A Look into New Cybersquatting and Phishing Domains Targeting Facebook, Instagram, and WhatsApp

Table of Contents

Executive Report

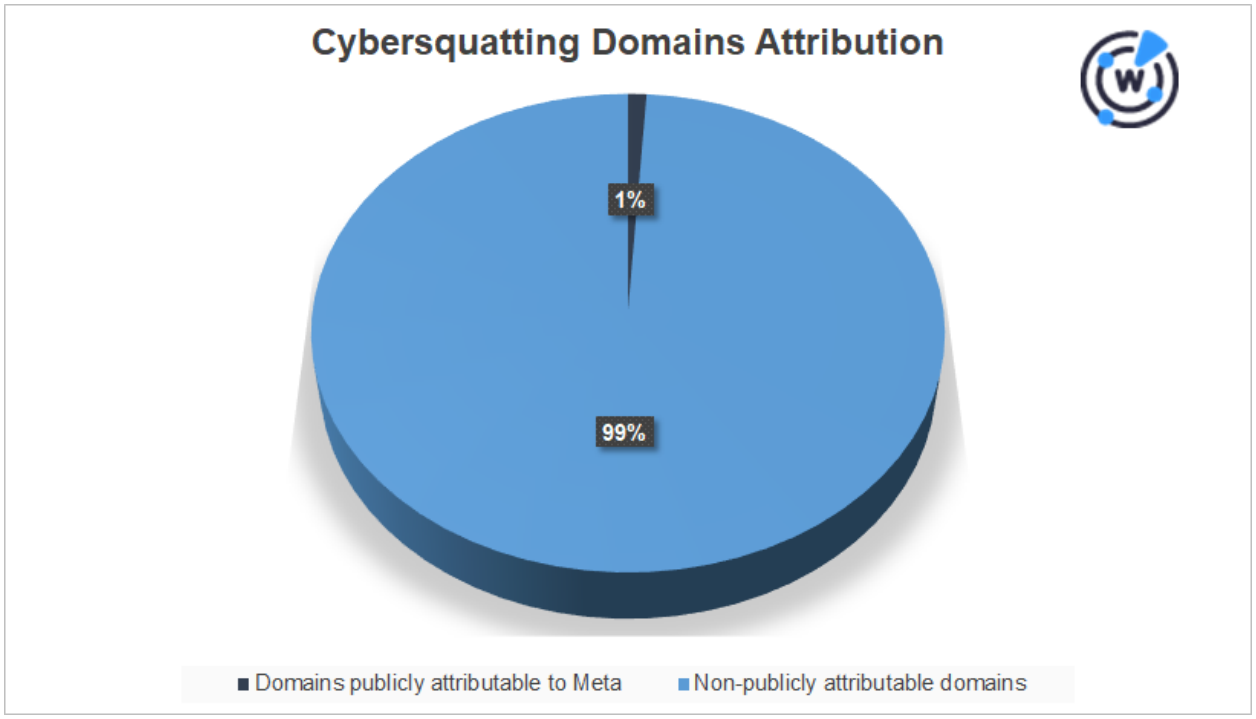
When Facebook changed its parent company name to Meta in October 2021, we detected more than 5,500 newly registered domains (NRDs) a week after the announcement. In more recent news, a judge dismissed the company's cybersquatting and trademark infringement case against Namecheap. Around 61 domains were transferred to Meta's ownership. What does cybersquatting activity look like since then?

WhoisXML API researchers checked the Domain Name System (DNS) for domain registrations related to Facebook, Instagram, and WhatsApp, the subjects of the dismissed case. Among our findings include:

- 1,100+ typosquatting domains targeting the three Meta applications were added since the case was dismissed on 25 April 2022
- 760+ domains currently resolve to 530+ unique IP addresses
- Close to 10% of these domains are already flagged as malicious as of 25 May 2022
- Some domains host suspicious login pages that could be fronts for credential theft
- 2,400+ domains bearing similar string combinations as some of the malicious domains

Who Is Behind the NRDs?

Several domains had redacted WHOIS details, although we found some Gmail, Yahoo!, and Hotmail email addresses. As such, pinpointing the actors behind the domains can be challenging. Out of more than 1,000 typosquatting domains we ran on Bulk WHOIS Lookup, we found that 12 shared the same registrant email address as the legitimate Meta domains.



The top registrar used by the cybersquatting domains was GoDaddy, while only two were registered through Namecheap.

Where Are the Domains Resolving?

