DNSでMessengerフィッシングの足跡をキャッチ

目次

1. 要旨
2. 付録：アーティファクトとIoCの例

要旨

最近、Facebookのビジネスアカウントを標的にしてパスワードを盗むマルウェアを使ったフィッシングキャンペーンが展開されています。攻撃者は、Facebookの偽アカウントおよび侵害されたアカウントの大規模なネットワークを駆使し、何百万ものフィッシングメッセージをMessengerで送信します。

MrTonyScamの一部と言われているこのフィッシャーは、通常、著作権違反を指摘したり、ある製品に関する詳細情報を要求したりします。被害者が添付されたRARまたはZIPアーカイブファイルをダウンロードすると、マルウェアドロッパーがGitHubリポジトリからペイロードを取得し、それが被害者のシステム上で実行されます。その後、マルウェアは被害者のブラウザに保存されているクッキーやログインデータを全て収集してZIPアーカイブにまとめ、攻撃者にそのアーカイブを送信します。

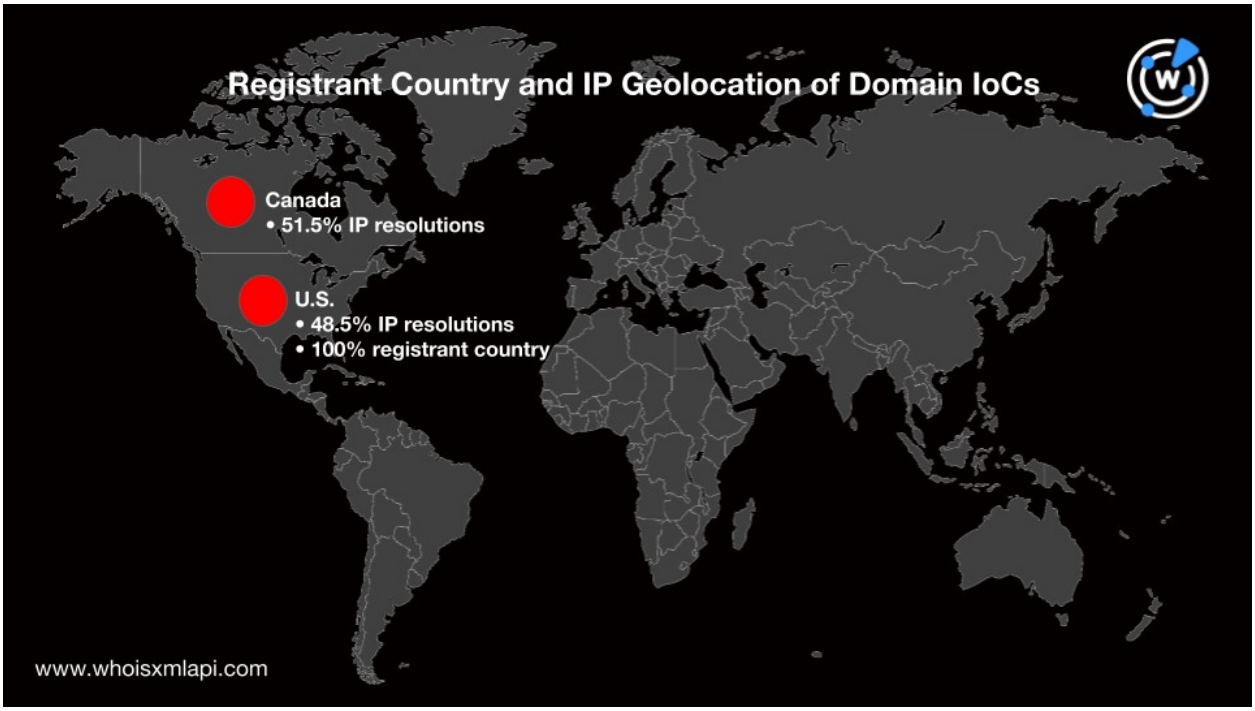
WhoisXML APIの研究者はこのほど、このキャンペーンに関連するセキュリティ侵害インジケーター（IoC）の公開リストを見つけました。そこで、リストで特定されている63個のドメイン名がDNSに残している痕跡を独自に調査しました。その結果、以下が明らかになりました。

- 関連性のあるドメイン名が50個未満のIoCを登録する際に使われた個人メールアドレス15個
- 共通のメールアドレスを使用していたドメイン名155個
- **movies-**、**office-**、**2023**、**x-album**など、IoCと同様の文字列を含むドメイン名924個
- IoCと同じ文字列を含み、かつ共通のIPアドレスを使用していたドメイン名18個

