Catching Messenger Phishing Footprints Using a DNS Net

Table of Contents

Executive Report

A phishing campaign is currently targeting Facebook business accounts with password-stealing malware. The attackers have been using a massive network of fake and compromised Facebook accounts to send out millions of Messenger phishing messages.

Dubbed a part of the MrTonyScam, the phishers typically cited copyright violations or requests for more information about business products. Victims who download the attached RAR or ZIP archive file trigger a malware dropper to fetch its payload from GitHub repositories that gets executed on the affected users' systems. The malware then collects all the cookies and login data stored on victims' web browsers, compiles them into a ZIP archive, and sends the archive to the attackers.

WhoisXML API researchers found a publicly available list of indicators of compromise (IoCs) related to the ongoing malicious campaign. We analyzed the digital infrastructure of 63 domains identified as IoCs and traced their DNS footprints that led to the discovery of:

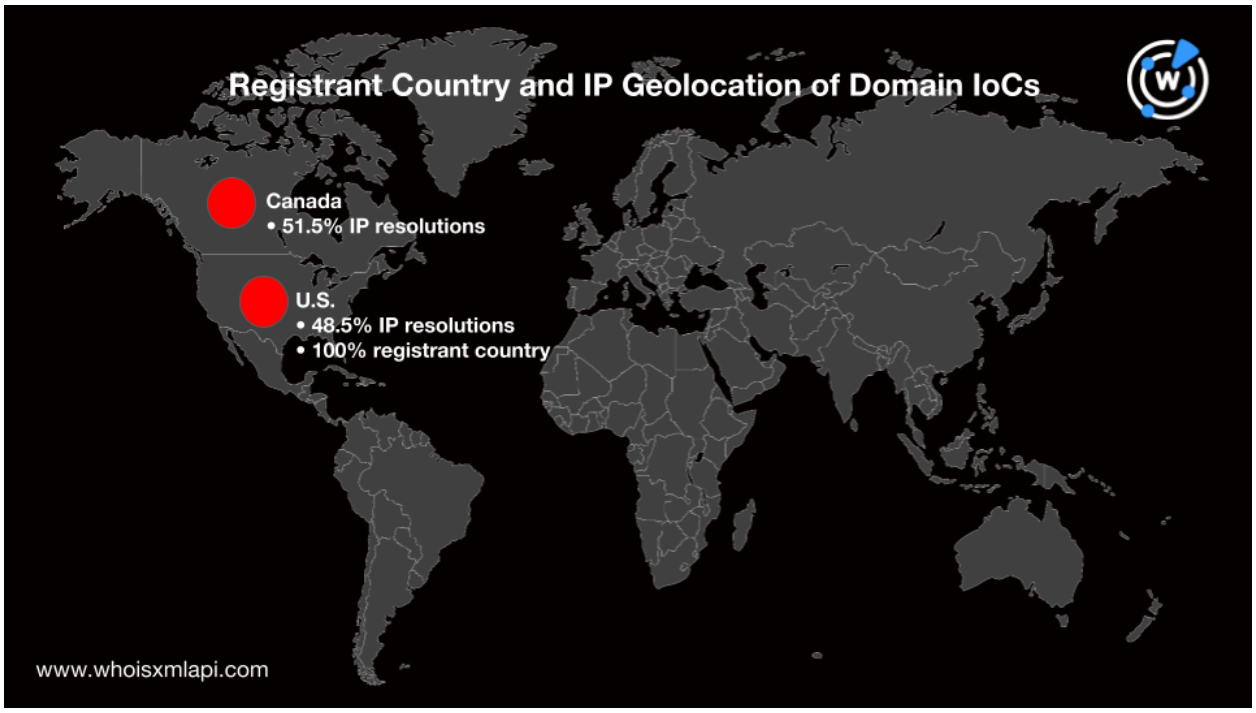
- 15 personal email addresses historically used to register the IoCs with less than 50 connected domains each
- 155 email-connected domains
- 924 domains containing similar strings as the IoCs, such as **movies-**, **office-** and **2023**, and **x-album**
- 18 IP-connected domains that also contained similar text strings found in the IoCs

Messenger Phishing Infrastructure: What We Know

Our analysis of the IoCs' IP resolutions through a bulk IP geolocation lookup revealed that about 79% still resolved to 180 unique IP addresses. That means many of them have multiple

resolutions, averaging 3–4 per domain. IP geolocation data pointed to Canada (51.5%) and the U.S. (48.5%) as their only locations and Cloudflare as their sole Internet service provider (ISP).

