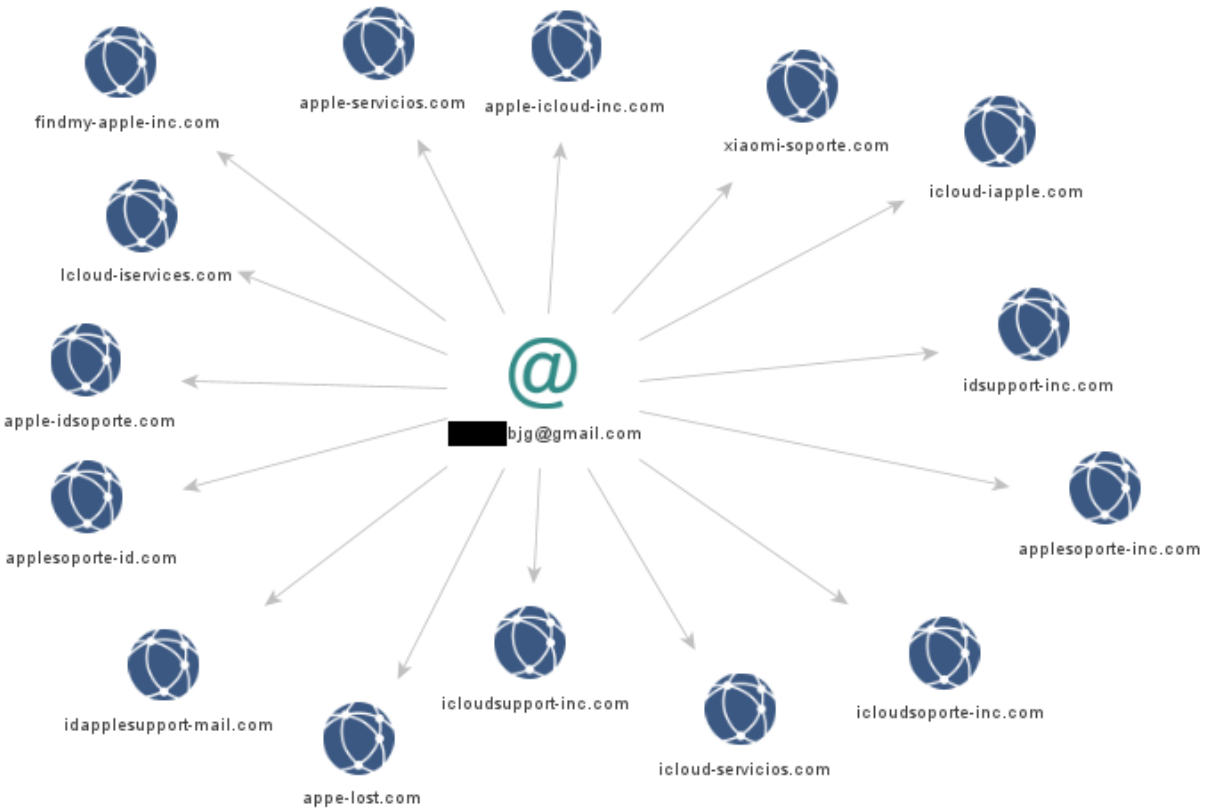
Screenshot of incident-prelevement-netflix[.]com

Screenshot of apple-mystore-portal[.]com

Threat Expansion through WHOIS Associations

The current WHOIS records of the malicious domains led us to 44 unique and unredacted email addresses. Reverse WHOIS searches uncovered 21,116 domains currently registered using the email addresses associated with the malicious domains we found.

An example was the email address used to register the malicious domain applesoporte-id[.]com. We found more than a dozen other domains mostly impersonating Apple. Their relationships are mapped in the following Maltego image.



—

Threat actors will continue to use phishing to gain initial access to target systems. Impersonating global brands like the ones in this report may remain a favorite phishing tactic because of its effectiveness in luring in victims.

Uncovering potential cybersquatting domains targeting these companies can help with real-time threat detection and response, including new domain blocking, threat actor monitoring, and predictive adversary disruption.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample Cybersquatting Domains Created from 1 January to 5 March 2023

- xn--obe-8oa4e[.]vg
- adobe[.]mn
- adobe2[.]app
- adobek[.]com
- iradobe[.]ir
- adobe-l[.]com
- adobeus[.]top
- adobepp[.]com
- adobe-cs[.]cn
- adobenu[.]com
- adobe-t[.]com
- adobeit[.]top
- adobeem[.]xyz
- adobeai[.]art
- adobes[.]blog
- adobe-fa[.]ir
- kadobet[.]art
- adobe-a[.]com
- adobehc[.]com
- adobes[.]shop
- getadobe[.]co
- adobesho[.]ir
- topadobe[.]ru
- adobelso[.]sbs
- wwwwadobe[.]ph
- adobegpt[.]com
- kadobedim[.]ir
- adobe[.]com[.]ng
- adobe[.]org[.]tr
- adobeform[.]sk
- adobefood[.]cn
- adobewtf[.]com
- adobenft[.]app
- mhsadobe[.]org
- adobeposa[.]vg
- hadobey[.]life
- casadobel[.]de
- aadobe[.]space
- adobecdp[.]com
- adpayne[.]ca
- adpaylet[.]com
- adp-payroll[.]online
- adpayrollsolutions[.]com
- adp-plan[.]hr
- adprohrm[.]com
- adpsicologa[.]es
- adptecnology[.]com
- adp-technology[.]com
- adp-psicologia[.]com
- adppropertymanagement[.]com
- adpkportal2023[.]com
- adpp[.]online
- adpuser[.]online
- adpmart[.]online
- adproit[.]online
- adplant[.]online
- adpo-online[.]ru
- adpride[.]online
- adpro-it[.]online
- adpocket[.]online
- adprofile[.]online
- adproonline[.]com[.]ph
- adp-payroll[.]online
- adpropiedades[.]online
- adp-enrollment[.]online
- adp-employ[.]com
- adpvad[.]tech
- adp-technology[.]com
- apple-suspension[.]xyz
- appleustasi[.]net

