姿の見えないWailingCrabをDNSで解明

目次

1. 要旨
2. 付録：アーティファクトとIoCの例

要旨

IoTのメッセージングプロトコルであるMQTTを悪用したマルウェア「WailingCrab」は、そのステルス性で悪名を馳せています。

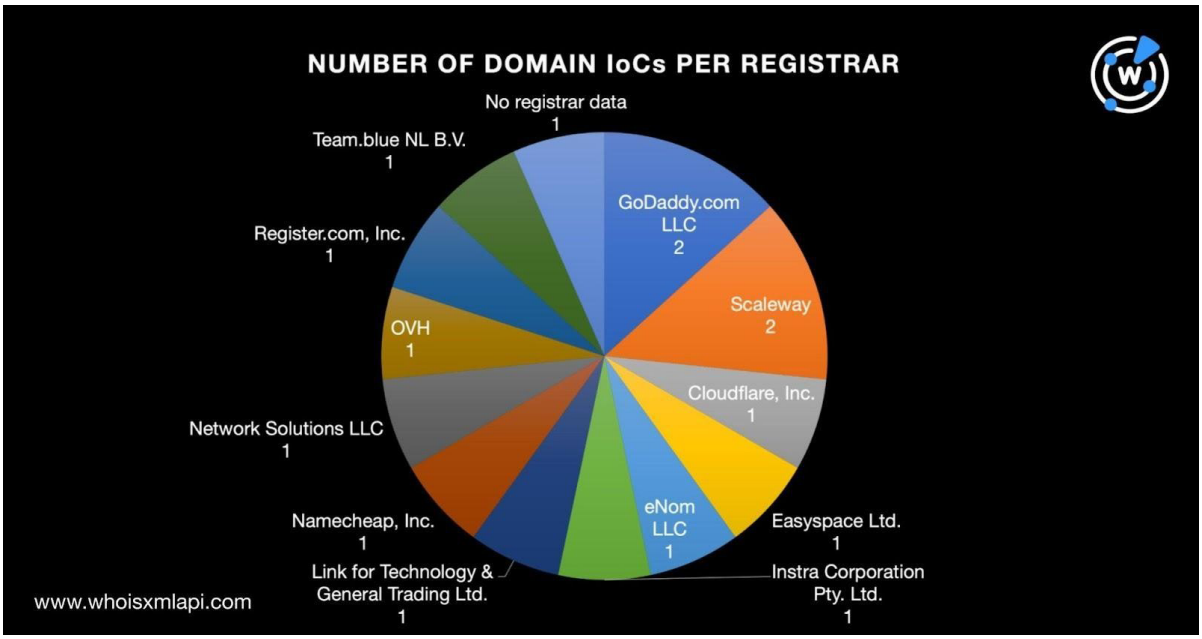
最近、IBM X-Forceのセキュリティ研究者がWailingCrabの詳細な分析結果を発表し、その中で1個のドメイン名と14個のURLを含む24個のセキュリティ侵害インジケーター（IoC）を特定しました。そこで、WhoisXML APIにおいてその14個のURLそれぞれからドメイン名を抽出し、合計15個のドメイン名のIoC（以下「ドメインIoC」）に整理し直しました。そしてそのドメインIoCを詳しく調査した結果、以下が検出されました：

- IoCの過去のWHOISレコードで見つかった公開メールアドレスをWHOISレコードに含むドメイン名26個
- IoCが名前解決したIPアドレス17個
- IoCの専用ホストと思われるIPアドレスを共用していたドメイン名524個
- IoCと共通の文字列を含むドメイン名978個
- IoCと共通の文字列を含むサブドメイン2,002個