Messengerフィッシングのインフラ

IoCと特定されたドメイン名（以下「IoCドメイン名」）の名前解決をBulk IP Geolocation Lookupで分析したところ、約79%は180個のユニークなIPアドレスに解決しました。つまり、多くのドメイン名が複数（平均3～4個）のIPアドレスに名前解決したことになります。IPアドレスが地理的に位置していたのはカナダ（51.5%）と米国（48.5%）のみで、Cloudflareが全てのIPアドレスを管理している唯一のインターネットサービスプロバイダー（ISP）でした。

次に、IoCドメイン名をBulk WHOIS Lookupで検索したところ、WHOISデータの共通性が明らかになりました。全てのドメイン名はNameSiloというレジストラを介して登録され、WHOISレコードはPrivacyGuardianのサービスによって保護されていました。また、全てのドメイン名は米国の登録者によって登録されていました。



このように全てのドメイン名の特徴が酷似していることから、これらは同じ組織によって登録、管理されている可能性があります。または、レジストラがMessengerのフィッシングキャンペーンを発見してドメイン名を差し押さえた可能性もあります。

IoCが持つDNSとドメイン名の繋がり

いくつかのIoCドメイン名はすでに公に特定され様々なセキュリティプラットフォームで報告されている可能性がありますが、脅威アクターは他のドメイン名を準備しているかもしれません。後述しますが、当社が今回の調査で発見したIPアドレス、メールアドレスまたは文字列に共通点のあるドメイン名は、Messengerフィッシング詐欺の潜在的なアーティファクトと考えられます。

WHOISで関連付けられたアーティファクト

悪意あるドメイン名の過去のWHOISレコードを調査したところ、73個の登録者メールアドレスが公開されていました。

その多くはGmail、Yahoo、Naver、Liveなどの一般的なメールサービスによって取得されたものです。

次に、50個未満のドメイン名の登録に使われたメールアドレス15個に焦点を当て、それらをReverse WHOIS Searchで調べました。というのも、他のメールアドレスは数百、ものによっては数千にのぼるドメイン名の登録に使用されており、ドメイン名投資家のものかもしれないためです。このようにサンプル数を減らそうと試みたものの、メールアドレスで紐づいたドメイン名が155個残りました。そのうちアクティブに名前解決したのは15個でした。

共通の文字列を含むアーティファクト

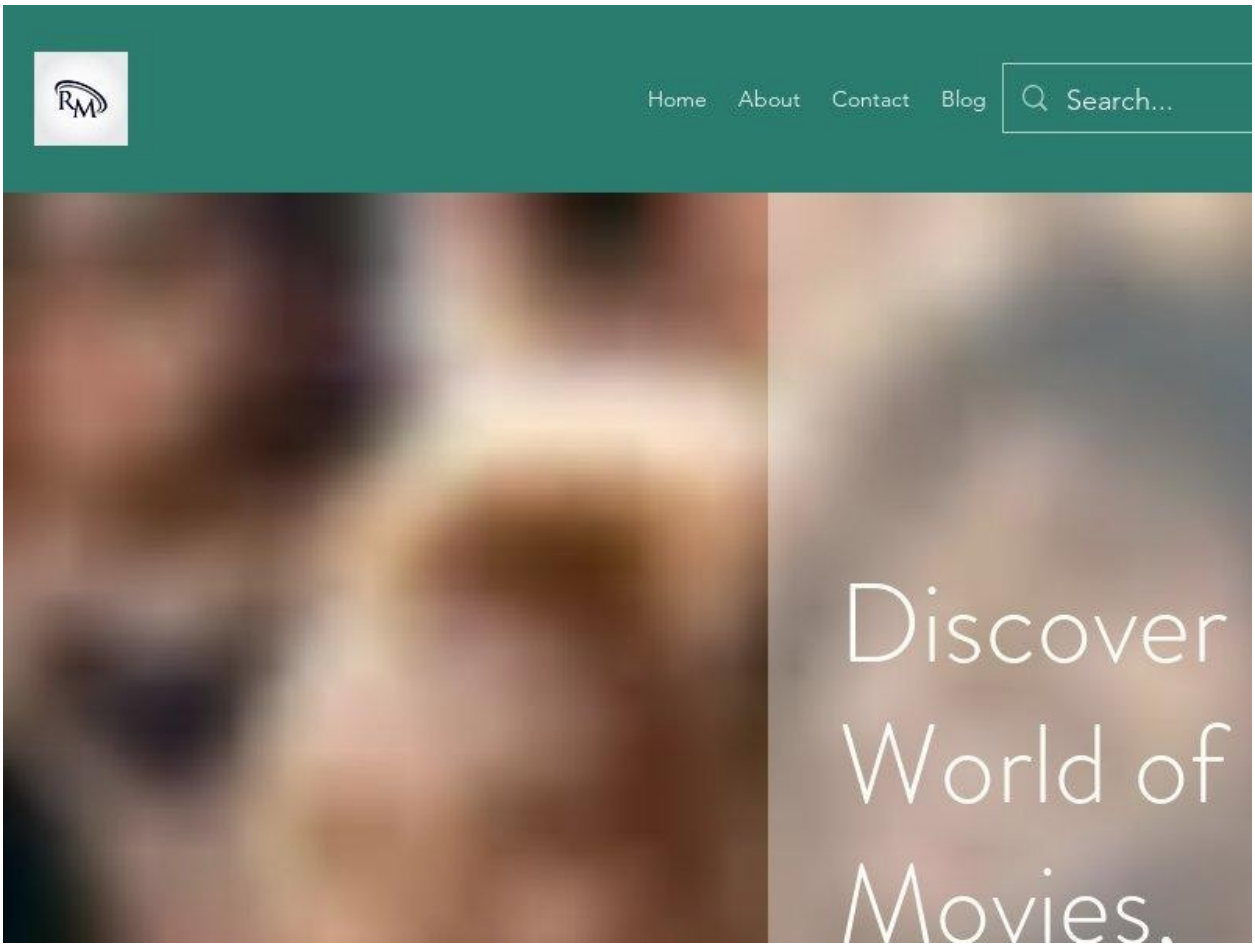
さらに、IoCにしばしば見られるものと同じ文字列を含むドメイン名を検索しました。具体的には、以下の文字列で始まるドメイン名をDomains & Subdomains Discoveryで探しました。

