Redisは脅威アクターに狙われ続けるのか？

目次

要旨

「CVE-2022-0543」としても知られる「Redis Lua Sandbox Escape and Remote Code Execution」という脆弱性が発見された2022年2月以降、Redisのインスタンスは脅威アクターの標的になっています。Mushtik Gangは、この脆弱性を最初に悪用したサイバー攻撃グループの一つです。彼らは悪意あるスクリプトで脆弱なデバイスを感染させ、ファイルをダウンロードしたり、シェルコマンドを注入したり、リモートからフラッド攻撃やSSH（Secure Shell）ブルートフォース攻撃を仕掛けたりしました。

先月、Palo Alto NetworksのUnit 42が、同じバグを狙った別の攻撃を発見しました。これは、「P2PInfect」という自己複製型のP2Pワームを使用したものでした。同社の分析では、5個のIPアドレスと2個のドメイン名からなるP2PInfectのセキュリティ侵害インジケーター（IoC）が特定されました。

WhoisXML APIでは今回、そのIoCリストを出発点としてDNSインテリジェンスを駆使した調査を行い、以下を発見しました。

- P2PInfectのIoCとして特定された1個のドメイン名と同様に**worldive** という文字列を含んだ6個のドメイン名
- **redis**という文字列を含む10,000超のドメイン名。一括マルウェアチェックの結果、そのうち20個は悪意あるドメイン名に分類
- **redis**という文字列を含む10,000超のサブドメイン。一括マルウェアチェックの結果、そのうち6個は悪意あるサブドメインと確認

P2PInfectのIoCに関するDNS情報

P2PInfectのIoCとして特定された2個のドメイン名をWHOIS Lookupで検索したところ、結果が返ってきたのはmyhealthlifego[.]comのみでした。このドメイン名は2022年10月に新規登録され、レジストラはPDR Ltd.、登録された国は中国でした。他方、2個のドメイン名をDNS Lookupにかけた結果、myhealthlifego[.]comは66[.]154[.]127[.]38（P2PInfectのIoC）に名前解決しました。

次に、IoCとして特定された5個のIPアドレスをBulk IP Geolocation Lookupで調べたところ、以下が判明しました。

- 3個はカナダを起源とするIPアドレス
- 残りの2個はそれぞれ中国と米国に位置
- 5個のうち2個の管理ISPはQuadraNet Enterprises LLCでした。その他、Alibaba.com Singapore E-Commerce Private Limited、Amazon Technologies, Inc.（EC2)およびTruVista Communicationsがそれぞれ1個ずつを管理していました。

IoCとして特定されたIPアドレスをReverse IP Lookupにかけたところ、ドメイン名をホストし続けていたアドレスは1個（66[.]154[.]127[.]38）しかありませんでした。このアドレスは、myhealthlifego[.]comの専用ホストでした。

IoCとして特定された1個のドメイン名に含まれる**worldive**という文字列をDomains & Subdomains Discoveryで検索した結果、見た目が似ている6個のドメイン名が特定されました。ただし、本稿執筆時点では、それらのうち悪意のあるドメイン名に分類されたものはありません。