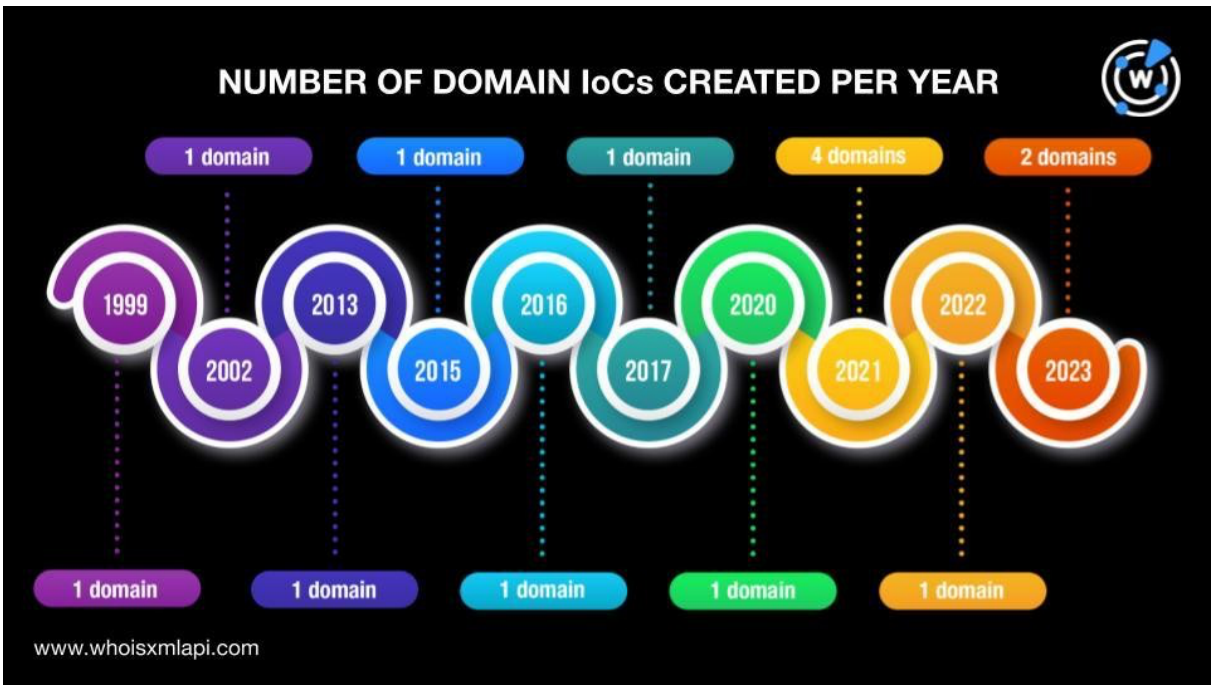
WailingCrabのIoC

まず、15個のドメインIoCをBulk WHOIS Lookupで検索したところ、以下が明らかになりました：

- レジストラのGoDaddy.com LLCとScalewayが、それぞれ2個のドメインIoCを管理していました。また、10個のドメイン名は10社の異なるレジストラによって管理されていました。残りの1個のドメイン名については、レジストラ情報を取得することができませんでした。

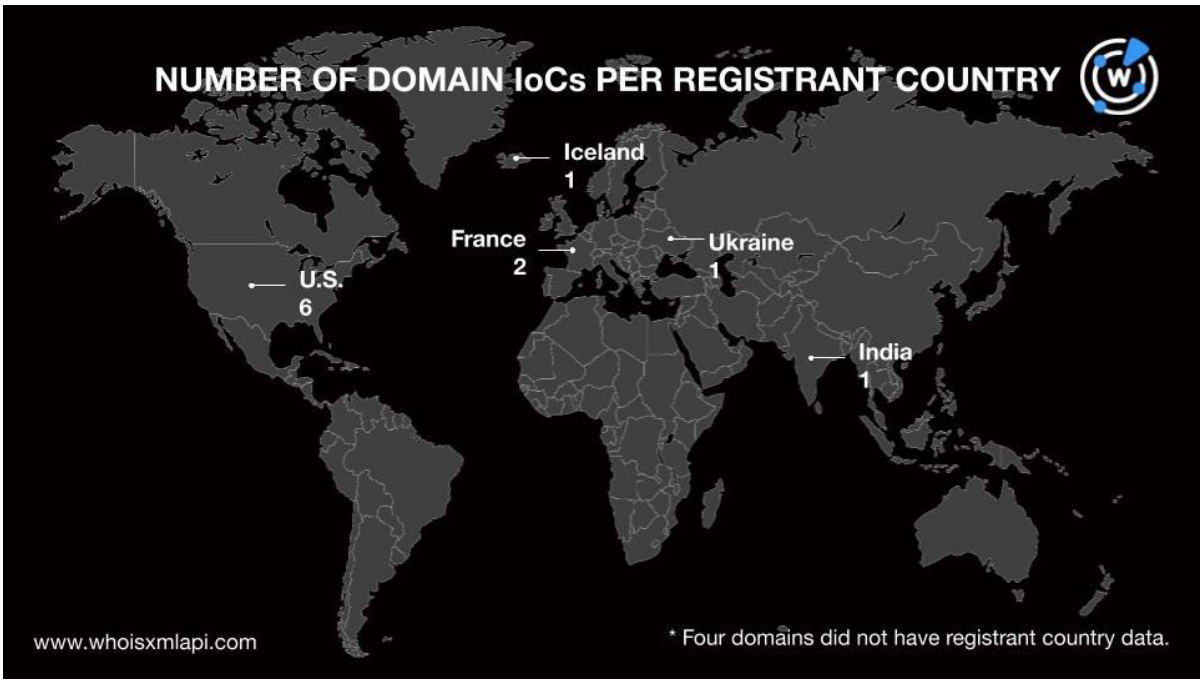


- 4個のドメインIoCは2021年に、2個は2023年に新規登録されたものでした。また、1999年、2022年、2013年、2015年、2016年、2017年、2020年、2022年に1個ずつ新規登録されていました。残りの1個のドメイン名については、新規登録日がWHOISで公開されていませんでした。