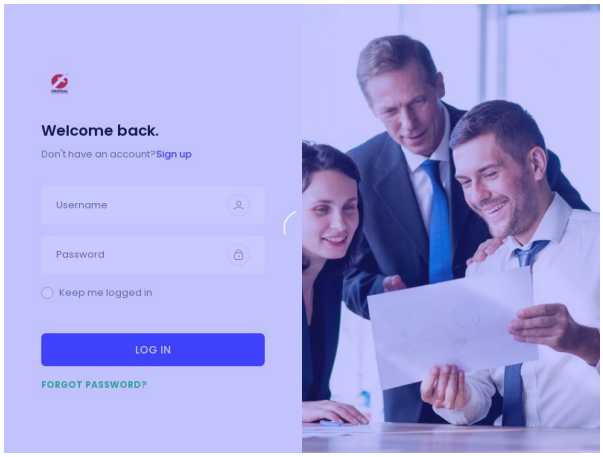
Using Bulk IP Geolocation Lookup, we found 1,043 resolutions, with 764 domains currently resolving to 537 IP addresses. Half of them were geolocated in the U.S., while the rest were spread across 36 other countries.

The situation is the same with the domains' registrant countries. Only half of the domains were registered in the U.S., while the other half were registered in more than 40 countries.

What Type of Content Do the Domains Host?

According to the Screenshot Lookup results, several domains were parked, while some sold likes and followers. However, the domain names hosting login pages could be even more problematic as they could be used to steal user credentials. Below are a few examples.

Screenshot of wwwloginfacebook[.]com

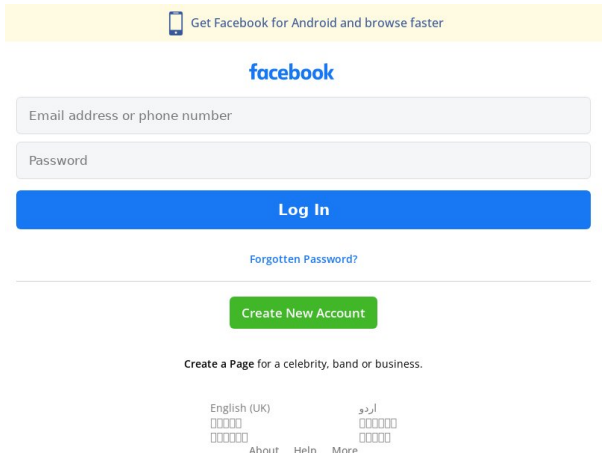


Screenshot of firstdialwhatsapp[.]xyz

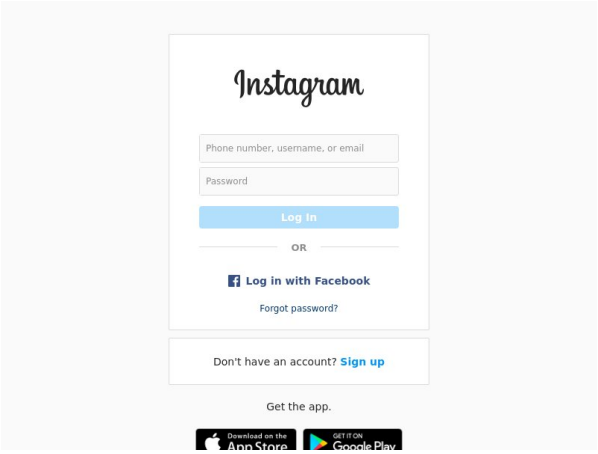
Screenshot of facebookfans[.]top

Screenshot of facebookfans01[.]xyz

Some domains hosted login pages that looked exactly like those belonging to the legitimate platforms.



Screenshot of faceboof[.]ml



Screenshot of xn--nstagram-fcg[.]ga

Malicious Domains Found

Aside from the suspicious web pages found through the screenshot analysis, some domains have already been flagged as malicious by various malware engines. Most of these domains fell under new generic top-level domains (ngTLDs) led by .tk, .ml, .cf, and .ga.

Furthermore, several malicious properties contained text strings that could easily lure users to malicious pages, including “help,” “support,” “verify,” “secure,” and “business.” Quite a few also used the word “copyright” alongside “instagram.” Focusing on this string combination present in some malicious domains, we found an additional 2,409 domains added over time that could be suspicious.

