



QRコードフィッシングの痕跡をDNSで探す

目次

1. [要旨](#)
2. [付録：アーティファクトとIoCの例](#)

要旨

QRコードは人々の生活を便利にするはずの技術ですが、昨今ではフィッシングに悪用されています。複数の調査結果によれば、今や[世界人口の86%](#)が金融を含む全ての取引に携帯電話を使用しています。したがって、QRコードフィッシングの増加も驚くべきことではありません。

QRコードがフィッシングに使われる背景には、標的になり得る人の数が多いこと、そしてオープンソースというQRコードの性質があると考えられます。また、QRコードの正当性を判断するのがハイパーリンクの場合よりもはるかに難しいとことも、理由のひとつでしょう。

最近、Trustwaveの研究者がこの傾向に着目し、QRコードを使った進行中のフィッシング詐欺に関する[詳細な調査](#)の結果を公開しました。これには、セキュリティ侵害インジケータ（IoC）として特定された18個のURLが含まれています。そこで、WhoisXML APIではこのほど、未報告の潜在的な関連アーティファクトを特定して同様の攻撃を防ぐべく、DNSを詳細に調査しました。その結果、以下が明らかになりました。

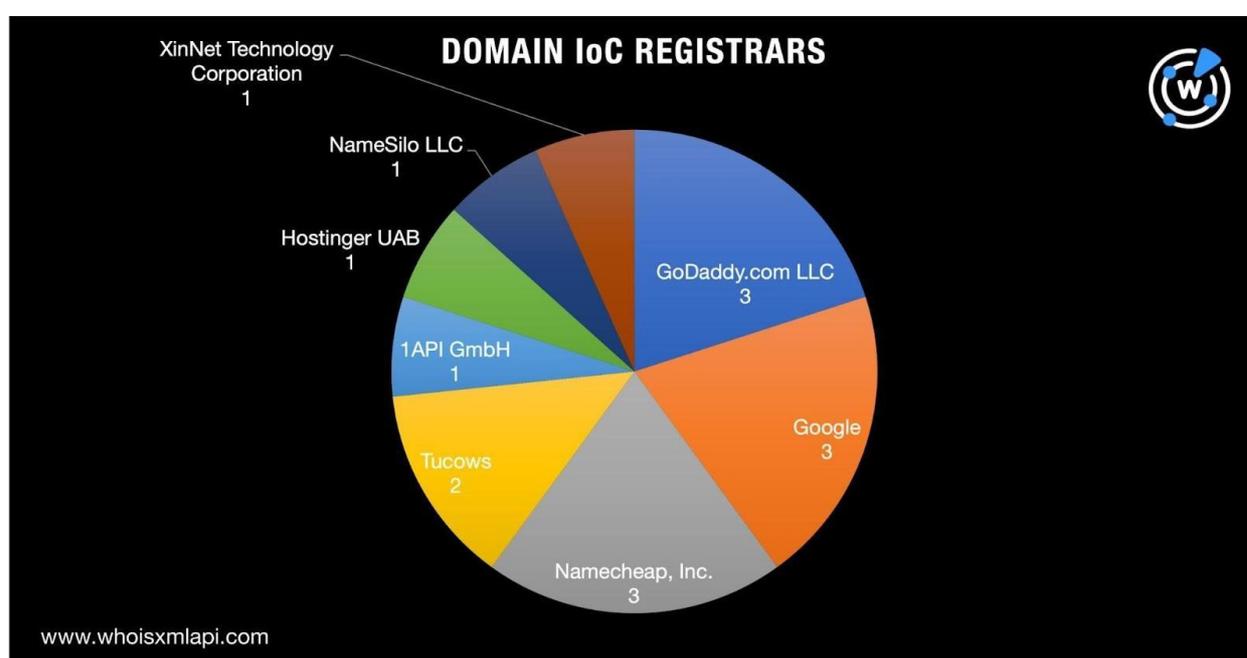
- IoCの1つとWHOISの登録者組織名が同一であったドメイン名10,000個。マルウェア一括チェックの結果、そのうち10個は悪意あるドメイン名と判明
- IoCである18のURLから抽出したドメイン名が名前解決した10個のユニークなIPアドレス
- それらのドメイン名が名前解決したおそらく専用のIPアドレスを共用する別の114個のドメイン名。マルウェア一括チェックの結果、そのうち26個は悪意あるドメイン名と確認
- URLから抽出したドメイン名の一部に見られたものと同じテキスト文字列を含む10,045個のドメイン名。マルウェア一括チェックの結果、そのうち4個は悪意あるドメイン名と確認
- URLから抽出したドメイン名のうち1個と同様にqr.codesという文字列を含んだ30個のドメイン名



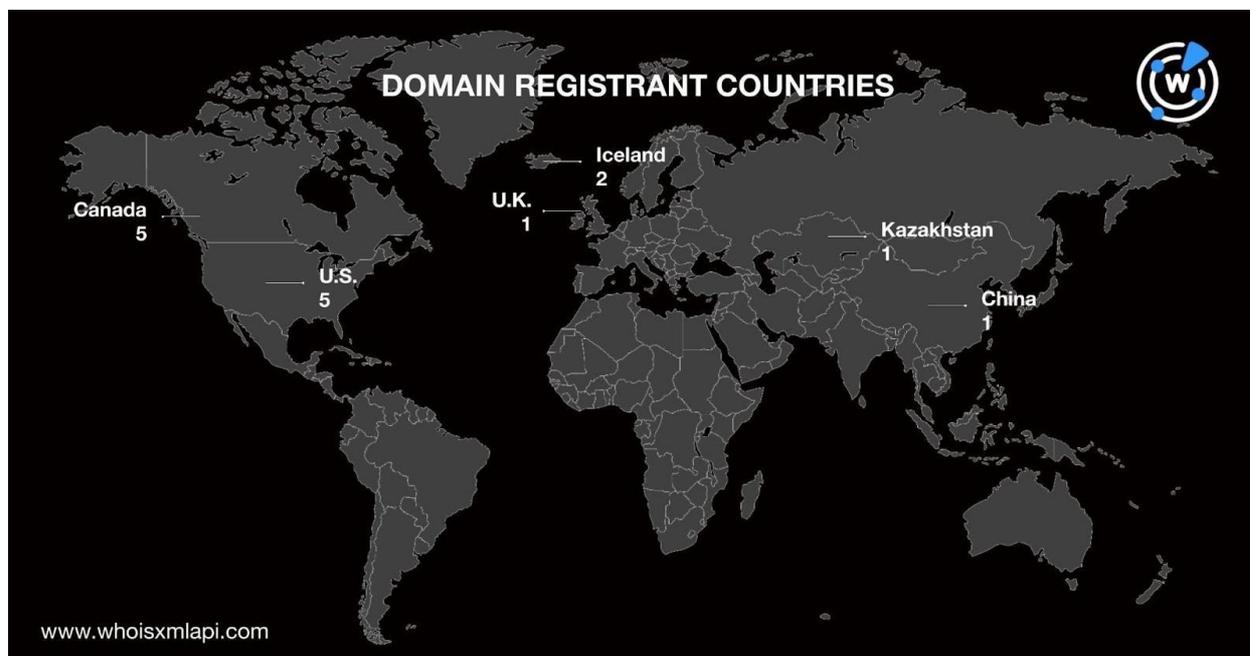
DNSから見えてきたIoCの実態

まず、脅威アクターのインフラについて可能な限り多くの情報を集めるため、IoCを[bulk WHOIS lookup](#)で検索してみました。そして、以下が判明しました。