- どのドメイン名も登録者名と登録者のメールアドレスが編集されて非公開になっていましたが、4個については登録者の組織名が公開されていました。

- 最も多くのドメインIoCが登録されていた国は米国（6個）で、2位はフランス（2個）でした。また、アイスランド、インド、ウクライナでそれぞれ1個が登録されていました。なお、4個のドメインIoCには登録者の国に関する情報がありませんでした。



DNSのレンズを通して見るWailingCrabのインフラ

他の潜在的な関連アーティファクトを洗い出すため、15個のドメインIoCについてWHOIS History Searchを実行しました。その検索結果から重複を削除し、最終的に過去のWHOISレコードに掲載されていた94個のメールアドレスを特定することができました。

さらに、1〜50ドメインの現在のWHOISレコードに表示され、かつプライバシー保護（非公開化）されていないものに条件を絞り、94個のメールアドレスをReverse WHOIS Searchにかけました。その結果、条件に合致するメールアドレスが6個残りました。重複とドメインIoCを取り除いた後の状態で、それらのメールアドレスは26個の別のドメイン名で共用されていました。

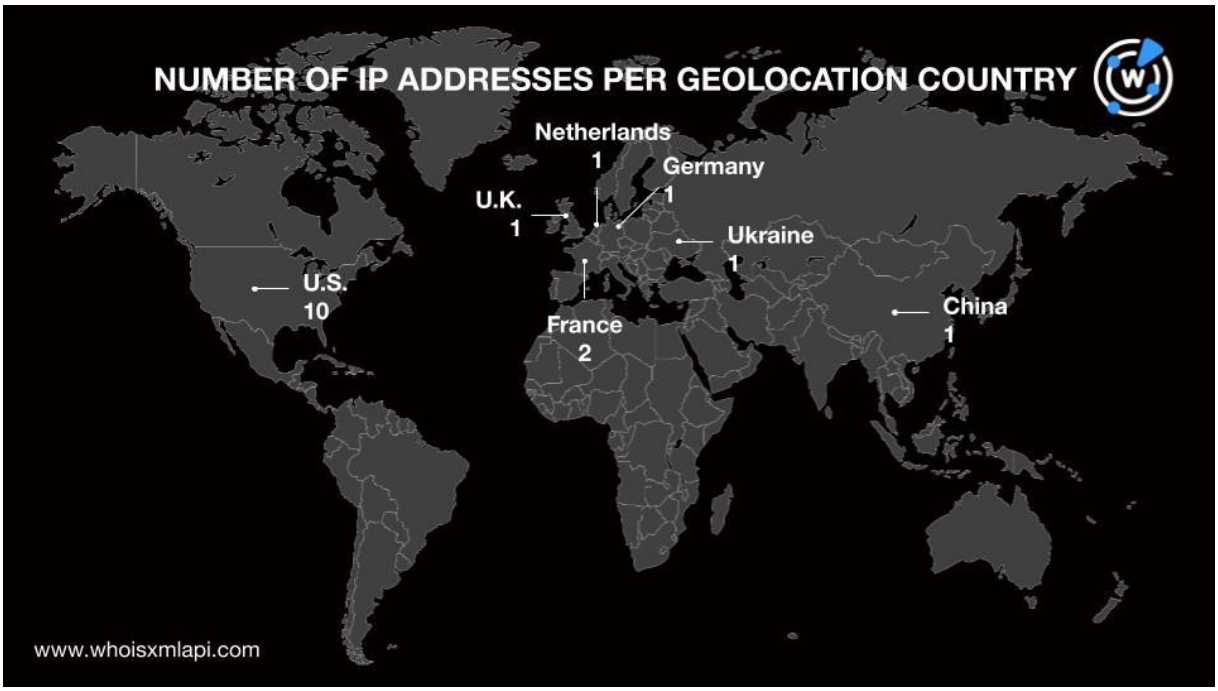
それらのドメイン名をScreenshot Lookupで検索したところ、共通のメールアドレスを使用しているドメイン名のうち5個が、有効なコンテンツをホストし続けていることが判明しました。しかし、一見したところ機能しているウェブサイトに繋がったのは2個だけでした。残りの3個のドメイン名は、エラーページまたは空白のページに誘導されるか、あるいはパークされていました。

