

Beware of Frappo and Related Cybersquatting Domains

Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Domains](#)

Executive Report

There's a new phishing-as-a-service (PaaS) solution in town, and it's called "[Frappo](#)." This new phishing toolkit enabled threat actors to launch impersonation attacks on at least 19 companies in the financial, entertainment, and telecommunications industries. WhoisXML API researchers monitored the Domain Name System (DNS) for registration activities related to the target brands since the phishing pages may be hosted on cybersquatting domains. Among our findings are:

- 16,800+ domains containing the names of the target companies added since 1 April 2022
- 14,400+ IP resolutions pointing to 5,800+ unique IP addresses
- Only 0.71% of the domains were publicly attributable to the target companies
- 800+ of the domains are already being flagged as malicious by various malware engines

Most Domains Can't Be Publicly Attributed to the Target Brands

As anyone in the cybersecurity community would expect, Frappo's target companies are among the most impersonated brands worldwide. These include large financial institutions in North America and other popular organizations, namely:

- Amazon
- ATB Financial
- Bank of Montreal (BMO)
- Bank of America (BOA)
- Chase
- Canadian Imperial Bank of Commerce (CIBC)
- Citibank



- Citizens
- Costco
- Desjardins
- M&T Bank
- Netflix
- Royal Bank of Canada (RBC)
- Rogers
- Scotia
- Tangerine Bank
- TD Canada Trust
- Uber
- Wells Fargo

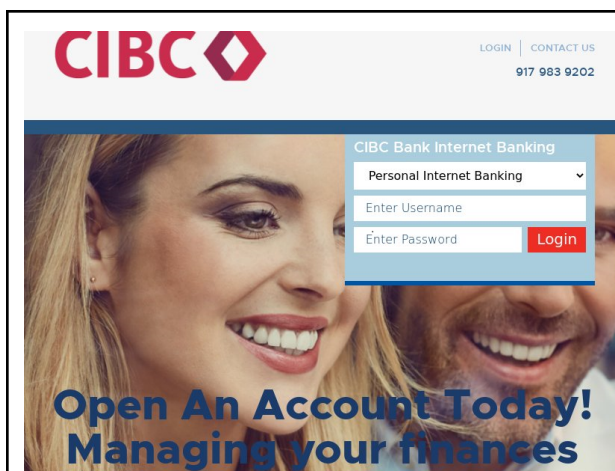
Using [Domains & Subdomains Discovery](#), we retrieved domains registered since 1 April 2022 that seem to imitate the official domains of these companies. For those prone to false positives, such as TD Bank (td[.]com) and ATB Financial (atb[.]com), we only included domains that begin with the exact second-level text string.

Out of more than 9,600 cybersquatting domains with available WHOIS records retrieved through [Bulk WHOIS Lookup](#), only 69 or 0.71% could be publicly attributed to the imitated brands. These domains used the companies' email addresses as registrant email addresses in their WHOIS records.

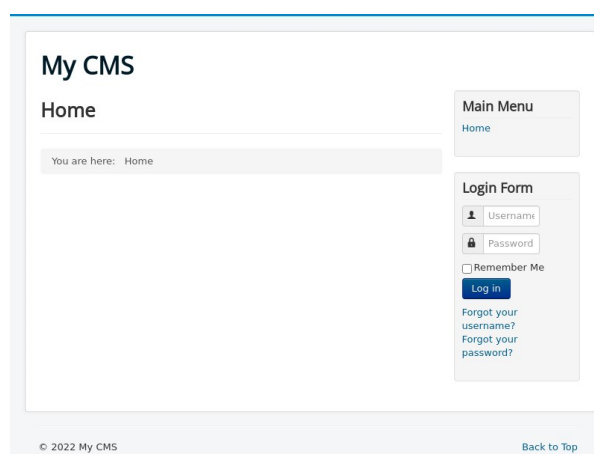
Screenshot Analysis of Resolving Cybersquatting Domains

Based on [Bulk IP Lookup](#) results, half of the domains in the study currently resolve to different IP addresses. What content do they host? While several domains were parked and resolved to 404 pages, our [Screenshot Service](#) uncovered some interesting web pages.