- URLから抽出した18個のドメイン名のうち15個には公開のWHOIS情報が存在。ただし、ほとんどのデータはかなり編集または非公開化済み。登録者組織名のフィールドに情報が記載されていたレコードは1つのみ
- WHOISレコードを取得できた15個のドメイン名のレジストラは、それぞれ3個のIoCを管理していたGoDaddy.com LLC、Google、Namecheap, Inc.を筆頭に、8社に分散



- 15個のIoCは全て新たに登録されたドメイン名
- qhsbobfv[.]topというドメイン名の登録者情報は公開されていたものの、中国語で記載
- 15個のドメイン名が登録された国は、5個ずつが登録されていたカナダと米国を筆頭に、6カ国に分散



DNSで見つかった関連性

IoCとして特定されたURLから抽出した18個のドメイン名についてBulk WHOIS Lookupを実行した結果、1件の登録者名が未編集の状態で見つかりました。[Reverse WHOIS Search](#)で調べたところ、その登録者名は10,000を超える別のドメイン名の過去のWHOISレコードにも表示されました。その10,000超を一括マルウェアチェックにかけた結果、10個のドメイン名はすでに悪意あるものとして検出されていたことがわかりました。現在までアクセス可能な状態を維持しているのはそのうち1個だけで、アクセスすると空白のページが表示されます。

公表のレポートに含まれていない潜在的な関連性を探るため、URLから抽出した18個のドメイン名を[DNS Lookup](#)にかけてみました。その結果、7個のドメイン名が10個のユニークなIPアドレスに名前解決しました。さらにそれらのIPアドレスについて[Reverse IP Lookup](#)で調べたところ、2個は専用アドレスのように見えました。その2個のアドレスは合計で、IoCリストに含まれていない114個のドメイン名をホストしていました。そして、そのうち26個は、一括マルウェアチェックにより悪意あるドメイン名として特定済みでした。

その26個の悪意あるドメイン名を[Screenshot Lookup](#)で分析した結果、24個は本稿執筆時点でアクティブなコンテンツをホストし続けていたことがわかりました。以下はその例です。



Bergabunglah Bersama Kami!

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout.

Jelajahi →



agenkebab[.]comのスクリーンショット

We use cookies to personalise content and ads, analyse our traffic and share information about site usage with our social media, advertising and analytics partners. We need your consent to use cookies for this website. You can choose not to allow some types of cookies. Select "Manage" to find out more and change our default settings. You can adjust your preferences at any time. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer.

Manage Accept all

Free delivery to ROI | Save €4 on parcel labels | 34% off Advantage Card Labels

Save on your sending with the Advantage Card

Save €45* on stamps

Pickled Pom Pom use the Advantage Card to save up to €45 on every pack of stamps they buy for their business. The Advantage Card gives great discounts on stamps and parcels to all businesses.

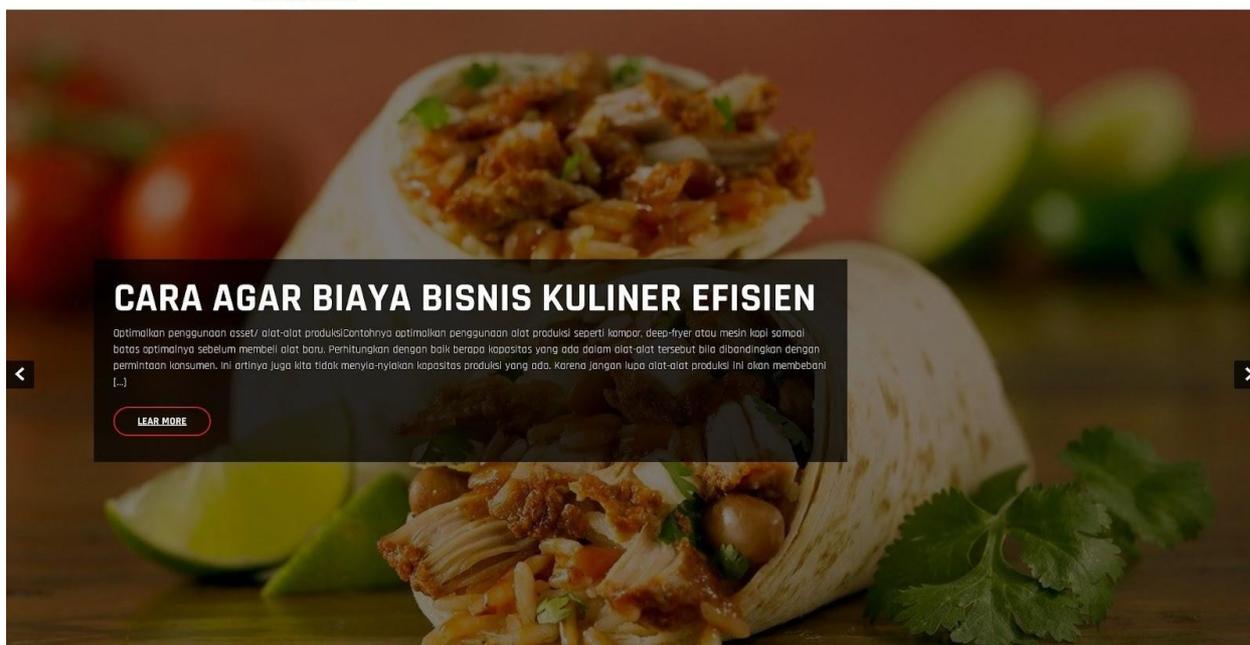
Buy Now

* T&Cs apply

National Stamps

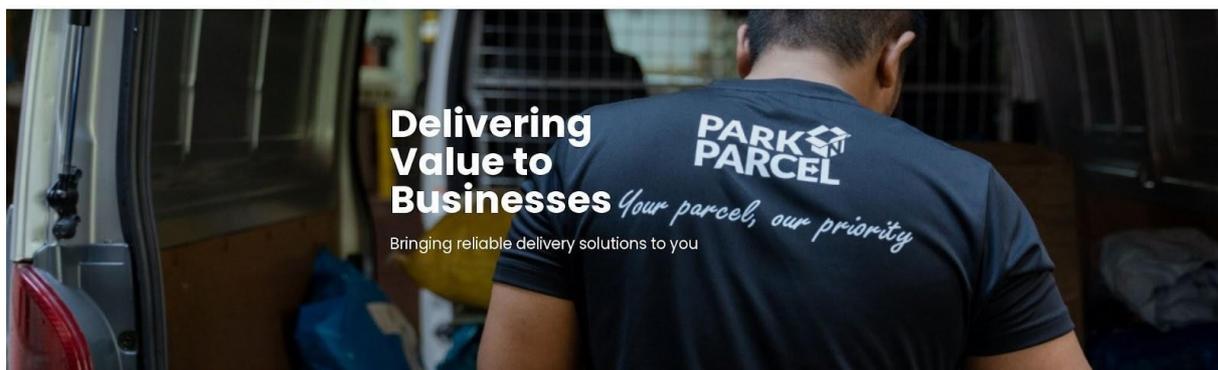
Want to send a letter in the Republic of Ireland? Buy one of our National Stamp products to help get it there.