共通のメールアドレスを使用していたドメイン名「**767cq[.]com**」のスクリーンショット

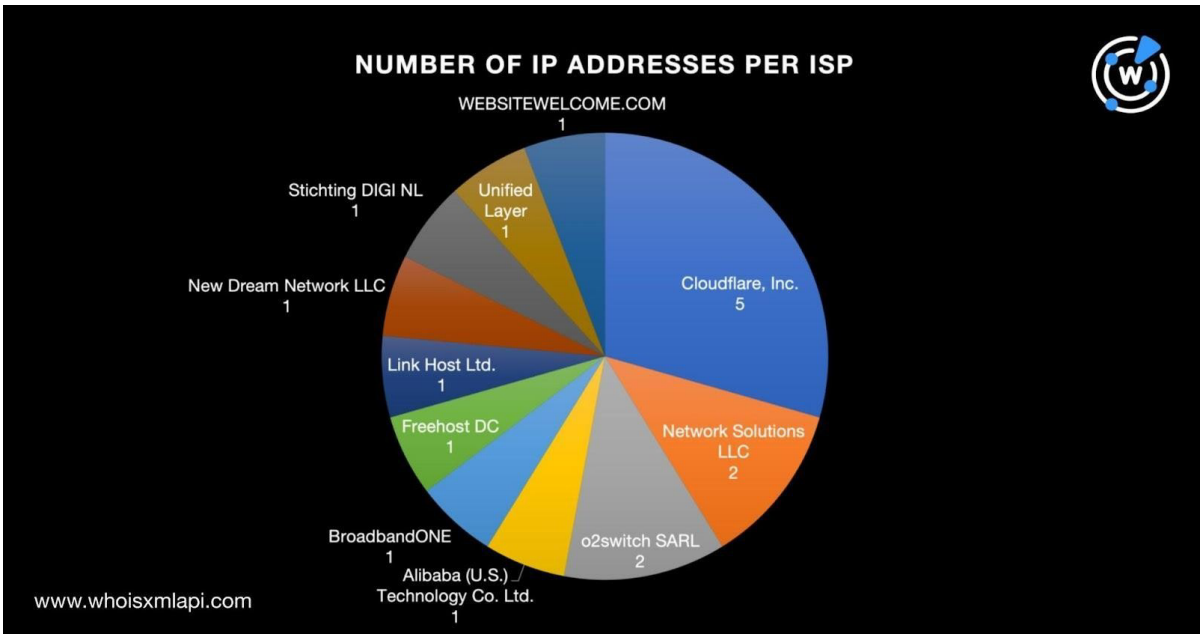
共通のメールアドレスを使用していたドメイン名「**sporactif[.]fr**」のスクリーンショット

次に、15個のドメインIoCをDNS Lookupにかけたところ、17個のユニークなIPアドレスに名前解決しました。その17個のIPアドレスをIP Geolocation Lookupで調べた結果、以下が判明しました：

- 10個は米国を指していました。2個はフランスに位置していました。また、中国、ドイツ、オランダ、英国、ウクライナに1個ずつありました。



- 最も多くのIPアドレスを管理していたISPはCloudflare, Inc.（5個）でした。次いで多かったのはNetwork Solutions LLCとo2switch SARLで、それぞれ2個を管理していました。この他、Alibaba (U.S.) Technology Co. Ltd.、BroadbandONE、Freehost DC、Link Host Ltd.、New Dream Network LLC、Stichting DIGI NL、Unified Layer、WEBSITEWELCOME.COMが1個ずつ管理していました。



- さらに、Threat Intelligence Lookupにより、特定された17個のIPアドレスのうち12個がそれぞれ1～3件の脅威と関連していることも判明しました。詳細は下表の通りです。

IPアドレス	THREAT INTELLIGENCE LOOKUPの結果	関連する脅威の種類
109[.]234[.]161[.]16	2件の脅威に関連	Phishing Malware
162[.]159[.]129[.]233	3件の脅威に関連	Malware Attack Generic
162[.]159[.]130[.]233	2件の脅威に関連	Malware Generic
162[.]159[.]133[.]233	2件の脅威に関連	Malware Generic

162[.]159[.]134[.]233	2件の脅威に関連	Malware Generic
162[.]159[.]135[.]233	2件の脅威に関連	Malware Generic
162[.]241[.]224[.]104	3件の脅威に関連	Phishing Malware Generic
185[.]104[.]29[.]64	2件の脅威に関連	Phishing Malware
185[.]13[.]5[.]52	1件の脅威に関連	Malware
188[.]64[.]139[.]53	1件の脅威に関連	Phishing
209[.]17[.]116[.]165	1件の脅威に関連	Phishing
50[.]116[.]86[.]129	2件の脅威に関連	Phishing Malware

また、17個のIPアドレスをReverse IP Lookupで検索したところ、9個は専用ホストで、それぞれがホストしているドメイン名の数は300個未満でした。重複、IoCおよび共通のメールアドレスを使用しているドメイン名を取り除いた後の状態で、合計524個のドメイン名がそれらのIPアドレスでホストされていたことがわかりました。