- applefindst-lnfo[.]cn
- applebaumgroup[.]ca
- apple-ios-59[.]top
- appleidservicecustomer[.]ml
- apple12[.]cf
- apple-findmyphone[.]cloud
- applefynd-mapas[.]cc
- appleandorange[.]top
- apple-lnc-location[.]info
- appleconversion[.]sbs
- applecityenterprise[.]org
- applestudios[.]dev
- applewatchultra[.]com[.]br
- appletonreis[.]com
- appleton-commercials[.]co[.]uk
- applefounds-team[.]live
- applebr-connect[.]in
- apple-etore[.]info
- applewallet-update3782[.]com
- apple-01[.]ru
- applehrmannlondon[.]com
- applefound-team[.]us
- applefound-help[.]live
- applexm[.]top
- applehome[.]com[.]tr
- apple-contact-service[.]com
- appledaxianshen[.]com
- appleteknologies[.]info
- applehitam[.]my[.]id
- apple-world[.]xyz
- apple20[.]ir
- apple8condovilla[.]com
- applefixchile[.]com
- appleiphone000[.]shop
- appledoesnt[.]care
- applesofgoldministries[.]blog
- appletastes[.]com
- amazon-paiement9[.]com
- amazoncomagt[.]com
- amazon24h[.]gq
- amazon-meta[.]com[.]cn
- amazonrelays[.]com
- amazonreley[.]com
- amazonind[.]cc
- amazoniasagrada[.]net
- amazoncowboys[.]com
- amazontoke-unfomuzo[.]life
- amazonquadros[.]com[.]br
- amazonluckybox[.]com
- amazon-go[.]one
- amazonforcollegestudents[.]com
- amazoncrareer[.]com
- amazonstarterkit[.]com
- amazoncontractorsinc[.]com
- amazonsell[.]pro
- amazonupdate66[.]us
- amazonfindsfriday[.]com
- amazoncore10[.]com
- amazonau[.]cc
- amazonjobs[.]ml
- amazonhjjp[.]top
- amazoncz[.]cz
- amazonvine[.]us
- amazonsoft[.]io
- amazonguru2[.]com
- amazonprint[.]in
- amazontrainingdubai[.]com
- amazonstudioservices[.]info
- amazonsellerservices[.]jp
- amazonsalesforyou[.]com
- amazon[.]jl[.]cn
- amazonpricetracker[.]app
- amazonlayoffs[.]com
- amazonlistingsservice[.]com
- amazonguzellik[.]design
- amazoninspireapplication[.]com
- xn--bankfamerca-ldb862b[.]ph
- xn--bankofmeri-x4ae95c[.]ws
- xn--bnkofameric-76ak[.]vg
- xn--bnkofmeri-l2aee18b[.]ws

- xn--bankofmrica-vpb0749g[.]vg
- xn--bankfmeric-l4af5270h[.]ph
- xn--bankfmerica-o7a454b[.]vg
- xn--bankfmerica-18a0460h[.]vg
- xn--bankfmerica-h3c75o[.]ws
- xn--bnkofmeica-q5ae024c[.]vg
- xn--bankofamerc-vyb80s[.]vg
- xn--bnkofmerica-76a963b[.]vg
- xn--bankofmric-mgbe4u[.]ws
- xn--bnkofamerca-x8a85g[.]vg
- xn--bankfameric-ikb0720h[.]vg
- xn--bankfameric-3jd1367g[.]vg
- xn--bnkoamerica-x8a66t[.]ph
- bankofamerica[.]cyou
- xn--bankofamric-v8a5d[.]arab
- xn--nkofamerica-w8a178b[.]arab
- bankofamerica[.]co[.]ma
- bankofamerica-ww[.]ws
- bankofamerica[.]com[.]do
- irpbankofamerica[.]org
- bankofamerica-r8[.]com
- bankofamerica-3b[.]com
- bankofamerica-3u[.]com
- bankofamerica-2b[.]com
- bankofamerica-1b[.]com
- bankofamerica-n1[.]com
- bankofamerica-8m[.]com
- bankofamerica-n3[.]com
- bankofamerica[.]net[.]do
- bankofamerica-3a[.]com
- bankofamerica-8a[.]com
- bankofamerica-n2[.]com
- bankofamerica-4d[.]com
- bankofamerica-5m[.]com
- bankofamerica-8i[.]com
- signingbox[.]de
- signin-xbox[.]com
- designinabox[.]nz
- designinabox[.]eu
- humandesigninabox[.]com
- thedebtbox-signin[.]com
- signin-thedebtbox-com[.]xyz
- www-signin-thedebtbox-com[.]xyz
- upfloginbox[.]com
- winboxlogin[.]net
- boxloginsign[.]com
- dropboxxlogin[.]io
- debtboxlogin[.]com
- loginmailbox[.]org
- h5winbox-login[.]com
- h5-winboxlogin[.]com
- gala-box-login[.]com
- thedebtboxlogin[.]com
- h5-winbox-login[.]com
- login-winbox88[.]com[.]my
- loginid-checkbox-virgilio-mail[.]com
- workboxai[.]work
- debox[.]work
- ccbox[.]work
- boxox[.]work
- catbox[.]work
- workerbox[.]cn
- workerbox[.]id
- realbox[.]work
- myworkbox[.]me
- fritzbox[.]work
- debox[.]network
- boxzippy[.]work
- workboxai[.]com
- workbox[.]today
- storebox[.]work
- worksbox[.]co[.]uk
- timeboxed[.]work
- workdaybox[.]com
- xn--dscord-iwa[.]gg
- xn--dscord-3va[.]co
- discordp[.]tk
- discordp[.]ga
- xn--iscord-v2a[.]com
- discord[.]ong