customsfee-supporthub[.]comのスクリーンショット



franchisekebab[.]comのスクリーンショット

IoTとされたURLのドメイン名でホストしている3つのページのスクリーンショットを見たところ、QRコードフィッシングの脅威アクターは、コンテンツが正規のページと紛らわしいウェブプロパティを使用していたようです。以下にその3つの例を示します。



Delivered
2M+
parcels

Serving over
3000+
businesses

Record of less than
0.001%
lost/damaged items

Our Main Services

Supporting small to large-scale businesses

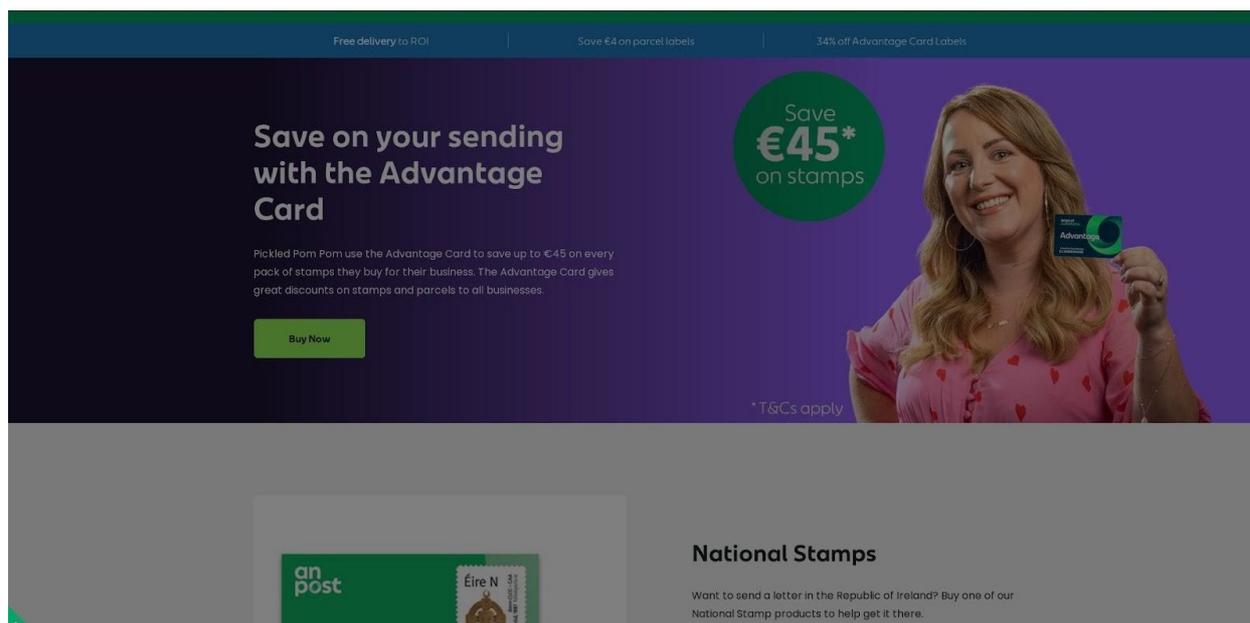


aircourier-company[.]comというloCでホストされていたページのスクリーンショット



viajalejos[.]netというloCでホストされていたページのスクリーンショット

We use cookies to personalise content and ads, analyse our traffic and share information about site usage with our social media, advertising and analytics partners. We need your consent to use cookies for this website. You can choose not to allow some types of cookies. Select "Manage" to find out more and change our default settings. You can adjust your preferences at any time. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer.



lockvwoodgroup[.]comというloCでホストされていたページのスクリーンショット



しかし、より興味深かったのは、IoCであるlockvoodgroup[.]comのウェブページと今回発見された共通のIPアドレスを使っている悪意あるドメイン名customsftee-supporthub[.]comのウェブページのスクリーンショットが同じだったことです。

他のページは、食品配達、宅配便、旅行サービスを提供するサイトなど、一般に潜在的被害者が探しそうな商品やサービスに焦点を当てているようです。そのため、そうしたサイトの真偽を確かめずに被害に遭う可能性が高くなっています。

[Domains & Subdomains Discovery](#)の検索結果によれば、今回抽出したドメイン名のうち6個に見られた以下の文字列は、他の10,045個のドメイン名にも見られました。

- 16092022.
- viajalejos.
- qrserver.
- lockvoodgroup.
- isirumah.
- qr.

その10,045個のドメイン名をマルウェア一括チェックにかけたところ、4個が悪意あるドメイン名に分類されました。本稿執筆時点で、そのうち1個はアクティブなコンテンツをホストし続けています。

Hair Loss Treatment

Hair Loss Home This is spider bait: Follicle scalp disorders and stop hair problems hair products prevention. The various treatments for hair replacement include minoxidil propecia finasteride proscar NANO superoxide dismutase and antiandrogens. Other aspects of drug treatment comprise alopecia hair follicle scalp stop scalp disorders hair care chemotherapy problems minoxidil propecia.

finasteride proscar copper drugs drugstore prescription nonprescription [Hair loss treatment](#) skin care medicines viagra propecia regrowth hair loss antibiotics men women health chemist regrowth balding hair loss treatment proctor shop pharmacy online pharmaceuticals hair loss treatment skin care medicines viagra propecia regrowth hair loss antibiotics men women health chemist regrowth balding hair loss treatment contraceptives. antiandrogens drugs.tf antibiotics men women finasteride health chemist proctor Stop hair-loss treatment hairloss treatment alopecia.

follicle scalp and disorders of hair propecia ntibiotics men women finasteride health shampoo vitamins health food antioxidants internet sales sundries The various treatments include minoxidil propecia finasteride proscar NANO superoxide dismutase and antiandrogens. Other aspects of drug treatment comprise alopecia hair follicle scalp disorders hair replacemnt problems minoxidil propecia [Hair loss treatment](#) finasteride proscar copper dismutase SOD superoxid men women product prevention dismutase proctor hairloss balding hair. hair-loss treatment hairloss treatment alopecia.