そのうち3個のドメイン名は、以下のように著名なブランド名を文字列として含んでいました：

- amazoneng[.]com[.]br
- zoom-business-simulation[.]com
- zoomsim[.]io

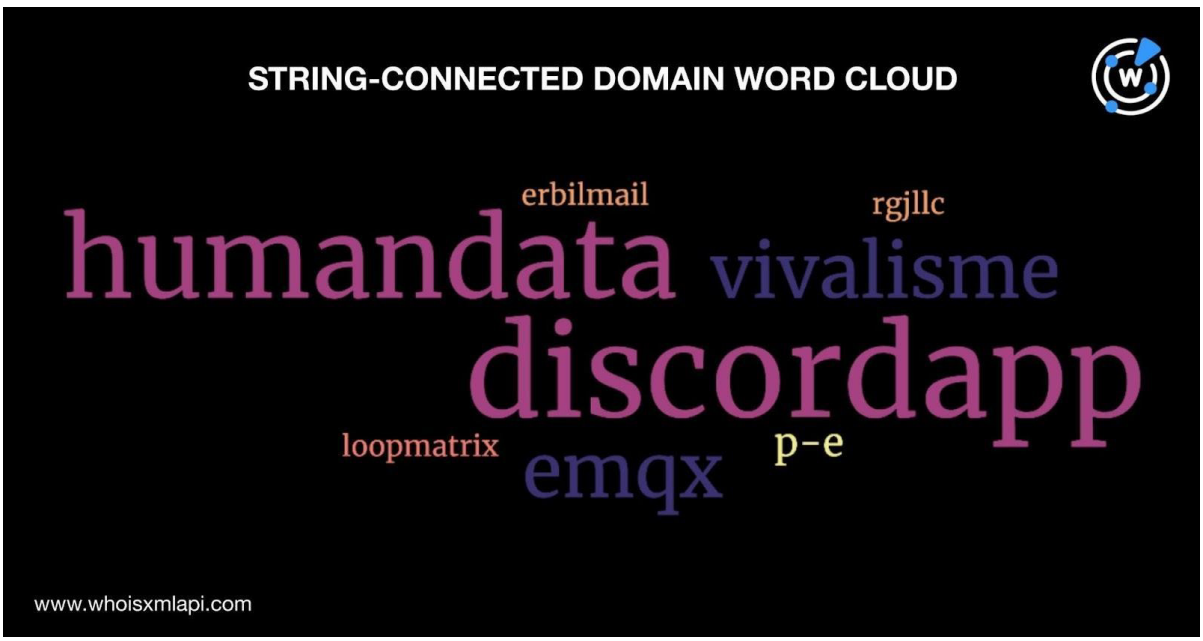
WHOIS Lookupを使い、上記の3個のドメイン名とAmazonの公式ドメイン名「amazon[.]com」およびZoomの公式ドメイン名「zoom[.]us」を比較したところ、上記の3個のドメイン名のいずれも、AmazonまたはZoomへの帰属をWHOISデータから確認できませんでした。具体的には：

- Amazoneng[.]com[.]brの登録者名、組織名、メールアドレスはamazon[.]comのそれと合致しませんでした。
- Zoom-business-simulation[.]comとzoomsim[.]ioの登録者名、組織名、メールアドレスはzoom[.]usのそれと合致しませんでした。

最後に、ドメインIoCに見られる以下の文字列を含んだドメイン名およびサブドメインをDNSで探しました。

- **discordapp**
- **emqx.**
- **erbilmail**
- **flow.**
- **humandata**
- **loopmatrix**
- **p-e-c.**
- **rgjllc**
- **vivalisme**

Domains & Subdomains Discoveryを実行した結果から重複、IoC、共通のメールアドレスまたは共通のIPアドレスを使用しているドメイン名を取り除いたところ、978個のドメイン名、2,002個のサブドメインが特定されました。なお、**flow.**を含むドメイン名とサブドメインは、合致するものがそれぞれ10,000個を超えており、大量の誤検出が含まれている可能性があるため、対象から除外しました。以下は、ドメイン名およびサブドメインに含まれる文字列を示したワードクラウドです。



—

WailingCrabのIoCリストをもとに当社で行った分析の結果、23の既知の脅威に関連している12個のIPアドレスを含む、3,547個の関連アーティファクトが新たに検出されました。

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

WailingCrabのIoC

- advocates4consumerprotection[.]com
- discordapp[.]com
- emqx[.]io
- epikurgroup[.]com
- erbilmail[.]com
- flow[.]enterprises
- humandata[.]solutions
- inspiration-canopee[.]fr
- loopmatrix[.]in

- luna-render[.]com
- p-e-c[.]nl
- rgjllc[.]pro
- studiolegalcarduccimacuzzi[.]it
- dc1-mtp[.]fr
- vivalisme[.]fr

IoCと同じメールアドレスを使用していたドメイン名の例

- 1st-360vr[.]com
- 40nb[.]com
- 4etong[.]com
- 510girl[.]com
- 51entry[.]com
- 51shangtao[.]com
- 51tgpm[.]com
- 52fanqian[.]com
- 61fushi[.]com
- 767cq[.]com
- 7lnk[.]com
- aisi301[.]com

IoCが名前解決したIPアドレスの例

- 109[.]234[.]161[.]16
- 109[.]234[.]161[.]167
- 162[.]159[.]129[.]233
- 162[.]159[.]130[.]233
- 162[.]159[.]133[.]233
- 162[.]159[.]134[.]233
- 162[.]159[.]135[.]233
- 162[.]241[.]224[.]104