2,409 domain(s) having your specific search terms found

Export CSV

instagramcopyright.me	instagramcopyright.cf	copyrightinstagram.tk
copyrightinstagram.cf	instagramcopyright.us	instagramcopyright.ir
instagramcopyright.in	copyrightinstagram.ml	instagramcopyright.tk
copyrightinstagram.ph	copyrightinstagram.gq	instagramcopyright.org
instagramcopyrightx.ga	xn--nstagramcopyrght-7rb...	instagram-copyright.ml
copyrightsinstagram.cf	copyright-instagram.vg	xn--instagramcpyright-6ie....
copyrightinstagrams.tk	copyrightinstagram.org	instagramscopyright.tk
instagramcopyrightw.ml	copyrightinstagrams.ml	instagram-copyright.cf
instagramcopyrights.ga	instagram-copyright.in	instagramcopyrightt.ga
instagramscopyright.gq	instagramcopyrighto.tk	copyright-instagram.cf

Show 30

1 2 3 4 5 ... 81

—

Cybersquatting domains continue to expand the DNS threat landscape at a rapid pace. About 100 of those targeting Meta's platforms have already been used to launch cyber attacks, barely a month after they were registered. Early detection of these domains can help reduce risks associated with phishing, impersonation, and other cyber attacks dependent on cybersquatting domains.

Furthermore, expanding threat analysis to include domains bearing the same text strings can help predict and block suspicious domains before they get weaponized.

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 Cybersquatting Domains Added Since 25 April 2022

- xn--fcbook-35b9330d[.]ph
- xn--faebok-4rb6701d[.]vg
- mfacebook[.]vg
- xn--facbk-dsa34ea[.]com
- xn--facebk-7wa6a[.]com
- xn--fcebok-3ta8932d[.]cpa
- dvfacebook[.]cf
- facebookq[.]xyz
- facebookvn[.]pw
- v2facebook[.]me

- facebook86[.]ga
- facebook-a[.]cf
- ffacebookk[.]fr
- facebook-0[.]com
- t0facebook[.]com
- facebook1[.]live
- facebook5s[.]com
- facebooktoo[.]us
- facebooknr[.]com
- facebook-vn[.]gq
- ms-facebook[.]ml
- facebookrz[.]com
- facebook11[.]cpa
- hotfacebook[.]me
- userfacebook[.]ml
- petfacebook[.]app
- facebookinfo[.]ga
- facebookdown[.]cf
- fakefacebook[.]gq
- mrtfacebook[.]com
- facebookclub[.]us
- metafacebook[.]bg
- dfacebookdod[.]cf
- facebookmeta[.]us
- xwhatsapp[.]cf
- whatsappa[.]cf
- fgwhatsapp[.]ml
- whatsapp6[.]vip
- whatsappro[.]ru
- whatsappsxy[.]ga
- whatsappbro[.]in
- gdwhatsapp[.]com
- apiwhatsapp[.]es
- whatsapp-18[.]tk
- 91whatsapp[.]net
- whatsappnom[.]cf
- whatsappiq[.]com
- whatsapp5s[.]xyz
- gb-whatsapp[.]cc
- whatsapping[.]io
- whatsappmg[.]com
- whatsapp223[.]ga
- whatsapp22[.]xyz
- whatsapp-ht[.]ml
- whatsappaq[.]com
- apiwhatsapp[.]co
- qrwhatsapp[.]com
- jkwhatsapp[.]com
- whatsappcs[.]net
- whatsapptvs[.]org
- whatsapp-api[.]ga
- whatsappbot[.]org
- cswhatsapp[.]info
- metawhatsapp[.]hk
- whatsappgold[.]it
- whatsappday[.]org
- whatsappvtc[.]com
- whatsappold[.]com
- instagram-instagram-instagram-instagram--instagram-instagram[.]tk
- instagram-instagram--instagram-instagram-instagram[.]tk
- instagram-instagram-instagram--instagram-instagram[.]tk
- instagram-instagram-instagram-instagram--instagram[.]tk
- instagram-instagram-instagram-instagram-store[.]ml
- instagram-instagram-instagram-instagam--instagram-instagram[.]tk
- instagram-instagram-instagram-instagam[.]cf
- instagram-instagram-instagram-instagam[.]ga
- instagram-instagram-instagram-instagam[.]gq
- instagram-instagram-instagram-instagam[.]tk
- xn--instrm-stab60d[.]vg
- xn--nstagram-skb[.]cf

- instagram-instagram-instagram-instagraam[.]tk
- instagram-instagram-instagram-instagraam[.]gq
- xn--nstagrm-bxa8e[.]vg
- instagram-instagram-instagram-instagraam[.]cf
- instagram-instagram-instagram-instagraam[.]ml
- instagram-instagram-instagram-instagraam[.]ga
- instagrams[.]ml
- instagrams[.]ph
- instagramnl[.]ml
- winstagram[.]lol
- winstagram[.]fun
- ssinstagram[.]ml
- instagrammer[.]tv
- instagrams[.]rest
- instagrammer[.]gq
- instagramnft[.]de
- wwwinstagram[.]be
- instagramix[.]net
- instagramlog[.]ml
- instagramvn[.]xyz
-