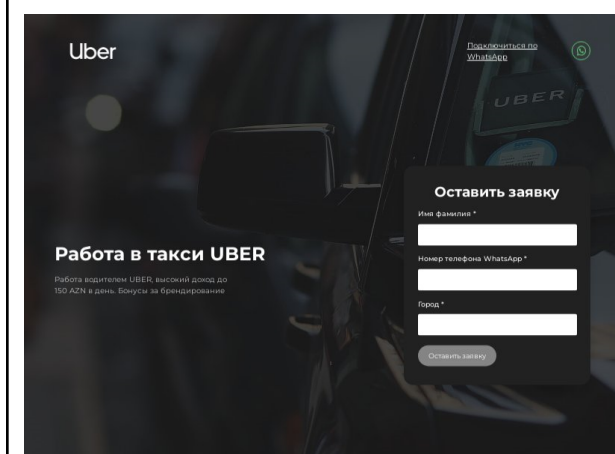
Some domains hosted login pages, including those already flagged as malicious. We showed some examples below.



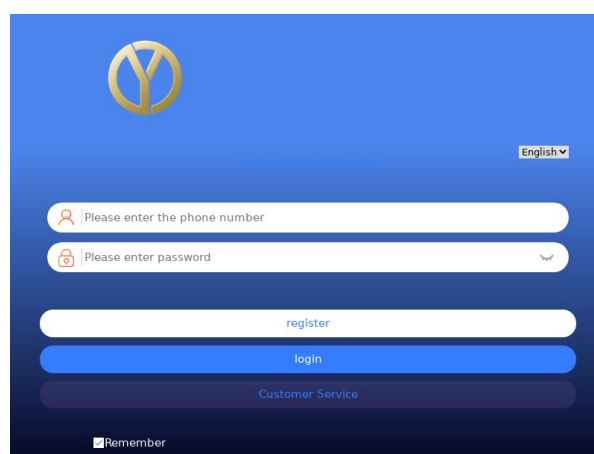
Screenshot of cibchw[.]com



Screenshot of wellsfargohelp[.]ga



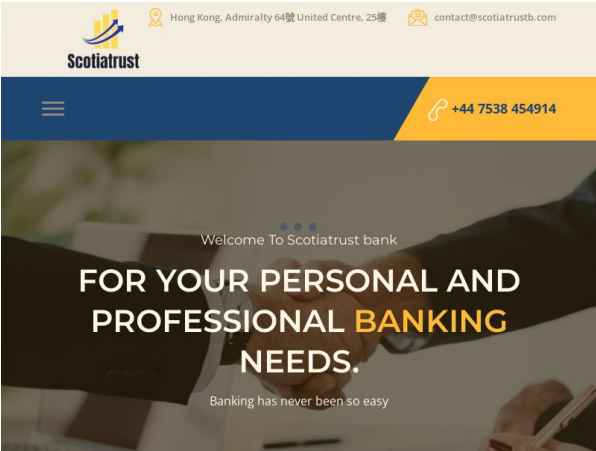
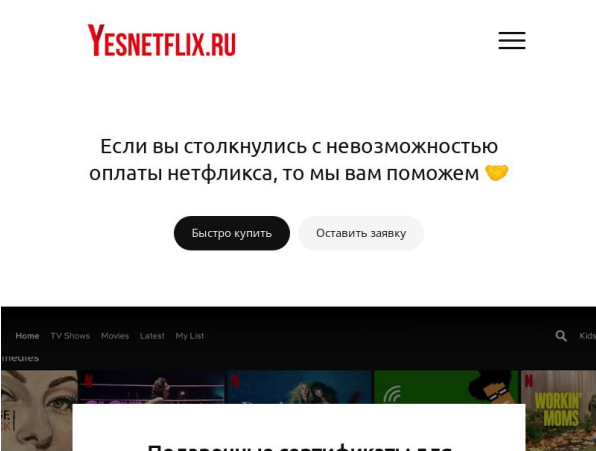
Screenshot of uber-az[.]site



Screenshot of amazonb[.]run

Some domains were also designed to look similar to those of the imitated companies, oftentimes sporting their brand logos and colors. Below are a few examples.



 <i>Screenshot of certificadoscstcomxcom</i>	 <i>Screenshot of scotiabankb[.]com</i>
 <i>Screenshot of amazon780[.]com</i>	 <i>Screenshot of yesnetflix[.]ru</i>

Semantic Analysis of Possible Frappo Domains

Although the domains in this study could be used in several malicious campaigns unrelated to Frappo, there is still a possibility that they host Frappo phishing pages. It's interesting to see how they could be used to lure potential victims to fake login pages. Aside from bearing the names of the target companies, the domains also used text strings that could make users believe they are being redirected to the correct websites.