- discordf[.]ws
- discordp[.]gq
- xn--discrd-6wb[.]com
- discords[.]ca
- xn--dscord-p9a[.]net
- xn--iscord-hyc[.]com
- mdiscord[.]ws
- discordio[.]gq
- discord-d[.]ru
- modiscord[.]nl
- 20discord[.]gg
- stdiscord[.]ml
- discord[.]vodka
- stdiscord[.]com
- discordzh[.]com
- discordai[.]sbs
- discordhq[.]net
- discordt[.]site
- discordb[.]site
- twdiscord[.]com
- ladiscorde[.]me
- discordmod[.]nl
- discordrv[.]com
- mfdiscord[.]com
- discordja[.]com
- discordgo[.]net
- discordsmp[.]it
- discord-2[.]com
- 14discord[.]com
- discord[.]movie
- discordia[.]vip
- discordcdn[.]tk
- discordapp[.]tv
- docusign[.]wang
- docusignz[.]net
- docusigncd[.]info
- fadocusign[.]buzz
- ins-docusign[.]com
- docusign-bbb[.]com
- docudocusign[.]com
- docusignauth[.]life
- 3dns-docusign[.]com
- mytgidocusign[.]com
- docusign-gani[.]com
- docusignnoffice[.]us
- dotlopdocusign[.]xyz
- docusign-login[.]life
- docusignnoffiice[.]xyz
- docusign-staples[.]com
- developerdocusign[.]com
- cekdocusigninweb[.]cloud
- paysecure-docusign[.]com
- docusign-aayandanish[.]com
- docusign-cameronsmith[.]com
- docusignpresidentsclub[.]com
- uwmclosing-docusignin[.]buzz
- docusign-meta-platforms[.]com
- xn--rpbox-6dc2z[.]vg
- 1dropbox[.]org
- 1dropbox[.]xyz
- apidropbox[.]me
- my-dropbox[.]ml
- dropboxai[.]com
- 1dropbox[.]live
- airdropbox[.]de
- 1dropbox[.]info
- dropbox-hr[.]com
- dropbox-id[.]com
- teardropbox[.]de
- dropboxweed[.]ph
- 1dropboxes[.]com
- dropboxdash[.]com
- 1dropbox[.]online
- dropboxauth[.]com
- dropbox-appz[.]ph
- odemedropbox[.]vg
- dropboxplan[.]com
- dropboxwala[.]com
- dropboxsign[.]one
- datadropbox[.]tech

- otherdropbox[.]com
- dropboxplus[.]arab
- dropboxgulpin[.]vg
- honeydropbox[.]com
- eventdropbox[.]com
- dropboxplans[.]com
- lockeddropbox[.]vg
- dropboxxlogin[.]io
- dropbox0pshare[.]us
- oreplydropbox[.]com
- dropboxreplay[.]com
- thedropbox[.]com[.]br
- dropbox-plans[.]com
- dropbox-mobile[.]com
- dropboxlive[.]com[.]au
- dropboxinvoice[.]com
- facebook[.]wf
- xn--faboo-5xa8ftm[.]eu
- xn--fcbk-loa5a0ga[.]com
- facebookx[.]uk
- facebook1[.]ml
- facebook33[.]xn--fiqz9s
- facebookip[.]ml
- xn--fcebk-rqa8574ca[.]arab
- frfacebook[.]ga
- facebookk[.]ink
- okfacebook[.]top
- w3facebook[.]com
- facebookimp[.]cf
- facebook-lg[.]ml
- facebookzh[.]net
- facebook-ly[.]gq
- facebook-24[.]de
- facebookons[.]tv
- facebookis[.]gay
- sssfacebook[.]io
- onsfacebook[.]co
- facebookk[.]wiki
- facebookzh[.]org
- facebookons[.]nl
- awfacebook[.]com
- zkfacebook[.]com
- facebook-05[.]ga
- facebooke[.]shop
- ad-facebook[.]co
- facebookf2f[.]vg
- sinfacebook[.]ml
- facebookwplo[.]cf
- okfacebookno[.]ga
- facebookmeta[.]nl
- facebook333[.]com
- gmafacebook[.]com
- nexfacebookp[.]ml
- facebookmart[.]co
- nofacebookca[.]ml
- google-googleads[.]cn
- xn--gle-whb40aa[.]ph
- xn--ggle-v0ba[.]gq
- xn--goge-5qa45t[.]vg
- xn--ogle-qqa80t[.]vg
- google9[.]gq
- xn--google-2ua[.]it
- googlep[.]cn
- googler[.]io
- xn--ggl-mra11la[.]com
- xn--goge-21a8d[.]com
- egoogle[.]ir
- ogoogle[.]es
- google1[.]ga
- xn--goge-rqa98b[.]com
- googleb[.]ml
- 4google[.]in
- google7[.]ga
- googlepv[.]ga
- hogoogle[.]ml
- argoogle[.]cn
- 9google[.]net
- nogoogle[.]ml
- googlepv[.]cf
- kkgoogle[.]de