A bulk WHOIS lookup for the domains also revealed uniform WHOIS details. All of them were registered with NameSilo while PrivacyGuardian protected their WHOIS records. The domains all specified the U.S. as their registrant country.



The glaring similarities among all of the domains suggest they could have been registered and controlled by the same entity. Alternatively, the domains' registrar may have repossessed them after figuring in the Messenger phishing campaign.

Tracing the IoCs' DNS and Domain Connections

While several IoCs have already been publicly named and possibly reported on various security platforms, the threat actors may have other domains in their arsenal just awaiting deployment. The IP-, email-, and string-connected domains we found and discussed in greater detail below could be considered potential artifacts of the Messenger phishing scam.

WHOIS-Connected Artifacts

As a possible early threat detection effort, we examined the malicious domains' historical WHOIS records, which led to the discovery of 73 publicly available registrant email addresses.

Many of them were obtained from Gmail, Yahoo!, Naver, Live, and other commonly used email services.

We then ran reverse WHOIS searches for the email addresses. We focused on 15 email addresses that were used to register less than 50 domains each. The other addresses were used to register hundreds or even thousands of domains and may once have belonged to domain name investors. Despite the sample reduction, we still found 155 email-connected domains, only 15 of which had active resolutions.

String-Connected Artifacts

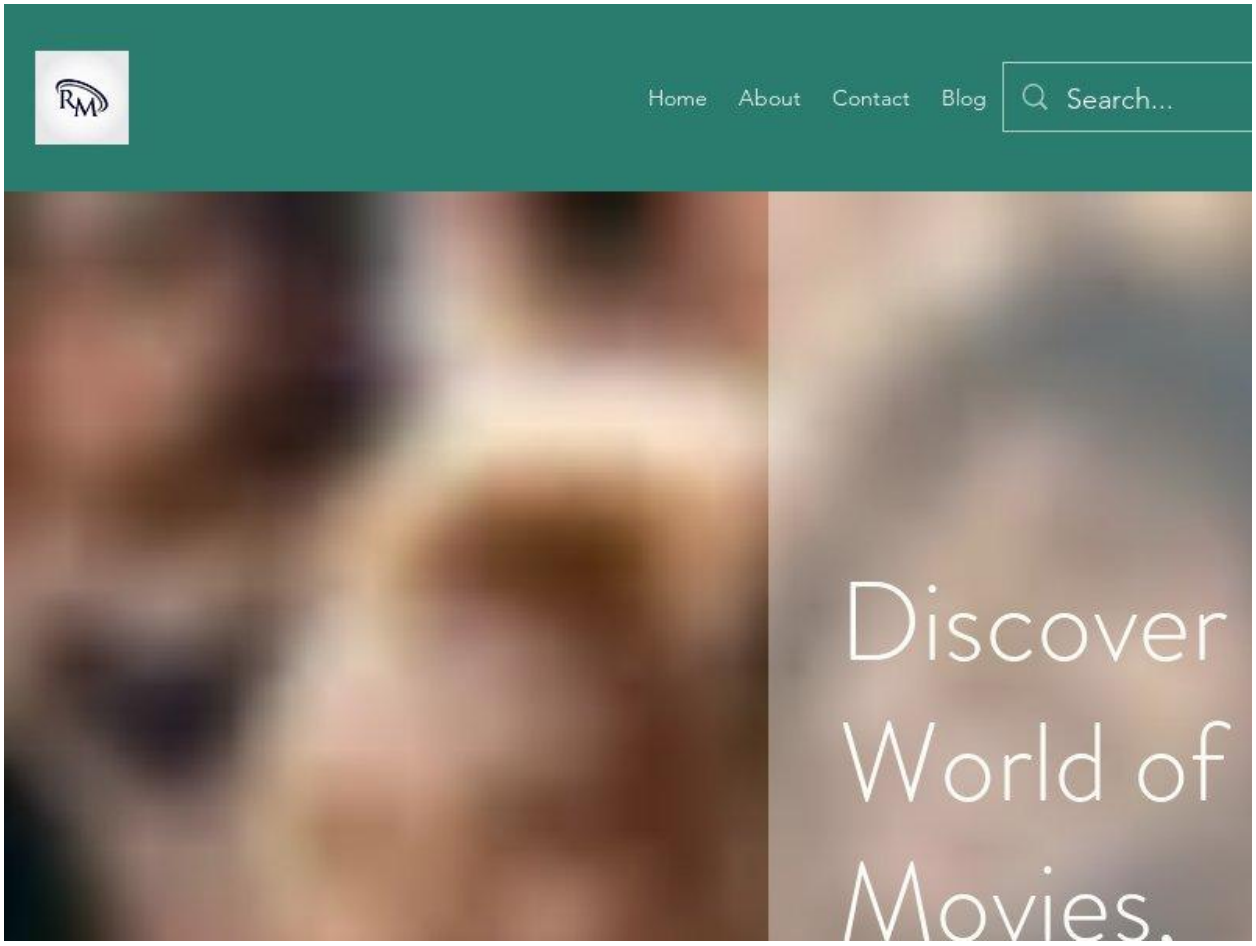
Next, we retrieved domains that contained text strings that repeatedly appeared among the IoCs. We used Domains & Subdomains Discovery to uncover domains that started with the strings:

- **movies-**
- **x-album**
- **x-image**
- **x-photo**
- **x-picture**

We also looked for domains that:

- Started with **canva** and contained **2023**
- Started with **office-** and contained **2023**
- Started with **chatgpt** and contained **premium**

Our searches yielded 924 domains added from 1 January to 18 September 2023. About 94% of them still have active resolutions. While these connected domains may not necessarily be related to the Messenger phishing campaign, it's important to note that some of them have already been classified as malicious by a malware check, including movies-shows-more[.]com, which continued to host or redirect to this page:



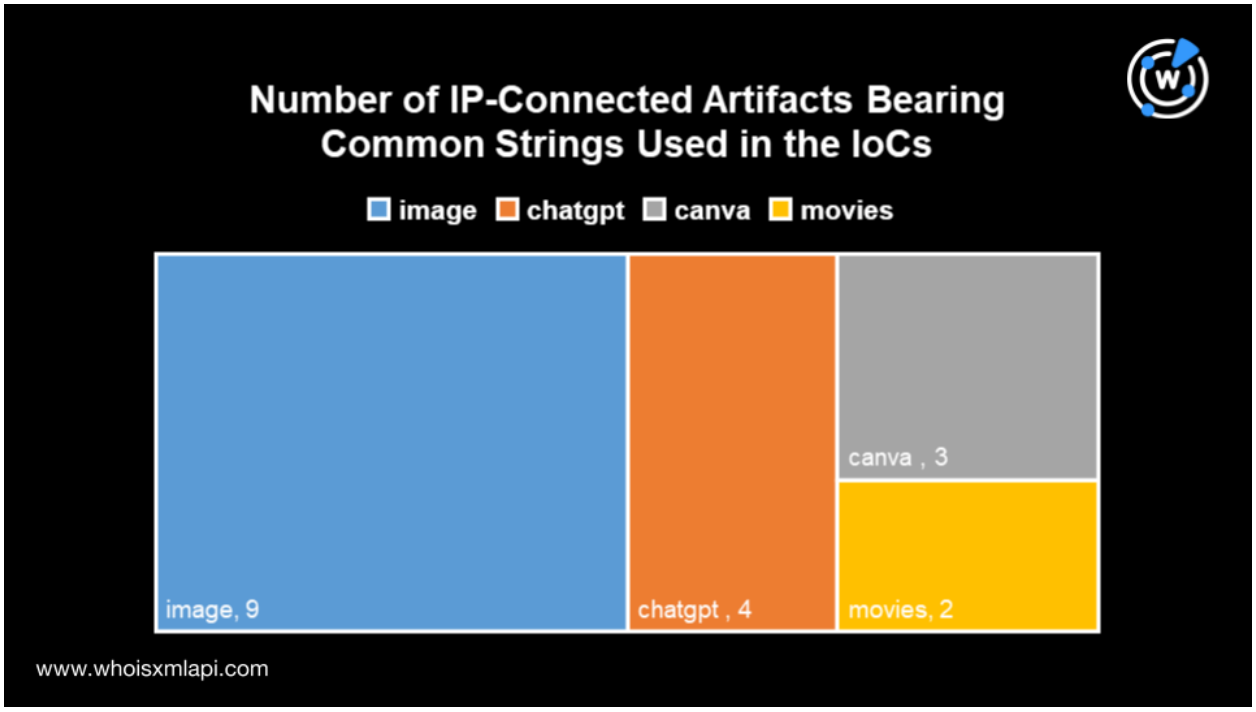
Screenshot of movies-shows-more[.]com

The use of brand names like Canva, Office, and ChatGPT by the identified domains also raises suspicion.

IP-Connected Artifacts

We then traced the IoCs' DNS footprints by performing reverse DNS searches to find other domains sharing their IP resolutions. We found that they were primarily hosted on shared infrastructures since each IP address hosted more than 300 domains. As such, they may not be part of malicious IP networks and instead are just public IP addresses that multiple domains share.

However, we discovered several IP-connected domains also containing strings that appeared in some of the IoCs.



Some of these IP- and string-connected domains hosted suspicious content. For example, a screenshot of chatgptlogn[.]com shows that the domain hosted a page with several login links and contained the ChatGPT logo.

Screenshot of chatgptlogn[.]com

—