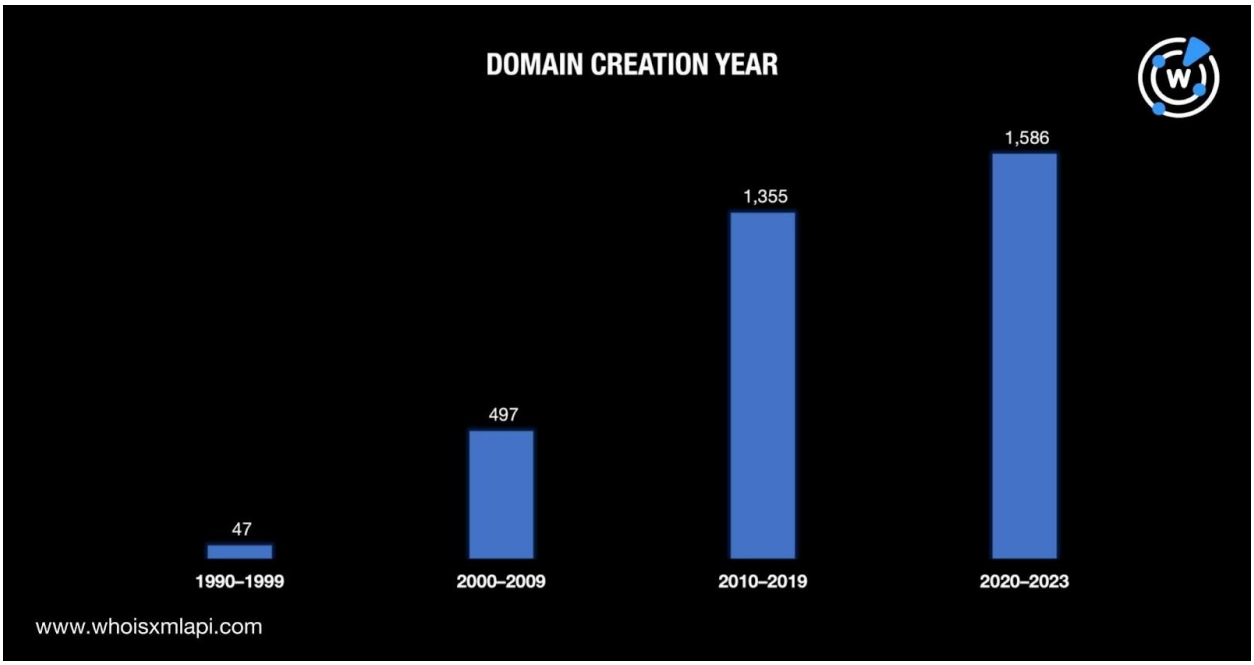
その6個のドメイン名のうちoneworldive[.]comは、いずれのWHOISレコードも非公開化されておらず、合法的な企業に属するドメイン名と思われました。実際、Googleで検索したところ、登記済みの合法的なダイビング・旅行会社が見つかりました。この会社はサイバースクワッティング対策として、公式ドメイン名であるoneworlddive[.]comのスペル違いを取得したのかもしれません。

Redisデバイスは他の攻撃の標的になっているか

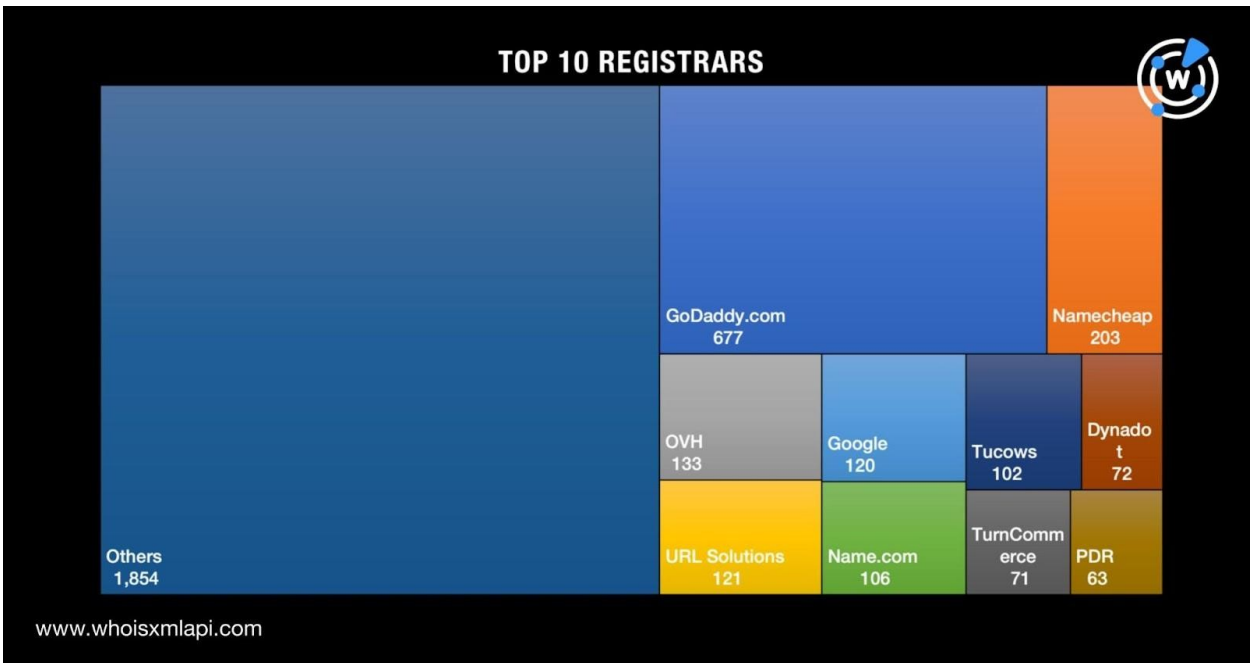
P2PInfectのDNS上の関連性を判断する以外にも、フィッシングやDNS乗っ取り攻撃など、脅威アクターが他の方法でRedisインスタンスを標的とした可能性があるかどうかを調査しました。この調査では、ドメイン名とサブドメインの両方を当社のDomains & Subdomains Discoveryで調べる際に、検索語として**redis**を使用しました。