Sample IP Addresses to Which the Cybersquatting Domains Resolved

- 45[.]79[.]222[.]138
- 88[.]198[.]29[.]97
- 2606:4700:3032::ac43:8c73
- 2606:4700:3032::6815:5144
- 104[.]21[.]81[.]68
- 172[.]67[.]140[.]115
- 134[.]209[.]28[.]104
- 127[.]0[.]53[.]53
- 103[.]169[.]160[.]66
- 195[.]20[.]48[.]253
- 195[.]20[.]48[.]84
- 104[.]247[.]82[.]50
- 15[.]197[.]142[.]173
- 3[.]33[.]152[.]147
- 195[.]20[.]55[.]199
- 66[.]81[.]199[.]56
- 2606:4700:3033::6815:31f8
- 2606:4700:3036::ac43:9a7c
- 104[.]21[.]49[.]248
- 172[.]67[.]154[.]124
- 2606:4700:3033::6815:37e0
- 2606:4700:3032::ac43:adc8
- 172[.]67[.]173[.]200
- 104[.]21[.]55[.]224
- 185[.]27[.]134[.]216
- 216[.]120[.]146[.]201
- 195[.]20[.]51[.]212
- 195[.]20[.]50[.]150
- 167[.]172[.]180[.]37
- 34[.]102[.]136[.]180
- 52[.]60[.]87[.]163
- 195[.]20[.]52[.]204
- 34[.]98[.]99[.]30
- 195[.]20[.]55[.]44
- 2606:4700:3031::6815:23bc
- 2606:4700:3031::ac43:b299
- 172[.]67[.]178[.]153
- 104[.]21[.]35[.]188
- 199[.]59[.]243[.]220
- 170[.]33[.]9[.]230
- 172[.]247[.]112[.]114
- 46[.]242[.]233[.]52
- 195[.]20[.]52[.]11
- 3[.]64[.]163[.]50
- 64[.]225[.]91[.]73
- 185[.]27[.]134[.]230

- 195[.]20[.]55[.]230
- 103[.]233[.]193[.]42
- 2606:4700:3036::ac43:c75c
- 2606:4700:3037::6815:15a2
- 104[.]21[.]21[.]162
- 172[.]67[.]199[.]92
- 72[.]167[.]191[.]69
- 2a00:f940:2:2:1:3:0:90
- 31[.]31[.]198[.]7
- 127[.]0[.]0[.]10
- 195[.]20[.]51[.]88
- 35[.]76[.]232[.]248
- 45[.]77[.]240[.]178
- 20[.]199[.]126[.]61
- 195[.]20[.]52[.]68
- 195[.]20[.]50[.]140
- 66[.]235[.]200[.]146
- 82[.]84[.]74[.]21
- 109[.]234[.]110[.]254
- 79[.]98[.]25[.]1
- 142[.]132[.]211[.]248
- 2606:4700:3035::ac43:cfe9
- 2606:4700:3037::6815:5b10
- 104[.]21[.]91[.]16
- 172[.]67[.]207[.]233
- 216[.]239[.]34[.]21
- 216[.]239[.]38[.]21
- 216[.]239[.]32[.]21
- 216[.]239[.]36[.]21
- 2[.]57[.]138[.]187
- 203[.]170[.]80[.]250
- 103[.]174[.]235[.]11
- 193[.]53[.]245[.]139
- 54[.]160[.]124[.]18
- 3[.]208[.]142[.]147
- 166[.]62[.]75[.]68
- 173[.]254[.]252[.]165
- 195[.]78[.]67[.]50
- 64[.]70[.]19[.]203
- 199[.]66[.]92[.]226
- 91[.]195[.]240[.]94
- 208[.]91[.]197[.]91
- 66[.]66[.]66[.]66
- 2606:4700:3037::6815:4eee
- 2606:4700:3037::ac43:8a6e
- 172[.]67[.]138[.]110
- 104[.]21[.]78[.]238
- 202[.]124[.]241[.]178
- 195[.]20[.]55[.]194
- 2001:8d8:100f:f000::201
- 217[.]160[.]0[.]217
- 195[.]20[.]50[.]62
- 86[.]111[.]242[.]97
- 74[.]220[.]199[.]6
-