Our DNS deep dive into the recently reported Messenger phishing campaign allowed us to catch some suspicious and malicious properties related to known IoCs via WHOIS, DNS, and string usage. What started as an IoC expansion exercise led us to find other potential malicious campaigns likely targeting Canva and ChatGPT users and people browsing for movies online.

If you wish to perform a similar investigation or 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 and IoCs

Messenger Phishing IoCs

- apps-blue[.]com
- canva2023[.]com
- cdn[.]axphotoalbum[.]top
- cembuyukhanli[.]com
- chatgpt-premium[.]com
- dl[.]payforme[.]top
- dl[.]privatecollection[.]top
- download5s[.]com
- gaming-box[.]com
- helenrosi[.]com
- ictorganisers[.]com
- jinghuaqitb[.]com
- jmooreassoc[.]com
- karbilyazilim[.]com
- kimhasa[.]com
- lydownload[.]net
- movies-box[.]net
- movies-cine[.]com
- movies-cinema[.]com
- myprivatephotoalbum[.]top
- nctitds[.]top
- nskfyl[.]com
- office-2023[.]com
- office2023[.]net
- office-2023[.]net
- payforme[.]top
- phcde[.]top
- photo-cam[.]com
- photography-hq[.]com
- pictures-album[.]com
- preppypm[.]com
- privatecollection[.]top
- programe[.]top
- ritikajoshi[.]com
- romeflirt[.]com
- shble[.]com
- simpli[.]top
- somalisounds[.]com
- sportydesktops[.]com
- super-mario-deluxe[.]net
- takeforme[.]xyz
- te1[.]techgeetam[.]com
- vaishnaviinterior[.]com
- ve1[.]claker[.]top
- ve1[.]techgeetam[.]com
- ve2[.]techgeetam[.]com
- viayonetici[.]com
- videovip[.]org
- wetterkameras[.]com
- www-x-videos[.]com
- x-album[.]com
- x-album[.]net
- x-albums[.]net
- x-image[.]net
- x-images[.]com
- x-images[.]net
- x-photobucket[.]top
- xphotos[.]net
- x-photos[.]net
- xphotos-album[.]com
- x-picture[.]net
- xpictures[.]net
- x-pictures[.]net