, follicle scalp and hair loss. facial skin care hair loss treatment alopecia hair-loss. Free radicals organic semiconductors alzheimers superoxide ros reperfusion injury peroxide catalase sod superoxide dismutase parkinsonism parkinson's disease organic semiconductor polyacetylene amorphous inflammation antioxidant spin trap label tempo tempol dementia deafness psychosis homocystinuria homocysteine thiolactone cancer treatment redox signaling messenger active hair loss treatment oxygen deafness inner ear cis platinum adriamycin pbn nxy-059 astrazenica electron transfer hydroxyl radical catalase.

peroxidase anticancer high conductivity alcaptonuria phenothiazine [Hair loss treatment](#) dopa uric acid redox signaling lesch-nyhan manganese hemochromatosis iron copper porphyria. hair loss regrowth Ne silvae quidem horridiorque naturae facies medicinis carent, sacra illa parente rerum omnium hair loss treatment nusquam non remedia disponente homini, ut medicina fieret etiam solitudo ipsa, et ad singula illius discordia atque concordiae [Hair loss treatment](#) miraculis occurrentibus. quercus et olea tam pertinaci odio dissident, regrowth hair loss antibiotics men women health chemist.

regrowth balding hair loss treatment proctor shop pharmacy [Hair loss treatment](#) online pharmaceuticals hair loss treatment alterius scrobe [hair loss treatment](#) depacta emoriantur, quercus vero et iuxta nucem iuglandem, that is regrowth of lost hair is sometimes bvery easy and sometime rather difficult to accomplish. Perniciiala et brassicae cum vite odia; Haor loss ipsum hair loss blog [hair loss](#) olus, quo vitis fugatur, adversum cyclamino et origano arescit. Puln et annosas iam et quae sternantur arbores difficilii caedi, celerius [Hair regrowth](#) marcescere tradunt, si prius manu quam ferro attingantur. Hair loss pomorum onera a iumentis statim sentiri, ac, skin carehair loss blog medicines viagra propecia regrowth hair loss antibiotics men women health chemist.

qr[.]stのスクリーンショット

—



QRコードフィッシングのIoCとして特定された18個のURLからドメイン名を抽出して詳細に分析した結果、関連していると思われるアーティファクトが20,000超見つかりました。また、QRコードフィッシングのキャンペーンで使用された可能性のあるIPアドレスに加え、QRコードフィッシングの脅威アクターまたは他の脅威アクターのサイバー犯罪インフラの一部かもしれない悪意あるドメイン名も明らかになりました。

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

IoC

- xaoqohhckbb3pnxyqzj6pkuzckt2ur
beiyd5xlanmw52expmohl7dyd[.]onion
- um2kc2ahigbq7t2rchk3tnxnjzvrddb
xkcy573dqxc44wvi4ge5cad[.]onion
- safedelivery-company[.]com
- fq5rdcppmv7cqjhretm3owbnj4hskcv
37bcgx5rpbdbhqfefzix4tiyd[.]onion
- exmb25nic6n25sclnf44rrgynquns7u
3zjqa33x3uztwbmsuptf7gyid[.]onion
- dexmb25nic6n25sclnf44rrgynquns7
u3zjqa33x3uztwbmsuptf7gyid[.]onion
- carpoolk[.]com
- aircourier-company[.]com
- 3emyw4wto7tgupbisbdbkbyaamb7
p7dpxp6lnfqwyemskmmar3fugad[.]
onion
- 16092022[.]com
- bafybeiatig7bsbj3awxopocfjayzyv5jx
hrhgyjqkxrdz5sxikrpftt4am[.]jipfs
- viajalejos[.]net
- qrserver[.]com
- lockvoodgroup[.]com
- kamsaridevelopment[.]com
- isirumah[.]info
- bc1qx0anrq4v2aftl3eg22rfnyump7w
xln2e7ld60a[.]com
- qr[.]codes

登録者組織名が同一のドメイン名の例

- 00030[.]cn
- 000799[.]cn
- 005006[.]cn
- 005353[.]cn
- 005505[.]cn
- 005877[.]cn



- 006028[.]cn
- 006170[.]cn
- 006228[.]cn
- 006308[.]cn
- 006699[.]com[.]cn
- 006job[.]cn
- 007845[.]cn
- 007877[.]cn
- 007927[.]cn
- 008094[.]cn
- 008794[.]cn
- 00a3w[.]cn
- 00q02[.]cn
- 00tp[.]cn
- 010zhaosheng[.]cn
- 012led[.]cn
- 020dzbw[.]cn
- 020dzw[.]cn
- 0212311[.]com[.]cn
- 02139[.]cn
- 021lvyou[.]com[.]cn
- 021pump[.]com[.]cn
- 021rili[.]cn
- 022sms[.]com[.]cn
- 023esw[.]cn
- 02807[.]cn
- 030e[.]cn
- 030i[.]cn
- 0329xq[.]cn
- 0350safe[.]cn
- 0351zaozhiliao[.]cn
- 0355i[.]cn
- 0384nn[.]cn
- 03a1m1[.]cn
- 03q3hoqu[.]cn
- 0420c2b5[.]cn
- 0459car[.]cn
- 047q01[.]cn
- 0511kq[.]cn
- 0513xx[.]cn
- 053156[.]org[.]cn
- 0553web[.]cn
- 0580orange[.]cn
- 0599my[.]cn
- 0634562[.]cn
- 066288[.]cn
- 0662yes[.]cn
- 07013[.]cn
- 0711car[.]cn
- 0713tf[.]cn
- 0719it[.]cn
- 0755aa[.]cn
- 0756pco[.]cn
- 0775auto[.]cn
- 0781554[.]cn
- 0794xu[.]cn
- 0831job[.]cn
- 0838dh[.]com[.]cn
- 084g[.]cn
- 087196100[.]cn
- 0919275[.]cn
- 0951player[.]cn
- 0998dh[.]cn
- 09rf[.]cn
- 0a70rj[.]cn
- 0ac6n[.]cn
- 0bmxtdc[.]cn
- 0bu403[.]cn
- 0c1q0l[.]cn
- 0cat[.]cn
- 0d5ir[.]cn
- 0f6m1l3e[.]cn
- 0favv[.]cn
- 0fqlu9[.]cn
- 0g75ll[.]cn
- 0h7u[.]cn
- 0hd35k[.]cn
- 0jxi9x[.]cn
- 0k3[.]cn
- 0lwx1h[.]cn