These strings included tech and online terms, such as “services,” “support,” “auth,” and “mobile.” There were also account-related words like “login,” “signon,” “verification,” and “validation.” We also found some text strings that expressed a sense of urgency, such as “alert,” “help,” “security,” and “sale.” The word cloud below shows these and other common terms that appeared in the cybersquatting domains.



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 Domains

Sample of Cybersquatting Domains Added Since 1 April 2022

- bankchase[.]tech
- chasebankw[.]com
- chasebankiw[.]com
- allychasebank[.]us
- chasebankjpc[.]xyz
- chasebanknear[.]me
- chasebankauth[.]com
- chaseauthbank[.]com
- chasebankorg68[.]us
- chasetrustbank[.]com
- chasebankdileo[.]com
- zellechasebank[.]org
- zellechasebank[.]com
- account-chasebank[.]ga
- bankwithusatchase[.]com
- chasebank-recover[.]com
- chasebankripoffdep[.]us
- zellechasebanking[.]com
- chasebankonlineinc[.]com
- chase-bankservices[.]com
- chaseuniversalbanks[.]com
- chasebankservicesinfo[.]com
- chasebank-loginsecure[.]com
- chasebank-redirectlogin[.]com
- problem385infochasebank[.]com
- chasebank-redirect-login[.]com
- chasebank-reclaim-center[.]com
- chasebank-verifyaccounts[.]top
- secure-restore-chasebank[.]com
- chaseonlinebank[.]international
- chasebank-accountsecurity[.]com
- chasebank-redirect-secure[.]com
- chasebank-security-restore[.]com
- recoveryonline-chasebank07[.]com
- chasebank-validation-center[.]com
- chasebank-account-validation[.]com
- chasebank-secure-redirectlogin[.]com
- helpinformationchasebanksecure05[.]com
- chasebank-security-fraudprevention[.]com
- bankingonlineservicesupportinfochase[.]com
- citibankcreditcardindia[.]com
- citizensbank[.]me
- xn--itizensbank-l9a[.]com
- citizensbank[.]wtf
- citizensbank[.]cash
- citizensbank[.]fund
- citizensbank[.]life
- citizensbankr[.]com
- citizens--bank[.]com
- citizensbankwv[.]live
- citizensbank[.]center
- bankingcitizens[.]com
- citizensbank-0l[.]com
- citizensecbank[.]site
- citizensbankdept[.]com
- hydencitizensbank[.]vg
- citizensbankwv[.]click
- citizens0bank[.]online
- citizens3bank[.]online
- citizensbank[.]support
- citizens-bank[.]online
- secu-citizensbank[.]com



- bankwithcitizens[.]site
- citizensbank-auth[.]com
- www4-citizensbank[.]com
- citizensbank-login[.]com
- citizensstatebankt[.]com
- xn--itizensbankonline-bpb1u[.]com
- firstcitizensbankjm[.]com
- citizensfirstbanking[.]org
- citizensbankofcrypto[.]com
- citizensbankofperry[.]buzz
- citizensbankonline03[.]com
- citizensbanktransfer[.]com
- privatescitizensbank[.]com
- citizensbankontoline[.]com
- online02citizensbank[.]com
- 4citizensebanksonline[.]com
- wwwcitizensbank-logon[.]com
- 4citizensebanksonline[.]org
- citizensprogressivebank[.]vg
- ww3-citizensonlinebank[.]com
- ii-connect-citizensbank[.]us
- citizensprogressivebank[.]ph
- ll-connect-citizensbank[.]us
- bankingonline-citizens[.]com
- citizensbank-connect-us[.]com
- connect-citizensbank-us[.]com
- citizensecure-loginbank[.]com
- www3-citizensbankonline[.]com
- citizensbankverifylogin[.]com
- onlinelogin-citizensbank[.]com
- citizensbank-onlinelogin[.]com
- firstcitizensbankjamaica[.]com
- www-onlinebankingcitizens[.]com
- citizensbankonlineservlet[.]com
- citizensbank-onlinelogins[.]com
- citizensbankonlineloginsvr[.]com
- securecitizensbank-account[.]com
- wwwonlinelogin-citizensbank[.]com
- account-recovery-citizensbank[.]com
- www-onlinebankingcitizenslogin[.]com
- citizensbankonlineauthsvrconnect[.]com
- connectsvrauthcitizensbankonline[.]com
- connectsvrauthwebcitizensbankonline[.]com
- citibank[.]xn--node
- citibanko[.]ph
- citibank[.]arab
- citibanknv[.]com
- citibanks[.]live
- citibank202[.]com
- citibanknvs[.]com
- citibank347[.]com
- citibanksms[.]com
- citibank-sms[.]com
- citibankhelp[.]org
- citibanking1[.]com
- authcitibank[.]net
- citycitibank[.]com
- sms-citibank[.]com
- onlinecitibank[.]in
- zellecitibank[.]org
- zellecitibank[.]com
- meta-citibank[.]com
- zellecitibank[.]llc
- citibank-login[.]com
- verify-citibank[.]cc
- citibankreport[.]com
- citibankkwunto[.]com
- metacitibanker[.]com
- 1citibank-dash[.]com
- citibank-portal[.]com
- citibankreports[.]com
- citibankonline[.]com
- updatecitibanks[.]com
- alerts-citibank[.]com
- premiercitibank[.]com