- googlepv[.]gq
- 4google[.]org
- googlepv[.]ml
- aigoogle[.]co
- 4google7[.]cn
- googlee[.]ink
- djgoogle[.]ga
- mygoogle[.]au
- googlefp[.]in
- googlele[.]cn
- googleai[.]us
- googleyh[.]cn
- dcgoogle[.]nz
- xn--ogle-9wa43n[.]arab
- instagram-instagram-instagram-instagram--shop-instagram[.]gq
- instagram-instagram-online-instagram[.]ml
- xn--instgrm-8wa22s[.]vg
- xn--instaram-chb[.]net
- instagramm[.]uz
- xn--insagram-ryb[.]com
- dinstagram[.]ws
- instagramn[.]ws
- xn--nstagram-skb[.]dev
- instagramo[.]vg
- instagramdo[.]es
- joinstagram[.]ph
- instagramcf[.]ga
- instagramny[.]ws
- tvinstagram[.]co
- oninstagram[.]ca
- iinstagramu[.]ws
- xn--instagm-2wa497a[.]arab
- instagramme[.]ws
- m3instagram[.]ws
- instagramgo[.]ga
- cginstagram[.]ph
- instagramin[.]vg
- doginstagram[.]nl
- wvinstagram[.]com
- instagramsex[.]de
- instagramoz[.]com
- zkinstagram[.]com
- instagram-il[.]ws
- my-instagram[.]cf
- instagramail[.]ml
- foinstagram[.]com
- instagram360[.]ir
- instagramer[.]icu
- instagramer[.]cfd
- ocinstagram[.]com
- en-instagram[.]ml
- phinstagram[.]com
- neinstagram[.]com
- xn--mcrosoft-c2a[.]be
- microsoft[.]ky
- xn--mcrosoft-c2a[.]fr
- xn--icrosft-e1a7168d[.]vg
- mx[.]microsoft
- xn--mirsoft-35a34x[.]ph
- microsoft[.]xn--kprw13d
- int[.]microsoft
- microsofte[.]top
- microsofts[.]ltd
- mymicrosoft[.]ml
- gomicrosoft[.]id
- rmicrosofts[.]com
- microsoftss[.]com
- microsoftjs[.]top
- microsoft365[.]ms
- xn--microsft-b5a[.]works
- microsoft366[.]fr
- yymicrosoft[.]top
- microsoft365[.]ai
- microsoft[.]qh[.]cn
- 365microsoft[.]cf
- microsofthup[.]lu
- aimicrosoft[.]net
- microsoft365[.]nz

- microsoftis[.]gay
- microsoftgpt[.]com
- microsoftmesh[.]cn
- email-microsoft-365-onmicrosoft[.]com
- microsoftshop[.]pk
- xn--mcrosoft-21a[.]online
- microsofthelp[.]in
- microsoft-ikb[.]at
- omgmicrosoft[.]com
- microsoft20t[.]com
- microsoftgbt[.]com
- microsoft180[.]com
- microsoftdlp[.]com
- microsoftups[.]top
- netflixh[.]cc
- netflixe[.]cc
- enetflix[.]fr
- netflixe[.]me
- netflixcn[.]ga
- mynetflix[.]ru
- ynetflix[.]xyz
- netflixpr[.]cc
- netflixjr[.]tv
- netflixcn[.]ml
- netflixw[.]xyz
- netflixcn[.]cc
- netflixcl[.]cl
- netflixcn[.]tv
- netflix11[.]ir
- mynetflix[.]nl
- netflixpx[.]pw
- netflixlg[.]cc
- xn--ntfix-j0a28u[.]arab
- netflixxx[.]tv
- netflixe[.]icu
- yanetflix[.]me
- netflixal[.]fun
- netflixcom[.]pl
- my-netflix[.]de
- netflixmk[.]xyz
- paynetflix[.]fr
- netflixsub[.]ml
- v1-netflix[.]pl
- yanetflix[.]org
- netflix-cy[.]cf
- netflixad[.]com
- thenetflix[.]co
- netflixrf[.]ink
- netflixe[.]buzz
- netflixmlm[.]fr
- netflixhp[.]com
- netflixe[.]cyou
- netflix[.]music
- paypal[.]st
- xn--papal-rva[.]vg
- xn--ppl-9kal6o[.]ws
- xn--paypa-rnb[.]vg
- xn--ppl-9kal6o[.]vg
- xn--pypal-rwa[.]ph
- xn--papl-2na8p[.]ph
- xn--paypa-rnb[.]ws
- xn--aypal-ipb[.]vg
- xn--pypl-0nac[.]ph
- xn--papl-6ra3466b[.]vg
- cpaypal[.]in
- paypall[.]xn--fiqs8s
- paypals[.]su
- paypal-x[.]hk
- xn--paypa-we3s[.]arab
- paypalll[.]it
- paypalcn[.]top
- ampaypal[.]com
- paypalv1[.]com
- uspaypal[.]xyz
- mmpaypal[.]xyz
- paypal-iv[.]vg
- mppaypal[.]com
- nftpaypal[.]cn
- paypalnow[.]ph

- japaypal[.]com
- dapaypal[.]com
- fupaypal[.]com
- llpaypal[.]com
- newpaypal[.]co
- paypalr[.]info
- paypalinc[.]gq
- buypaypal[.]io
- tbpaypal[.]com
- paypalzh[.]net
- paypalzh[.]com
- paypalkart[.]ws
- xn--paypa-we3s[.]net[.]ph
- stripetappay[.]com
- paymentstripes[.]com
- stripespayment[.]online
- stripespayments[.]online
- stripepaymenttest112[.]ws
- stripe-processing[.]pw
- stripe-processing[.]site
- stripe-processing[.]space
- stripe-processing[.]online
- stripe-processing[.]foundation
- xn--wllsfarg-b1a1k[.]com
- su-wellsfargo[.]ml
- wellsfargoi[.]live
- iswellsfargo[.]com
- wellsfargoltd[.]com
- wellsfargo-sec[.]ru
- wellsfargoq[.]email
- wellsfargo-fu[.]com
- jv-wellsfargo[.]com
- wellsfargogpt[.]com
- sb-wellsfargo[.]com
- id-wellsfargo[.]com
- wellsfargo-bnk[.]com
- wellsfargoesco[.]com
- wellsfargoswift[.]com
- wellsfargovcnsc[.]com
- wire-wellsfargo[.]com
- wellsfargobank1[.]com
- wellsfargoescono[.]com
- creditwellsfargo[.]com
- wellsfargoessosc[.]com
- wellsfargoalert[.]info
- wellsfargovesvus[.]com
- wellsfargosecure[.]top
- wellsfargo-texas[.]com
- wellsfargocollgle[.]com
- wellsfargo-fraud[.]help
- wellsfargosecveri[.]com
- wellsfargoscredit[.]com
- wellsfargowordfind[.]ph
- wellsfargoservlce[.]com
- wellsfargolifestory[.]ws
- secure-wellsfargon[.]com
- wellsfargo-verify[.]info
- wellsfargocomgogle[.]com
- supportswellsfargo[.]com
- wellsfargolifesync[.]com
- wellsfargomail[.]support
- secure-wellsfargo[.]help
- whatsapp[.]au
- xn--whatspp-t4a[.]com
- whatsapp6[.]cf
- whatsapps[.]la
- whatsappu[.]us
- xn--whatsap-j53c[.]com
- whatsappo[.]co
- whatsappe[.]us
- cwhatsapp[.]io
- cwhatsapp[.]me
- bwhatsapp[.]me
- whatsappq[.]ml
- iwhatsapp[.]ca
- whatsappgb[.]pk
- whatsappi[.]app
- xn--whtsapp-bn4c[.]arab
- uswhatsapp[.]me
- whatsappai[.]in