IoCの専用ホストと思われるIPアドレスを共用していたドメイン名の例

- 1wp[.]com[.]br
- 247praise[.]com
- 2wdstore[.]com[.]br
- 317board[.]com
- 40lauriedrive[.]com
- 5tons[.]com
- 5tonscreative[.]com
- 8kgestaodemarcas[.]com[.]br
- abbottsfieldreccentre[.]com
- acmautomacao[.]com[.]br
- adrianodamas[.]com[.]br
- aefretifica[.]com[.]br
- afinadoscomamusica[.]com[.]br
- agenciafiber[.]com
- agenciafiber[.]com[.]br
- aguaesanea[.]com[.]br
- ahonkinggoose[.]com
- akhilaretreat[.]com
- alcsrv01[.]com[.]br
- aliancaautocenter[.]com[.]br
- almeidaartesanato[.]com[.]br
- alphaprincess[.]com
- amazoneng[.]com[.]br
- anchietabatidos[.]com[.]br
- andreabrooks[.]net
- andreabrookslcsw[.]com
- aobe[.]com[.]br
- aplikvisual[.]com[.]br
- ardoce[.]org[.]br
- arqfranciscojc[.]com[.]br
- art100limites[.]com[.]br
- artemisambiental[.]com
- artemisambiental[.]com[.]br
- audioarsenal[.]com
- audioarsenal[.]net
- autoeletricadonadon[.]com[.]br
- autoescolajvc[.]com[.]br
- babykillerwhale[.]com

- baraoestruturas[.]com[.]br
- bardavilaitaim[.]com[.]br
- basefortte[.]com[.]br
- bbusiness[.]ch
- bcmncorporation[.]com
- bdlucid[.]com
- bhiwadi[.]com
- bilhetex[.]com[.]br
- birdstar[.]com[.]br
- bmfplumbingllc[.]com
- bnbsync[.]co
- bnbsync[.]net
- bnbsync[.]org
- bnbtally[.]co
- bnbtally[.]com
- bnbtally[.]io
- bnbtally[.]net
- bnbtally[.]org
- bohicaconsultingtx[.]com
- bolosetortasdafatinha[.]com[.]br
- bradyhallstuff[.]com
- brawash[.]com[.]br
- breakthroughloading[.]com
- brentheeringa[.]com
- britnipatterson[.]com
- brooksideas[.]com
- brunabochnia[.]com[.]br
- buuug[.]com
- c4tc[.]co
- caartists[.]com
- cadeiraelevatoriasurimex[.]com[.]br
- cadeirastannah[.]com[.]br
- cafeina[.]digital
- camaradepaulistas[.]mg[.]gov[.]br
- camarasobralia[.]mg[.]gov[.]br
- candeloroengenharia[.]com[.]br
- capsindustry[.]com
- carladaniele[.]com[.]br
- caroneseguranca[.]com[.]br
- carrosbatidoss[.]com[.]br
- cashdomme[.]com
- casino-elliniko[.]com
- casinomarousi[.]com
- catchmeifucanbbq[.]com
- caucaiameular[.]com
- cbmaraba[.]com[.]br
- ccbbatidos[.]com[.]br
- cemporcentoenvelopes[.]com[.]br
- ceofloripa[.]com[.]br
- cervejariagotter[.]com[.]br
- chamine[.]cc
- charlotteswebcreations[.]com
- chriscollenberger[.]com
- citizensliberatingmichigan[.]com
- clinicaamorim[.]med[.]br
- clinicaanima[.]odo[.]br
- clinicadeolhoscottini[.]com[.]br
- clinicaespacovillage[.]com
- clinicarubiamota[.]com[.]br
- clinicaun[.]com[.]br
- clubedosposts[.]com[.]br
- cmxprojetos[.]com[.]br

IoCと共通の文字列を含むドメイン名の例

- 1aemqx[.]icu
- 3dhumandatabse[.]com
- 3dhumandataset[.]com
- 4memqx[.]tokyo
- 7emqx[.]wang
- 7s-discordapp[.]com
- a-p-e-c[.]com
- abcdemqx[.]cn
- academie-survivalisme[.]com
- academie-survivalisme[.]fr
- academiesurvivalisme[.]com
- academqx[.]ru