- metacitibanking[.]com
- secure2citibank[.]com
- citibanklyst[.]com[.]de
- noreply-citibank[.]com
- 1verify-citibank[.]com
- citibank-lyst[.]com[.]de
- citibank-activity[.]com
- secureforcitibank[.]com
- citibankonline[.]com[.]au
- secured0a3citibank[.]cf
- secured02citibank[.]com
- secured03citibank[.]com
- citibankhelp-card[.]com
- secure0eb7citibank[.]cf
- sms-email-citibank[.]com
- sms-alert-citibank[.]com
- 3dsecured-citibank[.]com
- citibank-dashboard[.]com
- metacitibankonline[.]com
- citibankservice[.]online
- citibankinvestment[.]com
- secured0b2citibank[.]com
- citibank-secure29b[.]com
- metaverse-citibank[.]com
- citibank-singapore[.]info
- realcapitalcitibank[.]com
- citibankonlineshell[.]com
- citibankmalaysianis[.]com
- compliance-citibank[.]com
- metaversecitibanker[.]com
- citibankcryptofunds[.]com
- asecure03e-citibank[.]com
- secureform-citibank[.]com
- citibankdemobusiness[.]com
- citibanktransactions[.]com
- metaversecitibanking[.]com
- securecitibankaccount[.]ml
- secure6c3-citibank8se[.]com
- verification-citibank[.]com
- onlinecitibanksupport[.]com
- citibank-transactions[.]com
- citibankonlinereports[.]com
- citibank-verification[.]com
- mycitibanktitaniumcard[.]kr
- citibank-verification1[.]com
- citibank-verification2[.]com
- metaversecitibankonline[.]com
- xn--bankfmerica-h3c75o[.]ph
- xn--bnkofmerica-w7a7b[.]vg
- xn--ankofmerica-eue7135g[.]vg
- xn--bankofmrica-q8a6g[.]vg
- xn--bankofmeria-17a99b[.]vg
- xn--bnkofmeric-w4a120bka[.]vg
- xn--bankofaeric-v8a4088g[.]vg
- xn--bkofmerica-s4ad2298g[.]vg
- xn--bnkfamerica-7jb07r[.]ws
- xn--bankofamica-59a1219g[.]vg
- xn--bnkofmrica-wmb273aea[.]vg
- xn--bankofmerica-lcb[.]vg
- xn--bankfmerica-teb26z[.]vg
- xn--bankofmeic-mgbe1478g[.]vg
- xn--bankofmrica-28a93d[.]ph
- xn--bankofamerc-lcb0899g[.]vg
- xn--bankofamria-jmb542b[.]vg
- xn--bnkofameric-i7a453b[.]ws
- xn--bankofmrica-e8a56d[.]ws
- xn--bnkofmeric-w4a35zka[.]ws
- xn--bankofameca-xec8019g[.]vg
- xn--bnkofmric-53a50aef[.]vg
- xn--bnkofmeric-j5a7742gka[.]ws
- xn--bankofameri-j8a95c[.]vg
- xn--bankofmeic-k5ae5329g[.]vg
- xn--bnkofmerc-b2aee2k[.]vg
- xn--bankfaerica-ow8ez8d[.]vg
- xn--bankofamerc-u7a0460h[.]vg
- xn--bankoamrica-dyc5318g[.]vg
- xn--bnkfmerica-34ad3t[.]ws
- xn--bnkofmeric-z5a00be[.]vg
- xn--bnkfamerica-tfb670b[.]vg
- xn--bnkoferica-yo2eq5bea[.]ws