Sample Additional IP Resolutions

- 2606:4700:3030::ac43:95df
- 2606:4700:3032::6815:5805

- 104[.]21[.]88[.]5
- 172[.]67[.]149[.]223
- 2606:4700:3030::6815:9d5
- 2606:4700:3031::ac43:a155
- 172[.]67[.]161[.]85
- 104[.]21[.]9[.]213
- 2606:4700:3030::ac43:9937
- 2606:4700:3030::6815:cc2
- 104[.]21[.]12[.]194
- 172[.]67[.]153[.]55
- 2606:4700:3036::ac43:a591
- 2606:4700:3034::6815:2ac7
- 172[.]67[.]165[.]145
- 104[.]21[.]42[.]199
- 2606:4700:3032::ac43:8550
- 2606:4700:3037::6815:de0
- 172[.]67[.]133[.]80
- 104[.]21[.]13[.]224
- 2606:4700:3032::ac43:80d0
- 2606:4700:3037::6815:23a
- 172[.]67[.]128[.]208
- 104[.]21[.]2[.]58
- 2606:4700:3034::ac43:bd7b
- 2606:4700:3037::6815:293f
- 172[.]67[.]189[.]123
- 104[.]21[.]41[.]63
- 2606:4700:3030::6815:1228
- 2606:4700:3037::ac43:b45b
- 104[.]21[.]18[.]40
- 172[.]67[.]180[.]91
- 2606:4700:3037::6815:4036
- 2606:4700:3037::ac43:b05e
- 104[.]21[.]64[.]54
- 172[.]67[.]176[.]94
- 2606:4700:3036::6815:134e
- 2606:4700:3037::ac43:b9a7
- 172[.]67[.]185[.]167
- 104[.]21[.]19[.]78
- 2606:4700:3036::ac43:8469
- 2606:4700:3035::6815:cd1
- 172[.]67[.]132[.]105
- 104[.]21[.]12[.]209
- 2606:4700:3034::ac43:bc0d
- 2606:4700:3031::6815:7d8
- 172[.]67[.]188[.]13
- 104[.]21[.]7[.]216
- 2606:4700:3033::6815:854
- 2606:4700:3030::ac43:8264

Sample IP-Connected Domains Using Common IoC Strings

- chatgptlogn[.]com
- chatgpt-premium[.]com
- freechatgpt[.]co
- chatgptz[.]xyz
- canva2023[.]com
- canvans[.]com[.]br
- canvasstudentclub[.]com
- 123movies800[.]online

Sample Email-Connected Domains

- basmah-ye[.]org
- aspaziua[.]com
- degree-du-hoc-anh[.]info
- tbkqp[.]cn
- yuehdar[.]com[.]tw
- colthing[.]info
- olite[.]com[.]cn
- mauriziomaranghi[.]us
- 8000ch[.]com
- 3dorgies[.]com
- 1ubr1[.]cn
- bascheti[.]top
- almusel[.]com
- 77877cp[.]com

- 04v0p[.]cn
- poker-s[.]org
- shfr[.]com[.]cn
- met-art[.]jp
- ca88yzcgw[.]com
- bigcocktwinks[.]net
- 22ago[.]cn
- boxetari[.]top
- arireklam[.]org
- admmmin[.]com
- 06txg1[.]cn
- metart[.]jp
- ca88yzcsj[.]com
- bitsensus[.]org
- 304bf[.]cn
- cellomusic[.]top
- baumannpvc[.]com
- amhg-18[.]com
- 0992cc[.]cn
- tovia[.]com
- msyz12c[.]com
- monstop-matome[.]com
- 37x4l[.]cn
- concerte[.]top
- birhevessonnefesinolmasin[.]com
- amjs-16[.]com
- 0a0501[.]cn
- qihuancheng88[.]com
- sexygayfriends[.]com
- 3i2o07[.]cn
- emailuri[.]top
- cocukeskisehir[.]com
- amjs-17[.]com
- 0mf69x[.]cn
- steadybackup[.]com
- 3mazl[.]cn