その結果、**redis**を含むドメイン名が10,000あまり見つかりました。

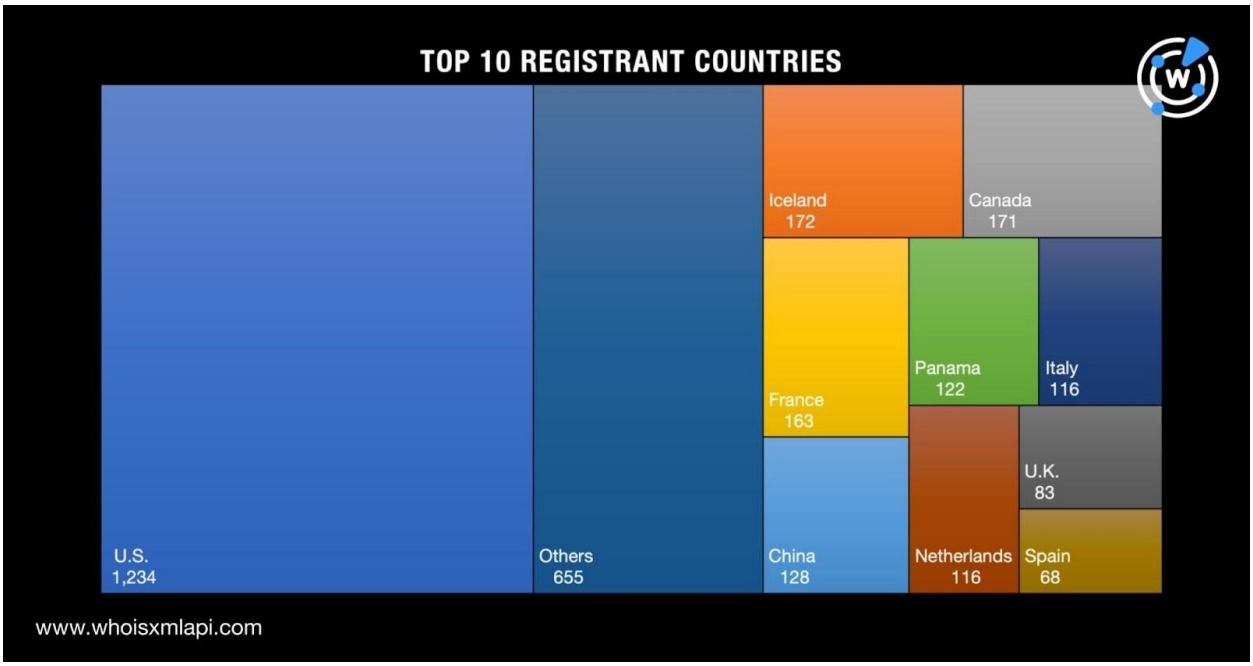
- WHOISレコードに作成日が記載されている3,485個のドメイン名は、1990年から2023年の間に作成されたものでした。