- 0mjmx[.]cn
- Orisks[.]cn
- 0s000[.]cn
- 0sy9w5p[.]cn
- 0yn7um[.]cn
- 0zth[.]cn
- 1-3n[.]cn
- 1-work[.]cn
- 10000[.]ha[.]cn
- 10000cl[.]cn
- 10000sn[.]cn
- 1000faka[.]cn
- 1000j[.]cn
- 1000kg[.]cn
- 1000ysd[.]cn
- 10010[.]fj[.]cn
- 10010game[.]cn
- 1004952[.]cn
- 10086[.]xj[.]cn
- 10086i[.]cn
- 100gu[.]com[.]cn
- 100huatong[.]cn
- 100myd[.]cn
- 100zjdy[.]cn
- 10100888[.]cn
- 10101020[.]cn
- 10103365[.]cn
- 10103636[.]cn
- 10105335[.]cn
- 10105959[.]cn
- 10106066[.]cn
- 10107373[.]cn
- 10108868[.]cn
- 10108898[.]cn
- 1024book[.]cn
- 108han[.]cn
- 10jmw[.]cn
- 10wanwen[.]cn
- 111658[.]com[.]cn
- 111toys[.]cn
- 1124m[.]cn
- 114eee[.]cn
- 114guangdong[.]cn
- 116114zp[.]cn
- 1183168[.]cn
- 118wang[.]cn
- 11coin[.]cn
- 120122[.]cn
- 12300[.]com[.]cn
- 123321dsw[.]cn
- 1234566[.]cn
- 123877[.]cn
- 123dc[.]cn
- 123dlm[.]cn
- 123mu[.]cn
- 123pass[.]cn
- 127qipapingguoban[.]cn
- 127qipaiwang[.]cn
- 1310000[.]cn
- 1314179[.]com[.]cn
- 133la[.]cn
- 13542508888[.]cn
- 135jm[.]cn
- 1366i27[.]cn
- 136784034[.]cn
- 138787[.]cn
- 139mfyx[.]cn
- 13cai[.]com[.]cn
- 13tz[.]cn
- 1412058[.]cn
- 14395[.]cn
- 14396[.]cn
- 14659[.]cn
- 14672[.]cn
- 150km[.]cn
- 1551hn[.]cn
- 155la[.]cn
- 158jj[.]cn
- 15999566722[.]cn
- 15bk[.]cn



- 1616d[.]com[.]cn
- 16183[.]cn
- 161n4[.]cn
- 161n5[.]cn
- 1688coin[.]cn
- 16com9[.]cn
- 16ren[.]cn
- 17748[.]cn
- 17credit[.]cn
- 17gansf[.]cn
- 17hegc[.]cn
- 17jmba[.]cn
- 17ko8[.]cn
- 17lwan[.]cn
- 17shoulu[.]cn
- 17y8[.]cn
- 1818hao[.]cn
- 18258[.]com[.]cn
- 18341[.]cn
- 18414[.]cn
- 18429iiu[.]cn
- 18463[.]cn
- 18784[.]cn
- 18800[.]cn
- 19900420[.]cn
- 1996game[.]cn
- 1996game[.]com[.]cn
- 1anxin[.]cn
- 1bsg[.]cn
- 1fdd3[.]cn
- 1flag[.]cn
- 1fu[.]cn
- 1fwt7d[.]cn
- 1hs[.]com[.]cn
- 1huoyun[.]cn
- 1k681[.]cn
- 1mfh9a[.]cn
- 1r458t[.]cn
- 1rbzyd[.]cn
- 1ru0w9[.]cn
- 1stinsurance[.]com[.]cn
- 1watch[.]cn
- 1wgu6y[.]cn
- 1xinli[.]cn
- 1xinshi[.]cn
- 1xqv2k[.]cn
- 1zshop[.]cn
- 200139[.]cn
- 200820[.]cn
- 2017rwnuh23[.]cn
- 2021lijunqi[.]cn
- 20348[.]cn
- 2042541[.]cn
- 20605555[.]cn
- 2060768[.]cn
- 20957[.]cn
- 20hl[.]cn
- 20w5p5[.]cn
- 20yi[.]cn
- 20yonyou[.]cn
- 21894[.]cn
- 21feizhuliu[.]cn
- 21jade[.]cn
- 223222[.]cn
- 2233play[.]cn
- 2253461[.]cn
- 23095[.]cn
- 2338204[.]cn
- 235wz[.]cn
- 236788[.]cn
- 237[.]net[.]cn
- 239239[.]cn
- 23yp[.]cn
- 241232[.]cn
- 248555[.]com[.]cn
- 25330[.]cn
- 258688[.]cn
- 25f3k0g[.]cn
- 26594[.]cn
- 26gedu[.]cn



- 27ag[.]cn
- 27hai[.]cn
- 282988[.]cn
- 285dq1[.]cn
- 287lays2[.]cn
- 28hse[.]cn
- 28pin[.]cn
- 2969224[.]cn
- 29925[.]com[.]cn
- 2adr[.]cn
- 2aynzp[.]cn
- 2bhome[.]cn
- 2bkt[.]cn
- 2bw8h0[.]cn
- 2fs68x[.]cn
- 2moc[.]cn
- 2u8a[.]cn
- 2w52[.]cn
- 2wuf6a[.]cn
- 2zk[.]com[.]cn
- 30295[.]cn
- 30819[.]cn
- 309t[.]cn
- 30idvw[.]cn
- 3116811[.]cn
- 31alu[.]cn
- 3338228[.]cn
- 336788[.]cn
- 337yin[.]cn
- 34ppp[.]cn
- 34s[.]cn
- 35125[.]cn
- 35126[.]com[.]cn
- 35500[.]cn
- 360anxindai[.]cn
- 360jyx[.]cn
- 365ad[.]cn
- 365dy[.]cn
- 365zhekou[.]cn
- 366eka[.]cn
- 36hhr[.]cn
- 36tianguan[.]cn
- 37132[.]cn
- 3746631[.]cn
- 37642[.]cn
- 37647[.]cn
- 3765ce[.]cn
- 3771517[.]cn
- 37m53x[.]cn
- 37twus[.]cn
- 38420[.]cn
- 38423[.]cn
- 38465[.]cn
- 38496[.]cn
- 38497[.]cn
- 38574[.]cn
- 38847[.]cn
- 3888886[.]cn
- 38904[.]cn
- 38baby[.]cn
- 39139[.]com[.]cn
- 392w[.]cn
- 39358[.]com[.]cn
- 39ysw[.]cn
- 3a9r9[.]net[.]cn
- 3c4f1s[.]cn
- 3caibok[.]cn
- 3dus[.]cn
- 3eb45b[.]cn
- 3gest[.]cn
- 3gpconverters[.]cn
- 3hcn[.]cn
- 3iv5[.]cn
- 3kuc[.]cn
- 3omk[.]cn
- 3phveb[.]cn
- 3ref[.]cn
- 3wood[.]com[.]cn
- 3wzjg[.]cn
- 3y8wld[.]cn