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

また、以下の条件に該当するドメイン名も探しました。

- **canva**で始まり、かつ**2023**を含む
- **office-**で始まり、かつ**2023**を含む
- **chatgpt**で始まり、かつ**premium**を含む

この検索の結果、2023年1月1日から9月18日までの期間に登録されたドメイン名が924個見つかりました。そのうちの約94%はまだ名前解決が有効な状態です。これらのドメイン名がMessengerのフィッシングキャンペーンに関与したとは限りません。しかし、一部はすでにマルウェアチェックの結果悪意あるドメイン名に分類されています。例えばmovies-shows-more[.]comは、以下のページをホストしているか、またはこのページにリダイレクトしていました。



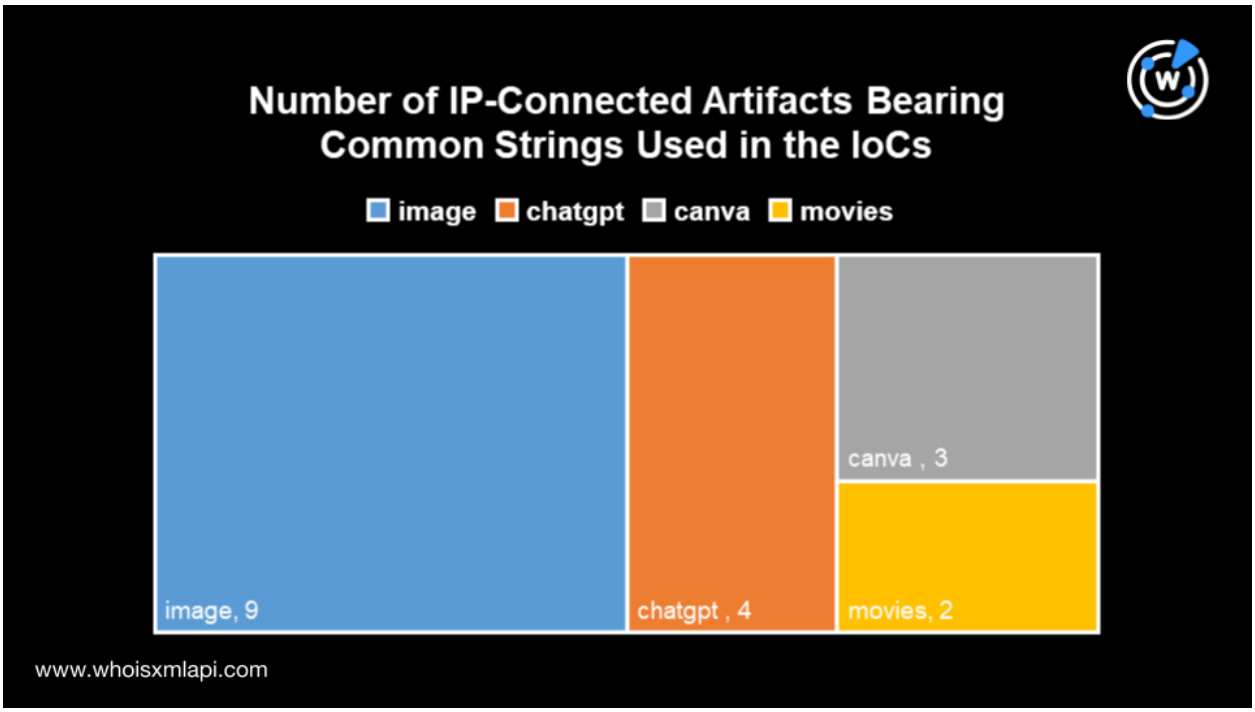
movies-shows-more[.]comのスクリーンショット

また、上記の検索で特定されたドメイン名がCanva、Office、ChatGPTなどのブランド名を使用していることも疑惑を引き起こします。

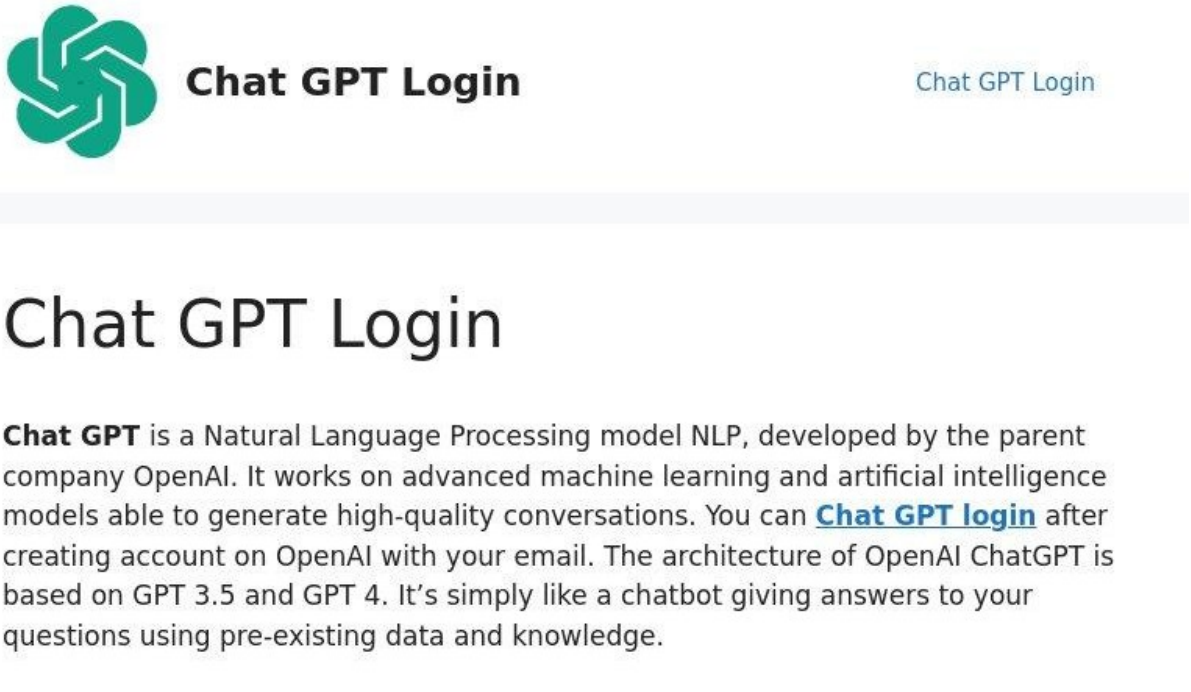
共通のIPアドレスを使用しているアーティファクト

次に、同じIPアドレスに名前解決する他のドメイン名を探すため、IoCドメイン名を[Reverse DNS Search](#)にかけました。その結果、各IPアドレスが300個を超えるドメイン名をホストしていたことから、IoCドメイン名は主に共用インフラ上でホストされていたと思われました。つまり、それらのアドレスは悪意あるIPネットワークの一部ではなく、複数のドメイン名が共有しているパブリックIPアドレスの可能性があります。

しかし、共通のIPアドレスに名前解決するドメイン名のいくつかは、一部のIoCドメイン名と同じ文字列を含んでいました。



そのようなドメイン名の一部は、不審なコンテンツをホストしていました。例えば、chatgptlogn[.]comのスクリーンショットから、このドメイン名が複数のログインリンクとChatGPTのロゴを含んだページをホストしていたことがわかります。



chatgptlogn[.]comのスクリーンショット

—

Messengerのフィッシングキャンペーンを対象に行った今回のDNS調査では、WHOIS、DNSおよび文字列の使用パターンから、既知のIoCと関連性を持つ不審な悪意あるプロパティが複数見つかりました。IoCリストの拡張作業から発展し、CanvaやChatGPTのユーザー、そしてオンラインで映画を閲覧している人々を狙った潜在的な悪意のキャンペーンを発見することができました。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

MessengerフィッシングのIoC

- 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

今回新たに見つかった名前解決の例

- 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

共通のIPアドレスを使用しIoCと同じ文字列を含んでいるドメイン名の例

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

共通のメールアドレスを使用しているドメイン名の例

- 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

共通の文字列を含むドメイン名の例

- 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

ブランド名を含むドメイン名の例

- 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