- ドメイン名登録者がレジストラを指定している3,522個のドメイン名は、677個を管理するGoDaddy.comを筆頭に、428のレジストラに分散していました。GoDaddyに次いでNamecheap（203個）、OVH（133個）、URL Solutions（121個）、Google（120個）、Name.com（106個）、Tucows（102個）、Dynadot（72個）、TurnCommerce（71個）、PDR（63個）がトップ10に入りました。



- 登録者の国が非公開化されていない3,028個のドメイン名は、95カ国で登録されていました。最も多かったのは米国で、1,234個でした。次いでアイスランド（172個）、カナダ（171個）、フランス（163個）、中国（128個）、パナマ（122個）、イタリアとオランダ（各116個）、英国（83個）、スペイン（68個）がトップ10にランクインしています。



redisを含むドメイン名を一括マルウェアチェックにかけたところ、20個が悪意あるドメイン名に分類されました。そのうち17個はマルウェアホスト、3個はスパム送信に使われていました。

それらの悪意あるドメイン名をScreenshot Lookupで検索した結果、7個はアクセス可能な状態にありました。そのうち2個は有効なコンテンツをホストしており、4個はエラーまたは空白のページに繋がりました。そして、残りの1個は売りに出されていました。有効なコンテンツをホストしていた2個のドメイン名のうち、wpredis[.]comは、ドメイン名だけを見ると、WordPressでホストされているRedis関連のブログのように思われます。しかし、下のスクリーンショットの通り、このドメイン名はブログをホストしているもののRedisとは何の関係もないようです。

wpredis[.]comのスクリーンショット

次に、**redis**を含むサブドメインのマルウェアを一括チェックしました。その結果、6つがマルウェアのホストであることが判明しました。

さらに、**redis**を含む悪意あるサブドメインのスクリーンショットを確認したところ、3個のサブドメインがアクセス可能な状態のままにありました。1個は有効なコンテンツをホストし続けており、2個はエラーページに誘導する状態でした。

—

今回、Redisの脆弱性を悪用したP2PInfectのIoCリストをもとに調査を広げ、IoCとして特定済みのドメイン名の1つに見た目が似ている別のドメイン名を見つけ出しました。また、脅威アクターがRedisを標的とした攻撃ですでに使用した、または将来悪用する可能性のあるドメイン名やサブドメインをDNSで検索した結果、25個の悪意あるウェブプロパティと20,000近くのアーティファクトを特定することができました。

なお、今回の調査結果は、「Redis Lua Sandbox Escape and Remote Code Execution Vulnerability」（CVE-2022-0543）に限らず、Redisの脆弱性を狙った攻撃が増えている可能性を示唆しています。見た目が似ているドメイン名はフィッシングキャンペーンに利用される恐れがあり、忘れられたサブドメインはDNS乗っ取りの媒介となる可能性があります。

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

Palo Alto Networksが特定したP2PInfectのIoC

- 35[.]183[.]81[.]182
- 66[.]154[.]127[.]38
- 66[.]154[.]127[.]39
- 8[.]218[.]44[.]75
- 97[.]107[.]96[.]14
- worldive[.]shop
- myhealthlifego[.]com

共通の文字列を含むドメイン名の例

- worldive[.]tk
- worldive[.]com[.]cn
- oneworldive[.]com

Redisのブランド名を含むドメイン名の例

- redis[.]ai
- redis[.]uz
- redis[.]sh
- redis[.]ro
- redis[.]it
- redis[.]hu
- redis[.]me
- redis[.]pt
- redis[.]ml
- redis[.]cf
- redis[.]ph
- redis[.]jp
- redis[.]ws
- redis[.]dk
- redis[.]nl
- redis[.]ga
- redis[.]xn--kprw13d
- redis[.]cl
- redis[.]cm
- redis[.]es
- redis[.]eu
- redis[.]xn--node
- redis[.]sk
- redis[.]nu
- redis[.]bg
- redis[.]us
- redis[.]se
- redis[.]ee
- redis[.]at
- redis[.]do
- redis[.]xn--mxtq1m
- redis[.]io