- xn--bankofamerc-lcb012b[.]vg
- xn--bnkfmeric-27a6564feaf[.]vg
- xn--bankofmeic-26b70wfa[.]vg
- xn--bankofamric-78a68d[.]ph
- xn--bnkofmric-l2aee4040h[.]vg
- xn--bnkfmerica-h4ad12w[.]vg
- xn--bnkofamerica-i7ac[.]ws
- xn--bankofmrica-8qb846a[.]ws
- xn--bankofmeric-wt9ef[.]vg
- xn--bnkofaerica-l8a082c[.]vg
- xn--bnkofaerica-l8a6688g[.]ws
- xn--bnkfmeric-52adf693b[.]cpa
- xn--lbankofamrica-jhb[.]ws
- xn--bnkofaerica-cfe18g[.]cpa
- xn--bankfmeric-7uc55cfa[.]cpa
- xn--lbankofmeric-8bbf[.]ph
- xn--bankofmeri-x4ae70c[.]cpa
- bankofgamerica[.]vg
- xn--bankofmrica-17a9h[.]cpa
- xn--bnkofamerica-76a3c[.]cpa
- xn--bakofameria-ulb89e[.]cpa
- xn--bnkofmeric-lgb3902gka[.]arab
- xn--bnkofamrica-tbb23a[.]arab
- xn--bnkfmeric-l2adf224b[.]arab
- xn--bankofamric-v8a99d[.]arab
- xn--bnkofmric-q4a61weaf[.]arab
- xn--bnkfamerica-87a234b[.]arab
- xn--bankofmerca-dkb28x[.]arab
- xn--bankofamric-u7a68d[.]arab
- xn--bnkfmeric-l2adf6860h[.]arab
- bankofamericatm[.]org
- bankofamericatm[.]net
- bankofamerica-u[.]com
- eyebankofamerica[.]ph
- bankofamericatm[.]com
- bankofamerica12[.]xyz
- bankofamericausa[.]us
- bankofamericarus[.]com
- bankofamericatms[.]net
- cpobankofamerica[.]cpa
- ezbankofamerica[.]arab
- bankofamericanear[.]me
- bankofamericallc[.]com
- bankofamerica-s2[.]com
- bankofamerica-0m[.]com
- bankofamericaatm[.]net
- amazonamazonamazon[.]cc
- amazonbot[.]amazon
- amazon-amazon[.]buzz
- pr1m3amazonamazon[.]com
- xn--amon-6na6997d[.]vg
- xn--zon-dlaa3326b[.]vg
- xn--amzon-sqa[.]fr
- xn--mzon-loa0976b[.]vg
- xn--amon-rzb0406d[.]ws
- xn--aman-7qa1166b[.]ws
- xn--maon-zsa03e[.]ph
- xn--maon-zmb6035b[.]ws
- xn--amzo-1na6626b[.]vg
- xn--amazn-9ta[.]fr
- xn--mzn-8oab51p[.]ph
- xn--maon-9sa03e[.]ws
- xn--maon-foa6176b[.]vg
- xn--amon-coa49w[.]ws
- xn--amaz-o2a7646b[.]vg
- xn--amon-6q5aw67g[.]vg
- xn--amzo-coa6g[.]ws
- xn--maon-poa4076b[.]ws
- xn--zon-gdba19g[.]vg
- xn--mzn-zna57i[.]ws
- xn--amaz-8qa60c[.]vg
- xn--amao-e2a69d[.]ws
- xn--mazo-koa81d[.]vg
- xn--azon-bta7106b[.]vg
- xn--amzon-4wa[.]vg
- xn--amazo-07a[.]co
- xn--mon-32a22bb[.]vg
- xn--mzo-tlab8426b[.]ws
- xn--mazo-9na29n[.]vg
- xn--mzon-u6bb[.]ws