- academy-discordapp[.]club
- activzemqx[.]cf
- activzemqx[.]ga
- adiscordapp[.]com
- aide-survivalisme[.]fr
- aihumandata[.]com
- apprendre-survivalisme[.]fr
- aremqx[.]online
- asemqx[.]work
- assaaemqx[.]com
- autonomie-survivalisme[.]com
- autonomie-survivalisme[.]fr
- bapkemqx[.]loan
- bdiscordapp[.]com
- beta-discordapp[.]ml
- betterdiscordapp[.]com
- betterdiscordapps[.]com
- bgemqx[.]com
- bighumandata[.]com
- blademqx[.]com
- blogsurvivalisme[.]com
- boutique-survivalisme[.]com
- boutique-survivalisme[.]fr
- boutiquedesurvivalisme[.]com
- boutiquedusurvivalisme[.]com
- boutiquedusurvivalisme[.]net
- boutiquedusurvivalisme[.]org
- boutiquedusurvivalisme[.]site
- brokeremqx[.]tk
- bsemqx[.]live
- btpgaemqx[.]club
- bushcraftetsurvivalisme[.]com
- bushcraftetsurvivalisme[.]eu
- bushcraftetsurvivalisme[.]fr
- c-i-p-e-c[.]com
- canarydiscordapp[.]com
- casartemqx[.]ac[.]cn
- casartemqx[.]cn
- casartemqx[.]com[.]cn
- casartemqx[.]net[.]cn
- casartemqx[.]org[.]cn
- cdd8emqx[.]top
- cddiscordapp[.]com
- cdiscordapp[.]com
- cdn-discordapp-com-attachments-532533534535-542543544545[.]ml
- cdn-discordapp[.]co
- cdn-discordapp[.]com
- cdn-discordapp[.]net
- cdn-discordapp[.]tk
- cdn-discordapp[.]xyz
- cdndiscordapp[.]com
- cdndiscordapp[.]ga
- cdndiscordapp[.]ml
- cdndiscordapp[.]xyz
- cdndotdiscordapp[.]com
- cdnxdiscordapp[.]com
- cdnydiscordapp[.]com
- chemqx[.]com
- chephumandata[.]com
- clxlb7dkzkymi7hx6br4itcekqydftc8onn9m4bz5pkq5ukylw5emqx[.]ws
- codiscordapp[.]com
- comdiscordapp[.]com
- comptoirdusurvivalisme[.]com
- comptoirdusurvivalisme[.]fr
- corddiscordapp[.]com
- corsicasurvivalisme[.]com
- cxemqx[.]buzz
- ddiscordapp[.]com
- designhumandata[.]net
- digitalhumandata[.]com
- digitalhumandata[.]org
- discdiscordapp[.]com
- discdiscordapp[.]ws
- discordapp-academy[.]com
- discordapp-academy[.]info
- discordapp-addon[.]com
- discordapp-addons[.]com
- discordapp-addons[.]net

- discordapp-application[.]com
- discordapp-applications[.]com
- discordapp-clone[.]com
- discordapp-download[.]space
- discordapp-events[.]com
- discordapp-fix[.]com
- discordapp-forms[.]com
- discordapp-formulary[.]com
- discordapp-formulary[.]ws
- discordapp-get[.]ru

IoCと共通の文字列を含むサブドメインの例

- discordapp[.]h6[.]fan
- billingwetransfericu-discordappsa[.]firebaseapp[.]com
- discordapp[.]aisilop[.]info
- discordapp[.]copowen[.]info
- autodiscover[.]discordapp[.]com[.]de
- discordapp[.]ww9[.]myhippo-comscm[.]payusaklarna[.]com
- www[.]discordapp[.]earlytrans[.]com
- www[.]discordapp[.]faceofabovebeauty[.]com[.]ng
- smtp[.]discordapplike[.]cz[.]cx
- server-discordapp[.]kathurian[.]uk
- discordapp[.]nmly[.]cc
- ww8discordapp[.]myhippo-com[.]php[.]payusaklarna[.]com
- ww4[.]discordapp-myhippo-com[.]payusaklarna[.]com
- discordapp[.]net[.]us3[.]cas[.]ms
- khakilameharddrive[.]discordapp[.]repl[.]run
- discordapp[.]auth0[.]net
- ww8[.]discordappppriv[.]payusaklarna[.]com
- discordapp[.]openai[.]army
- discordappww4[.]devstage5-com[.]payusaklarna[.]com
- ww4[.]myhippo-com[.]discordapp[.]origin-community[.]payusaklarna[.]com
- discordappdownload48259[.]jaiblogs[.]com
- 0[.]images-ext-2[.]discordapp[.]net[.]53b6[.]lo-01234567[.]v4[.]pcp[.]lookout[.]com
- ww2[.]manage[.]paylution[.]shbmgidiscordappnba2k[.]comsvc[.]unifiedaccessmanagement[.]com
- discordapp[.]perfectluxsistem[.]rs
- discordapp[.]2016-milkteaday-voting[.]bnw[.]dev[.]atg[.]se
- discordapp[.]xlf68[.]cn
- cdndiscordapp[.]pages[.]dev
- cdn-discordapp[.]aliexpress[.]vip
- smooch-web-shbmgidiscordapp[.]directly[.]com
- support-testdiscordapp[.]zendesk[.]com
- discordapp[.]pages[.]dev
- ww4[.]produtomyhippo-com[.]discordapp[.]payusaklarna[.]com
- ww9[.]myhippo-comdiscordapp-secret-manager[.]payusaklarna[.]com
- discordapp[.]com[.]admin-mcas-gov[.]us
- cdn-discordapp-com[.]guardstudio[.]com
- discordapp[.]comone2fan[.]mobz[.]link
- discordapp[.]net[.]cit[.]congruentindia[.]com
- discordapp[.]fhadeyprofessionalhairstylist[.]com
- discordapp[.]bitzy[.]cn