Sample Malicious Properties Flagged during the Malware Check Dated 25 May 2022

- Instagramhelp-badgecenter[.]ga
- Instagramobjectionformeta[.]ml
- Instagram-copyrigthsupport[.]ml
- Instagramhelpcenter-2314546[.]tk
- Instagram-photo-ahjcdygd[.]my[.]id
- Instagramcopyrightverifycenter[.]tk
- personel-help-support-Instagram[.]ga
- Instagrambadgeverified-contract[.]ml
- Instagramcopyrighthelpcenter-2345[.]tk
- Instagramhelpcopyrightingservicecenter[.]tk
- facebookbusiness[.]me
- business-facebook[.]me

- business-facebook[.]nl
- coverdacristianafacebook[.]tk
- safetyprivacyvacebook2022[.]cf
- safetyprivacyfvacebook2022[.]gq
- xwhatsapp[.]cf
- whatsappnom[.]cf
- whatsappcs[.]net
- whatsapp-invite[.]pw

Sample Domains Containing the “instagram + copyright” String Combination

- instagramcopyright[.]me
- instagramcopyright[.]cf
- instagramcopyright[.]ir
- copyrightinstagram[.]tk
- copyrightinstagram[.]cf
- instagramcopyright[.]us
- instagramcopyright[.]in
- copyrightinstagram[.]ml
- copyrightinstagram[.]ph
- instagramcopyright[.]tk
- copyrightinstagram[.]gq
- instagramcopyright[.]org
- instagramscopyright[.]gq
- copyrightsinstagram[.]cf
- copyright-instagram[.]vg
- xn--instagramcpyright-6ie[.]com
- copyrightinstagrams[.]tk
- copyrightinstagram[.]org
- instagramscopyright[.]tk
- instagramcopyrightw[.]ml
- instagramcopyrightx[.]ga
- instagram-copyright[.]ml
- xn--nstagramcopyrght-7rbn[.]com
- copyrightinstagrams[.]ml
- instagram-copyright[.]cf
- instagramcopyrights[.]ga
- instagram-copyright[.]in
- instagramcopyrightt[.]ga
- instagramcopyrightc[.]ml
- instagramcopyrighto[.]tk
- copyright-instagram[.]cf
- instagramcopyright[.]net
- instagramzcopyright[.]cf
- instagramcopyrightt[.]gq
- instagram-copyright[.]tk
- instagramcopyrights[.]gq
- copyright-instagram[.]gq
- instagramcopyright[.]com
- instagramscopyright[.]ml
- instagramcopyrightr[.]ml
- instagramcopyright[.]xyz
- xn--nstagramcopyright-bvc[.]xyz
- instagramcopyrightw[.]tk
- instagramcopyright[.]biz
- instagramscopyright[.]cf
- xn--nstagramcopyright-bvc[.]com
- instagramcopyrightl[.]cf
- copyrightpinstagram[.]tk
- copyright-instagram[.]fm
- instagramscopyright[.]ga
- instagram-copyright[.]eu
- instagramcopyrights[.]cf
- copyrightinstagram[.]net
- copyright-instagram[.]tk
- copyrightinstagrams[.]gq
- instagramccopyright[.]ml
- instagram-copyright[.]co
- instagram-copyright[.]us
- instagram-copyright[.]ga
- copyrightinstagram[.]com
- instagramscopyright[.]ws
- copyright-instagram[.]ga
- instagramcopyrightx[.]cf
- instagramofcopyright[.]ml

- instagram--copyright[.]cf
- copyrights-instagram[.]ml
- copyright-instagram[.]org
- instagramcopyrightss[.]ml
- instagram-copyrights[.]cf
- instagramscopyrights[.]tk
- copyrightinstagram[.]info
- xn--nstagramcopyrghts-bvcn[.]com
- copyrights-instagram[.]tk
- instagramcopyrightts[.]ml
- instagram-copyrightt[.]ml
- instagramcopyright[.]site
- copyright-instagrams[.]cf
- instagram-copyright0[.]ml
- instagramcopyrightes[.]ml
- instagramcopyrighten[.]cf
- instagram-copyright[.]xyz
- instagram--copyright[.]ga
- instagram-copyright4[.]cf
- copyrights-instagram[.]cf
- instagramcopyright[.]team
- instagramcopyrightfb[.]gq
- instagram-copyright[.]net
- instagramcopyright12[.]gq
- instagram-copyrights[.]ml
- copyrightofinstagram[.]ml
- instagram-copyright[.]org
- instagramcopyrightdm[.]ml
- instagramcopyright[.]help
- instagramcopyrightsq[.]ga
- copyrightheinstagram[.]tk
- instagramcopyrightht[.]ml
- xn--instagramcopyrghts-r0c[.]com
- instagramcopyright[.]shop
- copyrightt-instagram[.]tk
- instagramcopyrights[.]org