- redis[.]lt
- redis[.]pl
- redis[.]co
- redis[.]im
- redis[.]sg
- redis[.]su
- redis[.]kz
- redis[.]in
- redis[.]de
- redis[.]vn
- redis[.]al
- redis[.]fr
- redis[.]cn
- redis[.]tv
- redis[.]ru
- redis[.]tw
- redis[.]cz
- redis[.]xn--fiqz9s
- redis[.]uk
- redis[.]tk
- rediscoveredisto[.]com
- rediss[.]us
- redise[.]tk
- redisc[.]ru
- redish[.]tk
- redis[.]ink
- redisu[.]ga
- credis[.]uk
- redis[.]red
- redist[.]nl
- redisa[.]mx
- credis[.]pt
- redis[.]fit
- redisu[.]tk
- redish[.]cn
- redisc[.]si
- redisc[.]de
- credis[.]it
- redish[.]de
- redisk[.]de
- tredis[.]fr
- redisc[.]fi
- redist[.]pe
- jredis[.]io
- redisb[.]es
- redist[.]tv
- redis[.]app
- kredis[.]de
- bredis[.]de
- redist[.]de
- redish[.]me
- rediso[.]in
- fredis[.]lt
- redis[.]ltd
- redist[.]cn
- credis[.]fr
- redis[.]pro
- redist[.]hu
- redis[.]xin
- redist[.]pl
- kredis[.]be
- redist[.]tk
- aredis[.]tk
- fredis[.]tk
- redisk[.]ca
- gredis[.]it
- redisa[.]cl
- aredis[.]fr
- gredis[.]pl
- redisk[.]ru
- redisu[.]cn
- fredis[.]dk
- redish[.]se
- redise[.]ru
- fredis[.]de
- eredis[.]fr
- redisy[.]jp
- redisq[.]ru
- credis[.]cz
- gredis[.]ws

- redis[.]day
- credis[.]co
- redis[.]new
- tredis[.]pl
- redist[.]ru
- redisa[.]ir
- predis[.]se
- redist[.]in
- redist[.]at
- redish[.]dk
- credis[.]id
- redisa[.]in
- redish[.]co
- fredis[.]fr
- redish[.]uk
- redisa[.]pe
- oredis[.]eu
- kredis[.]in
- redisc[.]fr
- redisk[.]cn
- iredis[.]es
- redisp[.]nl
- redis[.]net
- credis[.]pl
- redism[.]cc
- dredis[.]it
- redis1[.]cn
- redis[.]vip
- redisa[.]ru
- redisk[.]it
- aredis[.]ch
- tredis[.]ru
- iredis[.]uk
- credis[.]be
- redisk[.]tk
- bredis[.]fi
- redis[.]run
- redism[.]ga
- fredis[.]no
- redis[.]llc
- bredis[.]ru
- credis[.]ro
- predis[.]tk
- redis[.]gdn
- credis[.]bg
- gredis[.]ru
- aredis[.]de
- kredis[.]it
- redis[.]fun
- rediso[.]ga
- credis[.]ba
- rediss[.]es
- credis[.]de
- redist[.]us
- credis[.]cc
- redism[.]us
- redisc[.]tk
- oredis[.]ma
- redish[.]ee
- tredis[.]de
- redisv[.]cl
- redis[.]xn--ngbrx
- redist[.]cf
- credis[.]es
- kredis[.]ru
- oredis[.]fr
- bredis[.]fr
- eredis[.]uk
- eredis[.]ru
- redis[.]pub
- rediss[.]ru
- predis[.]eu
- redish[.]ru
- predis[.]ca
- redise[.]ml
- redish[.]jp
- predis[.]es
- predis[.]cn
- redis[.]com
- redish[.]us