- whatsappv[.]ink
- whatsappu[.]ink
- whatsappa[.]ink
- ogwhatsapp[.]cc
- whatsappz[.]ink
- cwhatsapp[.]xyz
- gbwhatsapp[.]cn
- whatsappx[.]ink
- c-whatsapp[.]me
- gowhatsapp[.]io
- whatsappwe[.]de
- c-whatsapp[.]io
- whatsapptv[.]ng
- mywhatsapp[.]ga
- okwhatsapp[.]me
- mywhatsapp[.]pk
- whatsappwy[.]cn
- whatsappc[.]ink
- xwhatsapp[.]org
- jtwhatsapp[.]co
- whatsappa[.]top

Sample Malicious Cybersquatting Domains as of 5 March 2023

- adobe-a[.]com
- wv-adobe[.]top
- adobeemail[.]com
- www-adobeus[.]top
- adobeappdesk[.]com
- www-adobe-com[.]top
- adobeemaildoc[.]com
- adobesharing[.]online
- adobe-photoshop[.]top
- adobeclouddocument[.]com
- adobedocumentscloud[.]ga
- adobe-herunterladen[.]de
- adobe-documentscloud[.]ga
- adobeemaildocprotect[.]ink
- adobeemaildocprotect[.]com
- adobeemaildocprotect[.]tech
- adobeemaildocprotect[.]info
- adobeemaildocprotect[.]email
- adobereader-secured[.]online
- adobeemaildocprotect[.]online
- adobe-email-doc-protect[.]org
- adobe-email-doc-protect[.]com
- adobe-email-doc-protect[.]pro
- adobe-email-doc-protect[.]ink
- adobe-email-doc-protect[.]info
- adobe-email-doc-protect[.]tech
- adobeemaildocprotect[.]digital
- adobe-email-doc-protect[.]email
- teststripdropbox[.]com
- stripespayment[.]online
- stripe-processing[.]site
- stripe-processing[.]space
- adp-payroll[.]online
- adp-payroll[.]online
- www-facebook[.]vn
- facebookk[.]com[.]vn
- help-facebook[.]co
- mtrtrfacebook[.]com
- zara-facebook[.]com
- linkfacebook[.]buzz
- facebookes[.]online
- zara-facebook[.]co[.]in
- m-m-facebook[.]com[.]tr
- kabarfacebook[.]my[.]id
- m-tr-facebook[.]com[.]tr
- mfacebooksuppost[.]site
- facebooksecurityit[.]com
- mfacebooksuppost[.]click
- facebook-beta-live[.]com
- facebook-swadikap[.]site
- facebookonline[.]business
- facebookmetabussiness[.]com
- facebook-fanpage-verify7[.]ga
- facebook-fanpage-verify33[.]ga

- facebook-fanpage-verify11[.]ga
- facebook-fanpage-verify18[.]ga
- facebook-checkpoint-help-center142[.]ga
- facebook-checkpoint-help-center131[.]ga
- facebook-checkpoint-case100917476410205[.]com
- xn--instaram-chb[.]net
- xn--nstagram-skb[.]dev
- voteinstagram[.]ru
- age-instagram[.]com
- linstagram[.]com[.]tr
- instagrambeybit[.]com
- instagrambaybit[.]com
- theinstagramclub[.]com
- instagramreferse[.]com
- www-instagram-com[.]tk
- verifyinstagram[.]com[.]tr
- instagramappeal[.]com[.]tr
- xn--nstagram-security-bvc[.]com
- instagrammmmmmmmga[.]cfd
- instagram-connexion[.]live
- instagramhelpcenteral[.]ml
- instagram-instagram-p-hsrkfdpmgdn-igshid-nzg7hkl1ngl[.]cf
- instagramguidelines[.]online
- instagramforbusines[.]com[.]tr
- sharepictureshop-instagram[.]com
- tiktok-instagram-laikee-freee[.]site
- whatsappa[.]top
- whatsapphk[.]com
- topwhatsapp[.]in
- whatsapp-wt[.]com
- whatsapp-pp[.]com
- whatsapppop[.]net
- whatsappaapp[.]com
- whatsappaatt[.]com
- whatsapp-wss[.]com
- whatsapps-zh[.]com
- apiwhatsapp[.]co[.]in
- whatsapp-apap[.]com
- whatsapp-chatt[.]xyz
- whatsapp-reset[.]info
- whatsapp-iinvite[.]xyz
- whatsapp-invvite[.]xyz
- whatsapp-two-step[.]info
- chatwhatsapplulu[.]my[.]id
- japaypal[.]com
- tbpaypal[.]com
-

Sample Domains Connected to Malicious Cybersquatting Domains by Registrant Email Address

- aiksexchange[.]com
- axieinfinity-box[.]com
- bizoucoin[.]com
- coinsqu[.]com
- conesproject[.]com
- conesprojectdr[.]com
- conesprojectdrs[.]com
- csgo-dropskins[.]com
- csgo-freeskin[.]com
- csgo-freeskins[.]com
- csgocasec[.]com
- csgodrop-skins[.]com
- csgofree-skins[.]com
- csgorunc[.]com
- dicsord-gs[.]com
- dicsord-ni[.]com
- discord-steami[.]com
- discordair[.]com
- discordairdrops[.]com
- discordi-boost[.]com