- www[.]discordapp[.]1ck[.]me
- discordapp[.]page[.]link
- www[.]discordapp[.]samphilsdiapers[.]com
- 0[.]cdn[.]discordapp[.]com[.]be37[.]lo-01234567[.]v4[.]pcp[.]lookout[.]com
- discordappww8[.]mybackend[.]payusaklarna[.]com
- discord--discordapp[.]repl[.]co
- ww8[.]us-east-1-stagingdiscordapp[.]payusaklarna[.]com
- cdn-discordapp[.]7-7[.]fun
- ww8[.]myhippo-com-controldiscordapp[.]payusaklarna[.]com
- discordapp[.]useropen[.]cloud
- ww9[.]hippo-com-br[.]discordapp[.]payusaklarna[.]com
- discordapp[.]ww9[.]rivals-com[.]payusaklarna[.]com
- 1-dl--ptb-discordapp-net[.]translate[.]goog
- discordapp[.]blinewd[.]info
- cdn[.]discordapp[.]attatchments[.]com
- images-ext-1[.]discordapp[.]net[.]psyche[.]tny[.]town
- discordapp[.]dozacinv[.]com[.]ng
- cdn[.]discordapp[.]xacx[.]net
- rabbitmq-admin[.]sandbox-comdiscordapp[.]directly[.]com
- discordapp-ww4[.]myhippo-com-central[.]payusaklarna[.]com
- discordapp-com[.]connext[.]com[.]co
- discordapplications[.]cf[.]discord[.]holiday
- discordapp[.]signalcorefx[.]com
- discordapp[.]balgend[.]info
- 0[.]media[.]discordapp[.]net[.]c1f5[.]lo-01234567[.]v4[.]pcp[.]lookout[.]com
- news-wetransfericu-discordappsa[.]firebaseapp[.]com
- www[.]discordapp[.]comone2fan[.]mobz[.]link
- discordapp[.]repl[.]run
- cdn-discordapp-com[.]273679[.]xyz
- discordapp[.]metesys[.]com
- ml-service[.]cdiscordappbox[.]directly[.]com
- cdn[.]discordapp[.]com[.]ididitfor[.]fun
- vnc-discordapp[.]artifactory[.]evonik[.]com
- ww9[.]myhippo-com[.]discordapp[.]pub1[.]payusaklarna[.]com
- media[.]discordapp[.]net[.]mtsrouter[.]net
- comdiscordapp-ww2[.]manage[.]paylution[.]nba2k[.]comsvc[.]unifiedaccessmanagement[.]com
- discordapp[.]calderaconsultants[.]com
- www[.]discordapp[.]just[.]a2hosted[.]com
- discordapp[.]galacticinvestors[.]com
- discordapp-ww4[.]myconnectwisemyhippo-com[.]payusaklarna[.]com
- ww4[.]uploads[.]discordapp-myhippo-com[.]payusaklarna[.]com
- ww9[.]wholesaleae1[.]discordapp[.]ae1warrior[.]payusaklarna[.]com
- ww9[.]discordapp-comnojs[.]payusaklarna[.]com
- ww2[.]discordappleimdsrp[.]paylutionnba2k[.]com[.]unifiedaccessmanagement[.]com

- www[.]discordapp[.]com[.]hyperboy13[.]cf
- discordapp[.]co[.]com[.]au
- discordapp[.]berynch[.]info
- discordapp[.]com[.]admin-us[.]cas[.]ms
- discordapptest[.]gitlab[.]appsflyer[.]com
- discordapp[.]ww8[.]myhippo-com-frontpage[.]payusaklarna[.]com
- www[.]discordapp[.]roemahmarthatilaar[.]org
- discordapp[.]clopker[.]info
- discordappsa-whatsapp-clone-738d9[.]firebaseapp[.]com
- discordapp[.]sapioclub[.]com
- ww2[.]mobileimdsrp[.]shbmgidiscordapp-paylution[.]nba2k[.]com[.]unifiedaccessmanagement[.]com
- cdn[.]discordapp[.]zhitiands[.]net
- www[.]discordapp[.]earlycargo[.]com
- ww2[.]mobileimdsrp[.]shbmgidiscordapppaylution[.]nba2k-com[.]unifiedaccessmanagement[.]com
- cdn[.]discordapp[.]com[.]infiniterecall[.]com
- www[.]discordapp[.]ndukakpompcs[.]com[.]ng
- ww8-discordapp[.]ctl-myhippo-com[.]payusaklarna[.]com