- xn--zon-k4y3xb[.]vg
- xn--amao-jqa8987d[.]vg
- xn--mazn-foa1j[.]ph
- xn--amon-cta2256b[.]ws
- xn--mzon-bta81j[.]vg
- xn--mzon-bta81j[.]ws
- mamazon[.]io
- xn--mazn-koa3h[.]com
- xn--amazo-07a[.]net
- zamazon[.]it
- amazonb[.]nl
- amazone[.]vg
- xn--amazon-1ua[.]de
- xn--mzn-plab94i[.]cpa
- amazonk[.]co
- samazon[.]nl
- amazonm[.]ga
- amazonf[.]cn
- gamazon[.]io
- amazong[.]ws
- xn--mzon-zmbb[.]com
- xn--mon-8kab05g[.]cpa
- amazonb[.]vg
- xn--mazon-wqa[.]org
- amazonn[.]au
- amazonl[.]ph
- amazon5[.]ws
- amazone[.]kr
- 681-kltlamazonamazon[.]com
- 312-memexamazonamazon[.]com
- amazonsk[.]me
- hiamazon[.]cc
- amazon21[.]cc
- amazoncs[.]in
- amazonzx[.]tk
- amazonex[.]ws
- alamazon[.]cn
- amazon22[.]cc
- 682-kltolamazonamazon[.]com
- amazon98[.]ws
- ukamazon[.]uk
- amazonm[.]org
- amazonro[.]vg
- amazonn1[.]cf
- xn--amazna-exa[.]com
- zauber-zuber[.]de
- uberduber86[.]kred
- auber[.]ga
- uberr[.]ml
- auber[.]me
- uberx[.]xn--node
- uberb[.]io
- suber[.]ir
- quber[.]kz
- ubery[.]by
- tuber[.]ba
- uberz[.]au
- auber[.]uz
- uberx[.]ph
- muber[.]me
- vtuber[.]yt
- uberem[.]su
- xduber[.]ws
- lhuber[.]us
- pvuber[.]ws
- ubersv[.]au
- vtuber[.]cz
- twuber[.]tv
- sauber[.]ai
- dubero[.]vg
- zuberi[.]tk
- tuberr[.]vg
- vtuber[.]cl
- ecuber[.]vg
- cubery[.]co
- gruber[.]is
- lubery[.]ru
- xeuber[.]ru
- yuber[.]top
- uberto[.]ch



- kluber[.]pw
- huberg[.]ph
- suberk[.]ph
- hubero[.]li
- aluber[.]me
- cuberz[.]de
- vtuber[.]im
- iluber[.]ru
- hubero[.]io
- vtuber[.]mx
- ruberg[.]ch
- subere[.]de
- saubert[.]vg
- oruber[.]com
- suberna[.]ggq
- gaubera[.]cf
- my-uber[.]ca
- ubersk[.]com
- hubermi[.]ga
- buberny[.]ws
- subern[.]com
- n-huber[.]eu
- uberdog[.]co
- kuberass[.]us
- watuber[.]ru
- trubera[.]eu
- heubert[.]fr
- steuber[.]cf
- tuberng[.]uk
- faubert[.]co
- cuber[.]asia
- tubera[.]net
- uberapp[.]xn--kprw13d
- uberout[.]us
- on-uber[.]ca
- kuberr[.]net
- uberbau[.]fr
- xn--klber-lva[.]org
- hubertc[.]ph
- blubery[.]co
- lkhuber[.]us
- udmuber[.]tk
- puberty[.]vn
- bauberg[.]eu
- myrogers-rogers[.]ca
- myrogers-rogers[.]com
- rogers[.]sh
- krogers[.]uk
- rogersc[.]ph
- rogerse[.]de
- rogers[.]farm
- progersi[.]tk
- rogersux[.]me
- ckrogers[.]vg
- samrogers[.]eu
- mrrogers[.]biz
- rogersco[.]net
- rogersiot[.]tk
- samrogers[.]nl
- rogerscl[.]com
- crogers[.]cloud
- buckrogers[.]co
- mattrrogers[.]au
- rogerspllc[.]vg
- arcrogers[.]com
- rogerspay[.]net
- rogersale[.]com
- lirogershe[.]cf
- rogers6529[.]ml
- rogersa76[.]com
- rogerstar[.]top
- rogersingh[.]ca
- rogers17[.]site
- seanrogers[.]vg
- agrogerso[.]com
- progerscar[.]ml
- runrogers[.]com
- mattrrogers[.]co
- rogers-box[.]ch
- rogers-hc[.]com