- discordi-nitro[.]com
- discordiairdrop[.]com
- discordiboost[.]com
- discordinitro[.]com
- discordinitroi[.]com
- discordj-boost[.]com
- discordj-steam[.]com
- discordjairdrop[.]com
- discordjnitro[.]com
- discordjsteam[.]com
- discordl-nitro[.]com
- discordlairdrop[.]com
- discordlboost[.]com
- discordlnitro[.]com
- discordnitroi[.]com
- discordnltroi[.]com
- discordnltros[.]com
- discords-news[.]com
- discordsteamc[.]com
- discordsteamf[.]com
- discordsteami[.]com
- discordsteamj[.]com
- discordsteaml[.]com
- discordsteamr[.]com
- discordstean[.]com
- discrod-steam[.]com
- diusnx[.]com
- djscordairdrop[.]com
- djscordbasic[.]com
- djscordiairdrop[.]com
- djscordjboosts[.]com
- djscordlboosts[.]com
- djscordnitro[.]com
- djscordnltro[.]com
- djscordsteam[.]com
- dliscordsteam[.]com
- dlscord-news[.]com
- dlscordairdropi[.]com
- dlscordairdropl[.]com
- dlscordairdrops[.]com
- dlscordalrdrop[.]com
- dlscordbasic[.]com
- dlscordchat[.]com
- dlscordchats[.]com
- dlscordgid[.]com
- dlscordi-steam[.]com
- dlscordiairdrop[.]com
- dlscordialrdrop[.]com
- dlscordiboost[.]com
- dlscordiboosts[.]com
- dlscordisteam[.]com
- dlscordjairdrop[.]com
- dlscordjboosts[.]com
- dlscordjbost[.]com
- dlscordjsteam[.]com
- dlscordl-boost[.]com
- dlscordl-nitro[.]com
- dlscordlairdrop[.]com
- dlscordlboost[.]com
- dlscordlboosts[.]com
- dlscordlnitro[.]com
- dlscordlsteam[.]com
- dlscordnitroi[.]com
- dlscordsteami[.]com
- dlscorldnews[.]com
- dlscorldsnew[.]com
- facepunch-rusts[.]com
- ggcscase[.]com
- ggcscases[.]com
- gimsexchange[.]com
- hilexchange[.]com
- klinexchange[.]com
- navicase-steam[.]com
- nitro-airdrop[.]com
- nitrolsteam[.]com
- nitrosteamf[.]com
- nitrosteami[.]com
- nitrosteamj[.]com
- nitrosteaml[.]com
- nitrosteamt[.]com

- nitrrosteam[.]com
- nltrosteam[.]com
- qufrex[.]com
- raisexchange[.]com
- reimexchange[.]com
- rensexchange[.]com
- rust-giveaway[.]com
- rust-roulettes[.]com
- rust-roullete[.]com
- rustcasec[.]com
- rustfacepuchs[.]com
- rustgiveaways[.]com
- rustrouletle[.]com
- rustroulettec[.]com
- rustroulettes[.]com
- rustroullette[.]com
- rusts-case[.]com
- rusts-cases[.]com
- rusts-facepunch[.]com
- rustscases[.]com
- rustsfacepunch[.]com
- ruxexchange[.]com
- s1mple-csgo[.]com
- s1mplenavipro[.]com
- scl-tournament[.]com
- scl-tournaments[.]com
- steam-airdrop[.]com
- steam-airdrops[.]com
- steam-alrdrop[.]com
- steam-nitrol[.]com
- steamairdrop[.]com
- steamairdrops[.]com
- steamalrdrop[.]com
- steamcommunijy[.]com
- steamcommunitp[.]com
- steamcommunity-nitro[.]com
- steamconmmunjty[.]com
- steamdiscorda[.]com
- steamdiscordc[.]com
- steamdiscordp[.]com
- steamdiscordt[.]com
- steamdiscordx[.]com
- steamdiscordy[.]com
- steamdjscord[.]com
- steamdlscordi[.]com
- steamfdiscord[.]com
- steamfnitro[.]com
- steamidiscord[.]com
- steamidiscordi[.]com
- steamjdiscord[.]com
- steamjnitro[.]com
- steamlnitro[.]com
- steamniitro[.]com
- steamnitrof[.]com
- steamnitroi[.]com
- steamnitroj[.]com
- steamnitrol[.]com
- steamnitrro[.]com
- steamsdiscordl[.]com
- steamtnitro[.]com
- steancommunijy[.]com
- steancommunjty[.]com
- steancommunltys[.]com
- steanconmmunlty[.]com
- steanconmunjty[.]com
- steanconmunlty[.]com
- stleamgifts[.]com
- teslaexchang[.]com
- twitch-bonuse[.]com
- vesnexchange[.]com
- auth-paiement[.]fr
- netfiix-paiement-client[.]fr
- netflix-paiement-client[.]fr
- verification-proprietaire[.]fr
- account-deviceid[.]us
- account-idalerts-log[.]us
- alert-fmimx[.]us
- alerts-find-phone[.]us
- alerts-finder-id[.]us
- alerts-finder-idd[.]us