- 4000000005[.]cn
- 4000001234[.]cn
- 4000016767[.]cn
- 4000040000[.]cn
- 4000066666[.]cn
- 4000081234[.]cn
- 4000083939[.]cn
- 4000085678[.]cn
- 4000089900[.]cn
- 4000100100[.]cn
- 4000100617[.]cn
- 4000105678[.]cn
- 4000156651[.]cn
- 4000161616[.]cn
- 4000166166[.]cn
- 4000198198[.]cn
- 4000205858[.]cn
- 4000315315[.]cn
- 4000511988[.]cn
- 4000555520[.]cn
- 4000581908[.]cn
- 4000589988[.]cn
- 4000799977[.]cn
- 4000800233[.]cn
- 4000806060[.]cn
- 4000806666[.]cn
- 4000833111[.]cn
- 4000835999[.]cn
- 4000871666[.]cn
- 4000871800[.]cn
- 4000881952[.]cn
- 4000888566[.]cn
- 4000917917[.]cn
- 4000975976[.]cn
- 4000979797[.]cn
- 4000990999[.]cn
- 4001000538[.]cn
- 4001001111[.]cn
- 4001005111[.]cn
- 4001057878[.]cn
- 4001098866[.]cn
- 4001111111[.]cn
- 4001117999[.]cn
- 4001177517[.]cn
- 4001180117[.]cn
- 4001191941[.]cn
- 4001355188[.]cn
- 4001579999[.]cn
- 4001599090[.]cn
- 4001616365[.]cn
- 4001669999[.]cn
- 4001688688[.]cn
- 4001717917[.]cn
- 4001827777[.]cn
- 4001840018[.]cn
- 4001868666[.]cn
- 4001888888[.]cn
- 4001919999[.]cn
- 4001991999[.]cn
- 4006001189[.]cn
- 4006005577[.]cn
- 4006006666[.]cn
- 4006019999[.]cn
- 4006029566[.]cn
- 4006040010[.]cn
- 4006081111[.]cn
- 4006087777[.]cn
- 4006123111[.]cn
- 4006126688[.]cn
- 4006129999[.]cn
- 4006135135[.]cn
- 4006166655[.]cn
- 4006166666[.]cn
- 4006179999[.]cn
- 4006206998[.]cn
- 4006228228[.]cn
- 4006228811[.]cn
- 4006258899[.]cn
- 4006280066[.]cn
- 4006321666[.]cn



- 4006345678[.]cn
- 4006362266[.]cn
- 4006388666[.]cn
- 4006503333[.]cn
- 4006596666[.]cn
- 4006603333[.]cn
- 4006620878[.]cn
- 4006622666[.]cn
- 4006661111[.]cn
- 4006661166[.]cn
- 4006661999[.]cn
- 4006663666[.]cn
- 4006664000[.]cn
- 4006666917[.]cn
- 4006667777[.]cn
- 4006671988[.]cn
- 4006677500[.]cn
- 4006689999[.]cn
- 4006700700[.]cn
- 4006771988[.]cn
- 4006779696[.]cn
- 4006789688[.]cn
- 4006789977[.]cn
- 4006880999[.]cn
- 4006889999[.]cn
- 4006917917[.]cn
- 4006919999[.]cn
- 4006969666[.]cn
- 4006990000[.]cn
- 4006996666[.]cn
- 4006997999[.]cn
- 4006998998[.]cn
- 4006999666[.]cn
- 4007001000[.]cn
- 4007001864[.]cn
- 4007003888[.]cn
- 4007708866[.]cn
- 4007886666[.]cn
- 4007888777[.]cn
- 4007999999[.]cn
- 4008002211[.]cn
- 4008002345[.]cn
- 4008004900[.]cn
- 4008006666[.]cn
- 4008008666[.]cn
- 4008036699[.]cn
- 4008066969[.]cn
- 4008073636[.]cn
- 4008090808[.]cn
- 4008096666[.]cn
- 4008096868[.]cn
- 4008105858[.]cn
- 4008112112[.]cn
- 4008116666[.]cn
- 4008121121[.]cn
- 4008171666[.]cn
- 4008171717[.]cn
- 4008176111[.]cn
- 4008182233[.]cn
- 4008186337[.]cn
- 4008188333[.]cn
- 4008189999[.]cn
- 4008193388[.]cn
- 4008197197[.]cn
- 4008200187[.]cn
- 4008201902[.]cn
- 4008209999[.]cn
- 4008213213[.]cn
- 4008215757[.]cn
- 4008218866[.]cn
- 4008260555[.]cn
- 4008261166[.]cn
- 4008267900[.]cn
- 4008268008[.]cn
- 4008289669[.]cn
- 4008308003[.]cn
- 4008308999[.]cn
- 4008508805[.]cn
- 4008515515[.]cn
- 4008536100[.]cn



- 4008585237[.]cn
- 4008588888[.]cn
- 4008600981[.]cn
- 4008603366[.]cn
- 4008603838[.]cn
- 4008612345[.]cn
- 4008705151[.]cn
- 4008705400[.]cn
- 4008756789[.]cn
- 4008773333[.]cn
- 4008777777[.]cn
- 4008809985[.]cn
- 4008815500[.]cn
- 4008819090[.]cn

登録者組織名が同一の悪意あるドメイン名の例

- 0775auto[.]cn
- 114eee[.]cn
- 133la[.]cn
- 30idvw[.]cn
- 3re[.]cn
- aion55[.]cn

IPアドレスの例

- 172[.]67[.]169[.]165
- 104[.]21[.]54[.]242
- 104[.]21[.]90[.]104
- 127[.]0[.]0[.]1
- 179[.]43[.]189[.]137
- 103[.]20[.]190[.]131

同一のIPアドレスに名前解決したドメイン名の例

- agenkebab[.]com
- agensahara[.]com
- astral[.]co[.]id
- audiojaya[.]com
- bagel[.]id
- bahanbakukebab[.]com
- baiya[.]id
- balimegaspa[.]com
- baramultilumintu[.]com
- berlianagrolestari[.]com
- bogareslor[.]id
- burnerkebab[.]com
- burnerkebabmurah[.]com
- customsfee-supporthub[.]com
- dagingkebab[.]com
- dcs[.]web[.]id
- delifood[.]id
- demarin[.]id
- desabaharidua[.]web[.]id
- dongguluselatan[.]id
- filterairbandung[.]net
- filteraircimahi[.]com
- fkksm-mm2100[.]or[.]id
- franchisekebab[.]com
- ftp[.]pt-saj[.]id
- gariskata[.]com
- grobogkulon[.]id
- himmahstore[.]co[.]id
- hunianmurahsidoarjo[.]com
- idemug[.]com
- iklan98[.]com
- indofrozen[.]com
- indofrozenfood[.]com
- indomaxhost[.]com
- infodesagredek[.]com
- inkordanclothing[.]com
- jalurharomain[.]com
- jasabangunanmagetan[.]com