- rogersprp[.]com
- rogerslnd[.]com
- fredrogers[.]vg
- unprogers[.]com
- rogersacc[.]net
- rogersacc[.]com
- orogers[.]com[.]br
- myrogersca[.]xyz
- jamalrogers[.]ws
- rogersacc[.]info
- benarogers[.]com
- tomlrogers[.]com
- rogersavage[.]au
- rogersfund[.]org
- luxerogers[.]com
- geoffrogers[.]uk
- annarogers[.]org
- rogerseller[.]au
- rogersmktg[.]com
- kiddrogers[.]com
- 3rogersave[.]com
- rogersfarm[.]org
- hurogers[.]co[.]uk
- rogersthat[.]net
- rogers-2fa[.]com
- rogers1[.]com[.]de
- rogerspay[.]info
- rogerstone[.]xyz
- progerssive[.]cc
- rogerstokes[.]uk
- rogers0816[.]top
- adamnrogers[.]me
- emilyrogers[.]co
- rogersclix[.]com
- immrrogers[.]com
- rogersrides[.]ca
- nio-rogers[.]com
- lisarogers[.]org
- 83rogersrd[.]com
- rogerspetro[.]co
- rogers-sec[.]com
- olamrogers[.]com
- ecrogers[.]co[.]uk

Sample of IP Addresses to Which the Cybersquatting Domains Resolved

- 67[.]215[.]15[.]130
- 34[.]102[.]136[.]180
- 2606:4700:3035::6815:58e9
- 2606:4700:3034::ac43:99c0
- 172[.]67[.]153[.]192
- 104[.]21[.]88[.]233
- 198[.]54[.]117[.]244
- 209[.]99[.]40[.]222
- 46[.]8[.]8[.]100
- 23[.]236[.]62[.]147
- 35[.]186[.]238[.]101
- 188[.]93[.]95[.]11
- 52[.]37[.]80[.]123
- 85[.]217[.]171[.]152
- 45[.]147[.]229[.]128
- 162[.]144[.]13[.]150
- 52[.]3[.]162[.]226
- 34[.]203[.]101[.]184
- 72[.]52[.]10[.]14
- 92[.]38[.]169[.]186
- 64[.]34[.]156[.]165
- 208[.]91[.]197[.]160
- 127[.]0[.]53[.]53
- 85[.]233[.]160[.]22
- 172[.]67[.]156[.]227
- 104[.]21[.]89[.]64
- 54[.]204[.]23[.]37
- 34[.]227[.]188[.]100



- 206[.]188[.]197[.]57
- 162[.]255[.]119[.]162
- 192[.]236[.]177[.]232
- 72[.]167[.]191[.]69
- 52[.]54[.]37[.]95
- 52[.]20[.]218[.]92
- 172[.]67[.]161[.]137
- 104[.]21[.]15[.]43
- 198[.]46[.]209[.]155
- 206[.]188[.]197[.]240
- 198[.]54[.]115[.]25
- 2a02:4780:9:608:0:1472:23d9:1
- 45[.]84[.]205[.]219
- 45[.]61[.]138[.]90
- 103[.]172[.]125[.]158
- 104[.]21[.]60[.]31
- 172[.]67[.]191[.]28
- 88[.]198[.]29[.]97
- 2600:1f16:389:3110:7b4c:7fe1:ff56:c784
- 2600:1f16:389:3100:e9b0:cdc3:239e:24c
- 2600:1f16:389:3120:dca:9be9:8e80:ea84
- 3[.]134[.]153[.]35
- 3[.]130[.]123[.]90
- 3[.]133[.]215[.]23
- 198[.]12[.]123[.]178
- 45[.]135[.]135[.]231
- 198[.]185[.]159[.]145
- 198[.]49[.]23[.]144
- 198[.]49[.]23[.]145
- 198[.]185[.]159[.]144
- 54[.]153[.]56[.]183
- 52[.]147[.]15[.]202
- 162[.]241[.]61[.]64
- 2607:f1c0:100f:f000::2b9
- 74[.]208[.]236[.]180
- 185[.]230[.]61[.]173
- 185[.]61[.]152[.]54
- 2606:4700:3030::ac43:c856
- 2606:4700:3033::6815:15cf
- 172[.]67[.]200[.]86
- 104[.]21[.]21[.]207
- 2a00:b700::26
- 185[.]22[.]155[.]62
- 78[.]31[.]111[.]139
- 69[.]10[.]41[.]74
- 69[.]10[.]41[.]72
- 98[.]124[.]224[.]17
- 68[.]183[.]153[.]189
- 2001:19f0:7400:887f:5400:3ff:fef7:e136
- 78[.]141[.]246[.]244
- 35[.]172[.]94[.]1
- 100[.]24[.]208[.]97
- 23[.]227[.]38[.]69
- 44[.]227[.]238[.]106
- 35[.]155[.]30[.]240
- 34[.]98[.]99[.]30
- 62[.]113[.]105[.]160
- 192[.]0[.]78[.]25
- 192[.]0[.]78[.]24
- 15[.]197[.]142[.]173
- 3[.]33[.]152[.]147
- 67[.]205[.]152[.]56
- 147[.]75[.]40[.]150
- 209[.]17[.]116[.]163
- 50[.]87[.]176[.]218
- 134[.]122[.]24[.]4
- 66[.]96[.]134[.]37
- 52[.]54[.]92[.]195
- 64[.]70[.]19[.]203
- 206[.]188[.]193[.]151
- 74[.]220[.]199[.]6
- 174[.]129[.]25[.]170