- alerts-fmi-idd[.]us
- alerts-ilocations-idd[.]us
- app-ios-16[.]us
- app-lcloud-id[.]us
- appieid-support[.]us
- apple-alertid-findmy[.]us
- apple-alertld-findmy[.]us
- apple-ilocations-alerts[.]us
- appleid-phone-fmi[.]us
- check-id-support[.]us
- check-located[.]us
- check-location-support[.]us
- device-fmi-alertid[.]us
- device-support-id[.]us
- find-device-alert[.]us
- finder-recovery[.]us
- findmy-lcloud-alerts[.]us
- fmi-idevice-alert[.]us
- fmi-support-idcloud[.]us
- fmi-support-ldcloud[.]us
- icloud-maps-is[.]us
- icloud-sing[.]us
- idd-phone-alerts[.]us
- iforgot-cloud[.]us
- ilocated-cloud-secure[.]us
- iphonesupport-findmy[.]us
- isupport-alert-fmi[.]us
- lcloud-devices-login[.]us
- lcloud-findmy-idd[.]us
- lcloud-i-secure[.]us
- lcloud-info-io[.]us
- lcloud-info-p[.]us
- lcloud-lphone-idd[.]us
- lcloud-maps-00[.]us
- lcloud-ofcial-es[.]us
- lcloud-slng[.]us
- lcloud-support-ld[.]us
- siri-location[.]us
- support-alert-login[.]us
- support-cloud-phone[.]us
- support-idd-phone[.]us
- support-idd[.]us
- support-location-phone[.]us
- www-lcloud-es[.]us
- support-restriction-netflix[.]fr
- deskarez[.]fr
- dhl-lieferung[.]fr
- disneyplus-compte[.]fr
- envoie-chronopost[.]fr
- envoie-chronpost[.]fr
- france-netflix[.]fr
- netfix-service[.]fr
- netflix-cloturation[.]fr
- netflix-rez[.]fr
- abrasivewheelsinvestigation[.]com
- advancedautoinvestigation[.]com
- aerospaceengineersinvestigation[.]com
- alaskaairlinesflightattendantsinvestigation[.]com
- amazonclassactioninvestigation[.]com
- amazonrelayinvestigation[.]com
- americanpoolenterprisesinvestigation[.]com
- amphenolhollandhaloinvestigation[.]com
- amphenolhollhaloinvestigation[.]com
- amyskitcheninvestigation[.]com
- apparelbranddatabreach[.]com
- arizonapublicserviceretireesinvestigation[.]com
- arizonapublicservicesretireesinvestigation[.]com
- autumnlakehealthcareinvestgation[.]com
- autumnlakehealthcareinvestigation[.]com
- babyformulainvestigation[.]com
- bankemployeesinvestigation[.]com

- bankinginvestigation[.]com
- bankofamericainvestigation[.]com
- bankwageinvestigation[.]com
- bauschinvestigation[.]com
- baystatehealthinvestigation[.]com
- beachbodyinvestigation[.]com
- bectondickinsoninvestigation[.]com
- beveragedistributionlawsuit[.]com
- bigeasyinvestigation[.]com
- bloomberglpinvestigation[.]com
- blueshielddatabreachinvestigation[.]com
- boiselistingexperts[.]com
- bonefishgrillinvestigation[.]com
- brenntaginvestigation[.]com
- brgrkitcheninvestigation[.]com
- brookfieldinvestigation[.]com
- californiatravelnursesinvestigation[.]com
- calspasofsacramento[.]com
- canaminvestigation[.]com
- carpetcleanerfortrumpsupporters[.]com
- carrabbasinvestigation[.]com
- cascadebehavioralhealthinvestigation[.]com
- catalinacrunchinvestigation[.]com
- centralwashingtonhospitalinvestigation[.]com
- childrenshospitalinvestigation[.]com
- citibankemployeeinvestigation[.]com
- conocophillipinvestigation[.]com
- conocophillipsinvestigation[.]com
- cookgroupinvestigation[.]com
- corelogicinvestigation[.]com
- cpaporbipapinvestigation[.]com
- cruiselineinvestigation[.]com
- databreachinvestigation[.]com
- databreachsinvestigation[.]com
- dbschenkerinvestigation[.]com
- dbschenkersinvestigation[.]com
- densoinvestigation[.]com
- devsiteone[.]com
- dignityhealthinvestigation[.]com
- dnadiagnosiscenterinvestigation[.]com
- dnadiagnosticscenterinvestigation[.]com
- dottyscasinoinvestigation[.]com
- doughertyfraudrecovery[.]com
- doverinvestigation[.]com
- drivtennecoinvestigation[.]com
- drunkenfishinvestigation[.]com
- dupontinvestigation[.]com
- ecigaretteinvestigation[.]com
- ecsiinvestigation[.]com
- elsuperinvestigation[.]com
- emeresthealthinvestigation[.]com
- emergencyroomchargesinvestigation[.]com
- employeejusticeinvestigation[.]com
- eskenazihealthinvestigation[.]com
- federalworkersinvestigation[.]com
- fedexpilotsinvestigation[.]com
- fergusonenterprisesinvestigation[.]com
- fiservinvestigation[.]com
- fismanagementservicesinvestigation[.]com
- fitsodainvestigation[.]com
- flightclubinvestigation[.]com
- flyingjinvestigation[.]com
- generalmillsinvestigation[.]com
- georgiafarmbureauinvestigation[.]com
- gerberinvestigation[.]com
- greatwolflodgeinvestigation[.]com
- greyhoundinvestigation[.]com
- guardianemployees[.]com
- hanesbrandinvestigation[.]com