- jayatechbiofilter[.]com
- jualairminumamidisbandung[.]com
- jualansaya[.]com
- jualkebab[.]com
- kalaerolantari[.]web[.]id
- kaltimmultisekurindo[.]com
- karunialumasindo[.]com
- kebabfrozen[.]com
- kedaijamu[.]com
- kulittortilla[.]com
- kuripan[.]desa[.]id
- laemanta-utara[.]id

共通のIPアドレスに名前解決した悪意あるドメイン名の例

- agenkebab[.]com
- balimegaspa[.]com
- customsfee-supporthub[.]com
- franchisekebab[.]com
- himmahstore[.]co[.]id
- iklan98[.]com
- jasabangunanmagetan[.]com
- jayatechbiofilter[.]com
- kedaijamu[.]com
- mail[.]himmahstore[.]co[.]id
- mail[.]jasabangunanmagetan[.]com
- mail[.]kedaijamu[.]com
- multikencanaoffset[.]com
- pinotu[.]id

共通の文字列を含むドメイン名の例

- isirumah[.]id
- isirumah[.]net
- isirumah[.]com
- isirumah[.]site
- sisirumah[.]com
- isirumah[.]co[.]id
- isirumah[.]store
- ngisirumah[.]com
- isirumah[.]homes
- myisirumah[.]org
- isirumah[.]co[.]de
- sewaisirumah[.]id
- isirumah[.]web[.]id
- isirumah[.]online
- teknisirumah[.]id
- tokoisirumah[.]com
- beliisirumah[.]com
- sewaisirumah[.]com
- mengisirumah[.]com
- teknisirumah[.]com
- caraisirumah[.]com
- hargaisirumah[.]com
- blog-isirumah[.]net
- kedaiisirumah[.]tokyo
- ngisirumah[.]furniture
- demo2-blog-isirumah[.]vg
- jasadesainsupervisirumah[.]com
- tanamanrempahsumberpendapatani
sirumah[.]com
- lockvwoodgroup[.]co[.]uk
- qr[.]vg
- qr[.]me
- qr[.]ro
- qr[.]af
- qr[.]pl
- qr[.]la
- qr[.]id
- qr[.]st
- qr[.]gd
- qr[.]uk
- qr[.]cz
- qr[.]pa
- qr[.]vc
- qr[.]no



- qr[.]hk
- qr[.]gt
- qr[.]mn
- qr[.]cc
- qr[.]ly
- qr[.]fi
- qr[.]lu
- qr[.]sh
- qr[.]su
- qr[.]ls
- qr[.]cr
- qr[.]rs
- qr[.]ca
- qr[.]kg
- qr[.]gl
- qr[.]hr
- qr[.]gs
- qr[.]cn
- qr[.]us
- qr[.]pw
- qr[.]ke
- qr[.]ax
- qr[.]tv
- qr[.]ag
- qr[.]cm
- qr[.]co
- qr[.]cx
- qr[.]ai
- qr[.]mr
- qr[.]sg
- qr[.]my
- qr[.]ci
- qr[.]om
- qr[.]nu
- qr[.]is
- qr[.]sc
- qr[.]xn--fiqs8s
- qr[.]nl
- qr[.]ru
- qr[.]pt
- qr[.]lh
- qr[.]jo
- qr[.]eu
- qr[.]nz
- qr[.]uz
- qr[.]io
- qr[.]fr
- qr[.]ma
- qr[.]gg
- qr[.]tc
- qr[.]uy
- qr[.]mk
- qr[.]by
- qr[.]gr
- qr[.]se
- qr[.]lc
- qr[.]dk
- qr[.]si
- qr[.]ae
- qr[.]tj
- qr[.]tl
- qr[.]cl
- qr[.]do
- qr[.]al
- qr[.]mw
- qr[.]mg
- qr[.]lv
- qr[.]lt
- qr[.]xn--mxtq1m
- qr[.]im
- qr[.]gy
- qr[.]qa
- qr[.]am
- qr[.]kz
- qr[.]tn
- qr[.]gp
- qr[.]ee
- qr[.]fo
- qr[.]sb
- qr[.]to



- qr[.]sk
- qr[.]be
- qr[.]hu
- qr[.]xn--node
- qr[.]de
- mqr[.]nu
- 5qr[.]ir
- oqr[.]in
- qqr[.]se
- yqr[.]se
- wqr[.]se
- dqr[.]hk
- 2qr[.]tw
- yqr[.]tv
- jqr[.]tv
- mqr[.]tv
- wqr[.]pw
- hqr[.]hk
- vqr[.]be
- qqr[.]be
- eqr[.]ie
- wqr[.]it
- pqr[.]in
- uqr[.]be
- 1qr[.]pw
- sqr[.]tl
- xqr[.]ca
- 3qr[.]ch
- jqr[.]pw
- 2qr[.]no
- pqr[.]it
- 5qr[.]in
- 4qr[.]co
- qqr[.]co
- qqr[.]eu
- zqr[.]kr
- xqr[.]pw
- bqr[.]eu
- hqr[.]uz
- iqr[.]uz
- 1qr[.]uz
- mqr[.]ai
- fqr[.]cn
- nqr[.]si
- qr[.]dev
- hqr[.]jp
- 9qr[.]io
- tqr[.]me
- 9qr[.]us
- 6qr[.]cn
- 1qr[.]cn
- 4qr[.]ru
- tqr[.]ru
- tqr[.]us
- uqr[.]me
- 7qr[.]fr
- bqr[.]cn
- bqr[.]fr
- kqr[.]nl
- mqr[.]fr
- uqr[.]nl
- uqr[.]fr
- 5qr[.]io
- oqr[.]ru
- oqr[.]nl
- 0qr[.]cn
- wqr[.]us
- qqr[.]vg
- vqr[.]es
- rqr[.]id
- 3qr[.]uk
- eqr[.]cl
- oqr[.]hk
- vqr[.]pw
- 7qr[.]id
- zqr[.]hk
- nqr[.]vc
- 1qr[.]my
- vqr[.]tv
- eqr[.]pt



- 9qr[.]me
- yqr[.]xn--kprw13d
- wqr[.]ch
- rqr[.]lt
- hqr[.]es
- fqr[.]au
- eqr[.]by
- uqr[.]it
- kqr[.]in
- eqr[.]jp
- qqr[.]kr
- fqr[.]me
- eqr[.]hu
- nqr[.]tv
- xn--qr-ua[.]de
- nqr[.]in
- yqr[.]sk
- 0qr[.]in
- hqr[.]cc
- cqr[.]io
- rqr[.]uk
- pqr[.]ir
- uqr[.]in
- zqr[.]me
- dqr[.]jp
- rqr[.]jp
- rqr[.]cc
- aqr[.]jp
- fqr[.]at
- eqr[.]vn
- 2qr[.]co
- gqr[.]ro
- mqr[.]kz
- iqr[.]es
- fqr[.]io
- jqr[.]tm
- vqr[.]us
- 9qr[.]nl
- 3qr[.]ru
- 7qr[.]us
- qr[.]org
- zqr[.]nl
- qr[.]rip
- tqr[.]ug
- bqr[.]re
- fqr[.]tv
- zqr[.]es
- 1qr[.]nu
- dqr[.]nu
- aqr[.]nu
- wqr[.]kr
- lqr[.]id
- sqr[.]la
- aqr[.]is
- aqr[.]kz
- yqr[.]ch
- jqr[.]xn--55qx5d
- iqr[.]ch
- fqr[.]co
- dqr[.]tw
- rqr[.]kr
- 4qr[.]eu
- 2qr[.]ir
- yqr[.]co
- dqr[.]be
- 2qr[.]vn
- eqr[.]fm
- bqr[.]pl
- sqr[.]uk
- xqr[.]eu
- gqr[.]co
- lqr[.]ca
- oqr[.]li
- aqr[.]eu
- gqr[.]tv
- pqr[.]be
- lqr[.]cc
- fqr[.]it
- fqr[.]uk
- 4qr[.]es