- redis[.]ooo
- redis[.]kim
- redisk[.]ga
- redish[.]eu
- redist[.]eu
- credis[.]eu
- redisa[.]es
- predis[.]ru
- predis[.]us
- redist[.]me
- redist[.]ga
- redise[.]cn
- credis[.]sk
- redisu[.]gq
- redisa[.]co
- kredis[.]fr
- predis[.]co
- tredis[.]eu
- redist[.]fr
- redise[.]co
- redisi[.]cf
- redisi[.]ga
- kredis[.]kz
- kredis[.]pl
- predis[.]it
- redisc[.]dk
- zredis[.]ru
- redisu[.]cf
- fredis[.]at
- fredis[.]xn--fiqs8s
- redise[.]ph
- redist[.]co
- redis[.]icu
- tredis[.]it
- redist[.]ro
- redist[.]sk
- redisc[.]it
- redis[.]cfd
- oredis[.]vg
- redis[.]biz
- credis[.]se
- predis[.]ai
- predis[.]fr
- rediso[.]de
- redis[.]ren
- redis3[.]vg
- redish[.]cf
- redist[.]ir
- redisk[.]io
- tredis[.]hu
- aredis[.]at
- iredis[.]io
- redis[.]one
- predis[.]io
- credis[.]ru
- redisp[.]cz
- rediso[.]ru
- gredis[.]eu
- credis[.]at
- redist[.]es
- redist[.]ca
- redisp[.]ru
- redis[.]org
- redis[.]xyz
- redis[.]mom
- credis[.]cn
- aredis[.]eu
- tredis[.]co
- rediso[.]cn
- redisa[.]ml
- redis[.]dev
- redisu[.]ml
- kredis[.]ga
- redis[.]lol
- redise[.]nl
- redist[.]mk
- redish[.]ch
- credis[.]nl
- credis[.]us
- predis[.]nl

- predis[.]de
- kredis[.]hr
- redisa[.]se
- predis[.]ga
- fredis[.]ru
- redist[.]be
- fredis[.]sk
- gredis[.]de
- redist[.]io
- kredis[.]lt
- redisa[.]tk
- redisgn[.]co
- tredish[.]hu
- redisin[.]ru
- redish[.]red
- redisx[.]com
- ymredis[.]tk
- redis[.]love
- xredis[.]xyz
- redis[.]blog
- redisg[.]com
- redisw[.]com
- dsredis[.]me
- redis-1[.]ws
- tredish[.]co
- meredis[.]gq
- redise[.]xyz
- redisea[.]ml
- riredis[.]ga
- foredis[.]ca
- igredis[.]tk
- redisru[.]ga
- credisy[.]fr
- redis[.]help
- redisbi[.]tk
- maredis[.]gr
- caredis[.]fr
- redissu[.]ml
- redista[.]es
- arredis[.]tk
- meredis[.]de
- redismc[.]us
- redise[.]net
- meredis[.]tk
- predisa[.]ru
- kredist[.]se
- arediss[.]fr
- redisrw[.]eu
- 2redis[.]top
- redisly[.]tk
- abredis[.]tk
- redisfe[.]tk
- redisre[.]gq
- redisre[.]ga
- redisli[.]ga
- enredis[.]tk
- meredis[.]eu
- credis[.]xyz
- redisco[.]sa
- redisju[.]ml
- credisi[.]co
- diredis[.]ml
- redisp[.]com
- mredis[.]com
- 3redis[.]top
- agredis[.]tk
- redish[.]biz
- redish[.]top
- redist[.]org
- heredis[.]uk
- atredis[.]ru
- rediso[.]net
- predist[.]pw
- dbredis[.]cn
- rediso[.]biz
- giredis[.]ml
- auredis[.]fr
- redish[.]dev
- riredis[.]cf
- predis[.]cat