Sample String-Connected Domains

- movies-5e7a[.]onrender[.]com
- movies-alliance[.]com
- movies-api-bd5r[.]onrender[.]com
- movies-api-five-steel[.]vercel[.]app
- movies-api-tvar[.]onrender[.]com
- movies-app-application[.]herokuapp[.]com
- movies-app-cfrp[.]onrender[.]com
- movies-app-course-backend[.]onrender[.]com
- movies-app-dxxg[.]onrender[.]com
- movies-app-jbxn[.]onrender[.]com
- movies-app-kwxh[.]onrender[.]com
- movies-app-znui[.]onrender[.]com
- movies-asgv[.]onrender[.]com
- movies-back-end-1a5h[.]onrender[.]com
- movies-backend-api[.]onrender[.]com
- movies-backend-e7kg[.]onrender[.]com
- movies-booking-application[.]onrender[.]com
- movies-bot-cho7[.]onrender[.]com
- movies-ch6[.]pages[.]dev
- movies-chill[.]life
- movies-collection-2023[.]ml
- movies-crud-t2h2[.]onrender[.]com
- movies-database-server[.]onrender[.]com
- movies-e83a[.]onrender[.]com
- movies-ehg8[.]onrender[.]com
- movies-en[.]com
- movies-esonline[.]firebaseapp[.]com
- movies-explorer-api-u78y[.]onrender[.]com
- movies-favoritee[.]glitch[.]me
- movies-flix-rk[.]netlify[.]app

- movies-frchannel[.]firebaseapp[.]com
- movies-frday[.]firebaseapp[.]com
- movies-frtalk[.]firebaseapp[.]com
- movies-gilt-zeta[.]vercel[.]app
- movies-info-0biu[.]onrender[.]com
- movies-list-app-ten[.]vercel[.]app
- movies-listing-hetic[.]onrender[.]com
- movies-manha[.]blogspot[.]com
- movies-now[.]ph
- movies-ondemand[.]onrender[.]com
- movies-online[.]best
- movies-planet[.]vercel[.]app
- movies-pnbq[.]onrender[.]com
- movies-practice-sh-pedro[.]onrender[.]com
- movies-recommender-system-6irk[.]onrender[.]com
- movies-recommender-system-aqh2[.]onrender[.]com
- movies-review[.]online
- movies-shows-more[.]com
- movies-stream[.]site
- movies-techs[.]com
- movies-timber[.]com
- movies-tuof[.]onrender[.]com
- movies-v0gc[.]onrender[.]com
- movies-watchlist-uijg[.]onrender[.]com
- movies-watchonline[.]georgia[.]su
- movies-watchonline[.]net[.]ph
- movies-wsyl[.]onrender[.]com
- movies-xenosthordieter[.]blogspot[.]com
- movies-yrgg[.]onrender[.]com
- movies-z26[.]pages[.]dev
- x-album[.]net
- x-albumphoto[.]top
- x-albums[.]net
- x-image[.]com[.]de
- x-images[.]cn
- x-images[.]net
- x-photo[.]net[.]cn
- x-photo[.]plus
- x-photoalbum[.]top
- x-photobot[.]onrender[.]com
- x-photobucket[.]top
- x-photobucket[.]xyz
- x-photograph[.]blog
- x-photos[.]shop
- x-photos[.]space
- x-photoscape[.]net
- x-photoscape-org[.]translate[.]goog
- x-picture[.]net
- x-picture[.]xyz
- x-pictures[.]store

Sample Brand-Containing Domains

- canva2023[.]com
- canvapro2023[.]site
- canvas2023[.]top
- canvass2023[.]it
- chatgptpremium[.]chat
- chatgptpremium[.]com
- chatgpt-premium[.]com
- chatgpt-premium[.]com[.]de
- chatgptpremium[.]de
- chatgptpremium[.]nl
- chatgptpremium[.]online
- chatgptpremium[.]xyz
- chatgptpromptspremium[.]com
- movies-5e7a[.]onrender[.]com
- office-2023[.]com
- office-2023[.]net

- office-2023[.]nl
- office-ember-ofc-2023[.]direct[.]quickconnect[.]to
- office-hk2023[.]direct[.]quickconnect[.]to
- office-spaces-2023[.]xyz
- office-wps-2023[.]com