- mqr[.]tw
- pqr[.]at
- jqr[.]de
- tqr[.]la
- tqr[.]de
- iqr[.]se
- bqr[.]it
- hqr[.]ca
- lqr[.]dk
- zqr[.]ca
- jqr[.]io
- aqr[.]in
- qr[.]cab
- 2qr[.]uk
- nqr[.]ru
- 6qr[.]us
- zqr[.]uz
- tqr[.]uz
- 4qr[.]me
- uqr[.]ru
- wqr[.]cl
- qr[.]biz
- aqr[.]cn
- pqr[.]fr
- eqr[.]de
- gqr[.]de
- xqr[.]ru
- wqr[.]nl
- hqr[.]tw
- nqr[.]ir
- dqr[.]cz
- dqr[.]gs
- kqr[.]es
- rqr[.]gg
- vqr[.]la
- hqr[.]ch
- cqr[.]cl
- hqr[.]fi
- 5qr[.]jp
- tqr[.]mx
- kqr[.]ca
- nqr[.]eu
- cqr[.]lv
- wqr[.]co
- dqr[.]de
- tqr[.]es
- pqr[.]uz
- 8qr[.]co
- aqr[.]es
- pqr[.]st
- cqr[.]cz
- aqr[.]cz
- aqr[.]uz
- 1qr[.]au
- 2qr[.]ch
- lqr[.]pl
- fqr[.]nl
- 0qr[.]io
- iqr[.]uk
- xqr[.]cc
- gqr[.]eu
- 4qr[.]ch
- qr[.]tel
- sqr[.]kz
- 4qr[.]it
- jqr[.]me
- oqr[.]kr
- kqr[.]de
- mqr[.]ro
- pqr[.]au
- 0qr[.]eu
- cqr[.]at
- xqr[.]uk
- rqr[.]ca
- sqr[.]sg
- iqr[.]fr
- cqr[.]ru
- rqr[.]us
- pqr[.]de
- 9qr[.]co



- eqr[.]se
- sqr[.]ru
- zqr[.]us
- 8qr[.]us
- bqr[.]gg
- bqr[.]gs
- qr[.]sex
- rqr[.]ir
- eqr[.]nu
- bqr[.]vn
- cqr[.]la
- 6qr[.]co
- yqr[.]es
- iqr[.]cm
- 5qr[.]me
- vqr[.]se
- oqr[.]se
- bqr[.]pt
- eqr[.]im
- lqr[.]af
- sqr[.]eu
- 1qr[.]dk
- wqr[.]ca
- fqr[.]kr
- fqr[.]mx
- qr[.]fox
- yqr[.]ph
- hqr[.]ph
- lqr[.]ir
- mqr[.]xn--kprw13d
- qqr[.]us
- vqr[.]it
- dqr[.]uk
- eqr[.]ai
- 7qr[.]eu
- iqr[.]ro
- oqr[.]au
- sqr[.]nu
- hqr[.]nu
- tqr[.]eu
- uqr[.]cc
- zqr[.]jp
- cqr[.]in
- zqr[.]io
- mqr[.]it
- mqr[.]mx
- eqr[.]ch
- iqr[.]tj
- nqr[.]ro
- sqr[.]no
- wqr[.]eu
- sqr[.]uz
- nqr[.]uz
- qqr[.]uz
- fqr[.]de
- kqr[.]li
- 0qr[.]ru
- 1qr[.]vn
- qqr[.]it
- rqr[.]nl
- sqr[.]sd
- gqr[.]io
- 1qr[.]de
- 0qr[.]us
- vqr[.]fr
- dqr[.]ru
- jqr[.]hk
- 9qr[.]in
- 0qr[.]de
- qqr[.]nz
- 7qr[.]cn
- 3qr[.]de
- zqr[.]cn
- lqr[.]cl
- vqr[.]me
- 6qr[.]ph
- kqr[.]tv
- 5qr[.]tw
- vqr[.]nu
- gqr[.]se



- wqr[.]gg
- zqr[.]id
- mqr[.]ge
- hqr[.]id
- jqr[.]xn--3ds443g
- 6qr[.]kr
- hqr[.]tv
- nqr[.]cx
- iqr[.]dk
- yqr[.]su
- oqr[.]it
- 1qr[.]pl
- lqr[.]me
- jqr[.]cx
- dqr[.]vg
- cqr[.]cc
- mqr[.]jp
- bqr[.]ph
- pqr[.]ch
- tqr[.]no
- dqr[.]pm
- oqr[.]eu
- eqr[.]it
- mqr[.]pt
- aqr[.]pl
- qr[.]run
- 0qr[.]nl
- oqr[.]io
- tqr[.]dk
- 7qr[.]ca
- 5qr[.]ca
- dqr[.]ca
- tqr[.]pw
- aqr[.]pt
- wqr[.]ir
- gqr[.]uk
- vqr[.]eu
- iqr[.]ae
- sqr[.]mx
- iqr[.]kz
- bqr[.]kr
- wqr[.]cz
- iqr[.]be
- sqr[.]jp
- vqr[.]uz
- jqr[.]uz
- iqr[.]us
- oqr[.]us
- pqr[.]cn
- mqr[.]nl
- vqr[.]ru
- aqr[.]fr
- pqr[.]us
- eqr[.]ir
- wqr[.]es
- jqr[.]cm
- yqr[.]cm

共通の文字列を含む悪意あるドメイン名の例

- qr[.]st
- saqr[.]ru

qr.codesを含むドメイン名の例

- a-qr[.]codes
- air-qr[.]codes
- catchy-qr[.]codes
- crypto-qr[.]codes
- e-qr[.]codes
- etica-qr[.]codes
- fast-qr[.]codes
- free-qr[.]codes
- generate-qr[.]codes
- gham-qr[.]codes



- gosuslugi-qr[.]codes
- info-qr[.]codes
- link-qr[.]codes
- me-qr[.]codes
- medi-qr[.]codes