- redisis[.]us
- redisn[.]com
- ceredis[.]be
- prediss[.]us
- raredis[.]ru
- caredis[.]eu
- redis24[.]io
- redisb[.]com
- redis[.]site
- redish[.]com
- horedis[.]eu
- anredis[.]cf
- redisco[.]es
- oredis[.]net
- redis[.]asia
- redisri[.]tk
- redis[.]info
- redisml[.]io
- redisai[.]io
- erredis[.]tk
- redist[.]top
- neredis[.]ru
- 1redis[.]top
- redis[.]guru
- redisly[.]ml
- fredis[.]org
- redismo[.]cf
- redisaw[.]us
- foredis[.]ru
- giredis[.]tk
- acredis[.]be
- fredisc[.]pl
- acredis[.]cz
- seredis[.]fr
- predise[.]cn
- gredis[.]com
- predis[.]net
- geredis[.]eu
- alredis[.]fr
- redisra[.]ml
- rediseb[.]de
- crediso[.]at
- predis[.]biz
- rediss[.]biz
- rediska[.]su
- redisu[.]com
- redisen[.]de
- inredis[.]es
- paredis[.]be
- atredis[.]us
- eredis[.]com
- arredis[.]de
- heredis[.]co
- redisko[.]es
- redisme[.]ga
- redisfi[.]cf
- horedis[.]ch
- redise[.]biz
- predisa[.]pt
- redisok[.]tk
- redisai[.]ml
- inredis[.]tk
- kredisi[.]vg
- predisi[.]de
- karedis[.]au
- heredis[.]se
- redise[.]com
- coredis[.]mg
- reredis[.]gq
- kredist[.]ru
- moredis[.]de
- redison[.]nl
- redisva[.]tk
- redisre[.]tk
- redisgo[.]uk
- orredis[.]ga
- moredis[.]ga
- agredis[.]ro
- redisco[.]ru
- gredis[.]biz

- redis1[.]cpa
- ikredis[.]eu
- redisio[.]cn
- reredis[.]cf
- redisju[.]es
- prediss[.]fr
- maredis[.]is
- rediski[.]ru
- myredis[.]cn
- aredis[.]org
- credis[.]com
- eredis[.]dev
- coredis[.]fr
- fredis[.]gay
- rediss[.]org
- heredis[.]ca
- eredis[.]xyz
- fredis[.]com
- tredis[.]com
- redist[.]pro
- crediso[.]ro
- redish[.]fun
- xn--crdise-cva[.]fr
- hiredis[.]ga
- redisos[.]ga
- bredis[.]org
- acredis[.]us
- gredis[.]net
- wiredis[.]tk
- rediski[.]cc
- heredis[.]lu
- credisu[.]tk
- predisp[.]tk
- redistr[.]io
- rediswr[.]eu
- redis[.]arab
- arredis[.]eu
- redis[.]wiki
- predish[.]cn
- credisa[.]co
- kredis[.]com
- syredis[.]fr
- credisa[.]ch
- redisco[.]be
- redisma[.]tk
- redisa[.]dev
- redissi[.]fr
- redist[.]net
- rediso[.]com
- redis[.]tech
- redise5[.]ee
- redisfi[.]ml
- euredis[.]eu
- credisa[.]ru
- rediski[.]tk
- redisca[.]cf
- redisky[.]cz
- fredis[.]xyz
- heredis[.]cm
- rediska[.]tk
- acredis[.]es
- toredis[.]tk
- credist[.]ar
- redis24[.]ru
- redisol[.]ph
- predise[.]gr
- giredis[.]cf
- giredis[.]gq

Sample Malicious Brand-Containing Domains

- redisw[.]com
- redisly[.]tk
- redish[.]top
- redis24[.]ru
- wpredis[.]com
- rediska[.]site