Sample Malicious Properties Flagged during the Malware Check Dated 23 May 2022

- 1mynetflixbillingrevise[.]support
- 1mynetflixclient-invoice[.]support
- 1secureaccess0-wellsfargohelp1[.]com
- aamazonverification[.]org
- accesnetflixfr[.]info
- accoune-amazon-update[.]info
- account-wellsfargosecurity[.]com
- accouo-amazon-updato[.]info
- againamazoncardnew[.]xyz
- amazon-4652[.]com
- amazon595[.]com
- amazon-assistanceinfo[.]com
- amazonceojp[.]gq
- amazon-delivery[.]net
- amazon-online[.]live
- amazonscp[.]ml
- amazonserv-mailapps[.]com
- amazon-suspendu22[.]com
- amazon-v[.]live
- anjeloidcaseamazon[.]com
- apple991amazon[.]com
- autenticacion-scotia[.]site
- ayoklahdimas2amazon[.]com
- bakuhantamamazon[.]com
- bankingonline-citizens[.]com
- bmotivatingmindslc[.]com
- cabaihmerahamazon[.]com
- caseidmarinamazon[.]com
- cautionaccountamazon[.]com
- cibcapp-ca[.]com
- cibc-myonline[.]com
- cibc-online-login[.]com
- cibc-signon-app[.]com
- cibc-signon-online[.]com
- citibank347[.]com
- citibanking1[.]com
- citibankonline[.]com[.]au
- citizensbank[.]me
- connect05wellsfargo[.]ml
- costco-membership-program[.]ca
- deenidcase23amazon[.]com
- desjardins-maintain-account-succesfully[.]ml
- desjardins-maintain-account-succesfully-in[.]ml
- enforce-protect-wellsfargo[.]com
- free-amazon[.]live
- gaslahajodioamazon[.]com
- idcamelmildamazon[.]com
- idsmithjamazon[.]com
- infoidtrigger531amazon[.]com
- juangkajai9amazon[.]com
- kapalomandangakamazon[.]com
- kasussanasiniamazon[.]com
- malamsekali10amazon[.]com
- mbilling-netflix[.]com
- mtbankonliine[.]com
- myamazonprofil[.]biz
- my-app-cibc[.]com
- mycibc-card[.]com
- mynetflix-login[.]com
- mysctia-alerts[.]com
- nect-wellsfargo[.]cf
- netflixmaroc[.]ml
- netflix-promociones[.]ml
- netflixscreenhelp[.]com
- netflix-seguridad-verificacion-de-identidad[.]ml
- netflixsupport[.]ca
- netflix-users[.]info
- patdenetflix[.]com



- pinaramaidamazon[.]com
- promo-netflix-argentina[.]ga
- redirectwellsfargo-support[.]com
- remindernetflix-account[.]com
- rogers-2fa[.]com
- rogers-sec[.]com
- ruberfareo[.]xyz
- sadesgigabyteinfoamazon[.]com
- scotia-alertslogin[.]com
- scotiabanks-login[.]com
- scotiabanxk4[.]co
- scotialogin-summary[.]com
- scotiaonline-logon[.]com
- scotiaweb[.]cc
- scotia-webalerts[.]net
- sec-bankofamerica0b[.]info
- sec-bankofamerica2c[.]info
- signon-scotiaonline[.]com
- support4scotia[.]com
- support-netflix[.]ca
- tampuahajolaiamazon[.]com
- uberlink[.]us
- valid-netflix1[.]com
- verifii992-amazon[.]com
- web-amazon-co[.]jp
- webregamazonid[.]cafe
- wells Fargo-verify01[.]com
- wells-fargo-verify12[.]com
- www-mynetflixapp[.]com
- www-scotia-myaccount[.]com
- www-scotiaonline-signin[.]com
- xn--mazon-wqa[.]org