- hanesbrandsinvestigation[.]com
- hatchgreenchilesinvestigation[.]com
- hclamericainvestigation[.]com
- headfraudrecovery[.]com
- healthdatabreachinvestigation[.]com
- homedepotinvestigation[.]com
- homedepotrentalinvestigation[.]com
- homedepotrentalsinvestigation[.]com
- hondacivicinvestigation[.]com
- hospitalityinvestigation[.]com
- hyattemployeeinvestigation[.]com
- infosystechnologyinvestigation[.]com
- innerecobrandinvestigation[.]com
- instaworkinvestigation[.]com
- iongroupinvestigation[.]com
- itwinvestigation[.]com
- jewelersinvestigation[.]com
- jinchungfraudrecovery[.]com
- johnhopkinshospitalinvestigation[.]com
- kayserrothinvestigation[.]com
- kombuchainvestigation[.]com
- kronoscloudinvestigation[.]com
- kwiktripinvestigation[.]com
- lawrencekiainvestigation[.]com
- lesterfraudrecovery[.]com
- lgdishwasersinvestigation[.]com
- lhcgroupincinvestigation[.]com
- lifeinsuranceinvestigation[.]com
- lifesettlementlawyer[.]net
- livekombuchainvestigation[.]com
- livenationinvestigation[.]com
- logisticsinvestigation[.]com
- luxeroneinvestigation[.]com
- massachusettsgeneralhospitalinvestigation[.]com
- masterlockinvestigation[.]com
- masterlocklawsuitinvestigation[.]com
- masterlockpucklockinvestigation[.]com
- mcmenaminsinvestigation[.]com
- mealandbreakinvestigation[.]com
- michaelsweaneyfraud[.]com
- misclassifiedbpa[.]com
- mitsubishichemicalamericainvestigation[.]com
- monsterenergyinvestigation[.]com
- neopetsdatabreachinvestigation[.]com
- nokiainvestigation[.]com
- northshoreinvestigation[.]com
- nowstainvestigation[.]com
- nurseinvestigation[.]com
- nursesinvestigation[.]com
- nvidiashieldinvestigation[.]com
- oilrefineryinvestigation[.]com
- paralegalservicesbakersfield[.]com
- pepsicoinvestigation[.]com
- pfizerpensioninvestigation[.]com
- phosphatidylserineinvestigation[.]com
- polarisatvlawsuit[.]com
- polarislawsuit[.]com
- ppaholdingsincinvestigation[.]com
- ppaholdingsinvestigation[.]com
- prisonerrightsinvestigation[.]com
- profilecabinetstoneanddesigninvestigation[.]com
- progressresidentialinvestigation[.]com
- qwickinvestigation[.]com
- reimersfraudrecovery[.]com
- retailinvestigation[.]com
- reynoldsinvestigation[.]com
- riteaidinvestigation[.]com
- rrdonnelleyinvestigation[.]com

- sexualassaultinvestigation[.]com
- shamrockcabinetinvestigation[.]com
- sherwinwilliamsinvestigation[.]com
- sikacorporationinvestigation[.]com
- silversaddleranchinvestigation[.]com
- smartmlsinvestigation[.]com
- southerncompanyinvestigation[.]com
- sprintinvestigation[.]com
- sprintpensioninvestigation[.]com
- statefarminsurnacecancellationinvestigation[.]com
- stewartoaks[.]com
- stksteakhouseinvestigation[.]com
- summitgrillinvestigation[.]com
- swedishmedicalcenterinvestigation[.]com
- targetdistributioncentersinvestigation[.]com
- techdatabreachinvestigation[.]com
- tenofovirdruginvestigation[.]com
- tenofovirinvestigation[.]com
- textmessageinvestigation[.]com
- traderjoesinvestigation[.]com
- trainderailmentinvestigation[.]com
- transdiginvestigation[.]com
- travelnursesinvestigation[.]com
- unitedimportsinvestigation[.]com
- universityandcollegeinvestigation[.]com
- universityandcollegeinvestigations[.]com
- universityofthepacificinvestigation[.]com
- untuckitinvestigation[.]com
- usbankinvestigation[.]com
- utilitytreeserviceinvestigation[.]com
- v8splashinvestigation[.]com
- vacationhomeinvestigation[.]com
- venturafoodsinvestigation[.]com
- wageviolationinvestigation[.]com
- walkerfraudrecovery[.]com
- wecenergygroupinvestigation[.]com
- westernunionrefund[.]com
- westernunionrefundinvestigation[.]com
- winitamericainvestigation[.]com
- wymansblueberryinvestigation[.]com
- zeezeesinvestigation[.]com
- auth-mygov-au[.]com
- bellco-msg[.]com
- h-export-machinery[.]com
- help-mygov-au[.]com
- hexport-machinery[.]com
- mypostal-update[.]com
- mytruist-alerts[.]com
- netflix-msgs[.]com
- stcu-alerts-msg[.]com
- track-mypostal[.]com
- truist-cs[.]com
- usbank-msgs[.]com
- yhbkhvjcdgswrwzhfcgvh[.]com
- accounts-flndmy[.]us
- apple-alerts[.]us
- apple-in[.]us
- apple-l[.]us
- apple-lcloud[.]us
- applefindmys[.]us
- appleflndmys[.]us
- applesupporteds[.]us
- esupports-findmy[.]us
- find-alert[.]us
- findmaps-icloud[.]us
- findmy-sopport[.]us
- findmylphones[.]us
- flndmysupports[.]us
- fnd-info[.]us
- icioud-flndmy[.]us
- icloud-ec[.]us
- icloud-myfinds[.]us

- isupport-findmyld[.]us
- isupports-flndmys[.]us
- juankksjajaj[.]us
- lcioud-ec[.]us
- lcloud-fndmy[.]us
- locate-arg[.]us
- lssuport-fndmy[.]us
- lsupport-flndmys[.]us
- lsupporteds-findmys[.]us
- mi-find[.]us
- support-findmys[.]us
- supported-find[.]us
- supported-id[.]us
- supportid-alert[.]us
- 006-robinhood[.]com
- 01authe[.]com
- 0nesimages[.]com
- 0vacl0set[.]com
- 1001krepays12120mofortherestofyourlife[.]com
- 10zpov[.]com
- 1100entertainment[.]com
- 11starr[.]com
- 1218craftworks[.]com
- 124proprint[.]com
- 144knation[.]com
- 16andabeat[.]com
- 16lauramargaretlane[.]com
- 1776trumedia[.]com
- 1835ranchrealty[.]com
- 1asapmovingcompany[.]com
- 1backends[.]com
- 1c7l[.]com
- 1c7p[.]com
- 1c7v[.]com
- 1c7y[.]com
- 1futuredreams[.]com
- 1gsgraphicdesignco[.]com
- 1guycarpet[.]com
- 1luvdesign[.]com
- 1luxurybeing[.]com