- fredis[.]online
- kredisafe[.]com
- conperedis[.]tk
- redis-ppl[.]com

Redisのブランド名を含むサブドメインの例

- redis[.]redis[.]cle[.]com[.]ua
- 2redisgredist[.]coredis[.]expediagroup[.]com
- redis[.]redis[.]typhoon-s1[.]ru
- redis[.]redis[.]alltr[.]xyz
- redis[.]redis[.]dnkroz[.]es
- redis-hiredis[.]yuna-card[.]com
- redis-hiredis[.]vk[.]cc
- redis-hiredis[.]preloved[.]co[.]uk
- howredisredis[.]mamx[.]group
- aredisredisount8[.]redisom[.]expediagroup[.]com
- howredisredis[.]telensa[.]com
- howredisredis[.]leagueoflegends[.]asia
- howredisredis[.]foodpanda[.]com
- redis[.]fmlredis[.]findmylost[.]nl
- 00[.]redis[.]redis[.]expediagroup[.]com
- ladredis[.]test[.]aredisrediss[.]bamboohr[.]com
- redisuroprediswredisst[.]tredisst[.]apps[.]bamboohr[.]com
- loadredisesredising[.]redisesredis[.]apps[.]bamboohr[.]com
- intreredisidgrouredis[.]test[.]aredisrediss[.]bamboohr[.]com
- aredisredisount-lb[.]redisom[.]expediagroup[.]com
- redis-6379[.]redis[.]litix[.]io
- redis-masrediser[.]kahoot[.]it
- redissoneredissonm[.]redissonom[.]expediagroup[.]com
- redis-10000[.]redis[.]cvs[.]com
- redis-redis-admin[.]modema-server[.]com
- dredistredisde-rredisjeev[.]lredisyerdevfyndiqemredisils[.]redisutodiscover[.]github[.]com
- redis[.]redis[.]apiv2[.]pir[.]ru
- kfkadredis03[.]test[.]aredisrediss[.]bamboohr[.]com
- rabbitredisq-redisqtt-adredisin[.]tadaam[.]be
- redis0[.]redis[.]cache[.]windows[.]net
- redis[.]clearhost[.]io
- redis[.]uh-group[.]tk
- redis[.]wicloz[.]rocks
- redis[.]polanddaily24[.]com
- redis[.]omnileaf[.]ml
- redis[.]perdananetwork[.]id
- redis[.]twitchy-event[.]com
- redis[.]korea-police[.]com
- redis[.]mbot[.]me
- redis[.]5-systems[.]ru
- redis[.]changelogfy[.]com
- redis[.]luongld[.]com
- redis[.]worklifebeyond[.]com
- redis[.]r1s-test[.]com
- redis[.]tkin[.]co
- redis[.]memedate[.]app
- redis[.]info-torg[.]ru
- redis[.]zoomsurcostarica[.]com
- redis[.]198201[.]top
- redis[.]dein-gameserver[.]tech
- redis[.]eresult[.]ml
- redis[.]errrr[.]news
- redis[.]goaland[.]info
- redis[.]i-media[.]io

- redis[.]iventy[.]fr
- redis[.]jidemo[.]at
- redis[.]jordanliu[.]net
- redis[.]kent[.]ac[.]uk
- redis[.]los-dc[.]com
- redis[.]lovean[.]net
- redis[.]next[.]health
- redis[.]paybro[.]com[.]mx
- redis[.]primpogoda[.]ru
- redis[.]rjmetrics[.]com
- redis[.]sakkathstudio[.]com
- redis[.]statnet[.]pl
- redis[.]tak-mail[.]com
- redis[.]wopsy[.]co
- redis[.]dongming168[.]com
- redis[.]komojo[.]de
- redis[.]athena-server[.]net
- redis[.]cfsoft[.]cn
- redis[.]41st[.]es
- redis[.]apjapan[.]ru
- redis[.]netpeak[.]cloud
- redis[.]ccc1618[.]xyz
- redis[.]bac901[.]com
- redis[.]webup[.]link
- redis[.]futureporn[.]net
- redis[.]lyre[.]us
- redis[.]snoringdragon[.]org
- redis[.]osfe[.]art
- redis[.]pantayun[.]net
- redis[.]means-business[.]info
- redis[.]livestockdata[.]net
- redis[.]bayestech[.]ru
- redis[.]szmengran[.]com
- redis[.]metaverseservlet[.]com
- redis[.]winrichjob[.]com
- redis[.]rmorrissey[.]io
- redis[.]copper-dev[.]com
- redis[.]jafcp[.]com
- redis[.]stoachup[.]be
- redis[.]finspire[.]tech
- redis[.]bareways[.]com
- redis[.]bompotis[.]com
- redis[.]cirql[.]app
- redis[.]pilm[.]app
- redis[.]zerano[.]digital
- redis[.]robcooper[.]dev
- redis[.]chateaufjeldsted[.]com
- redis[.]carloslapao[.]com
- redis[.]unionpay188[.]com
- redis[.]fairplayclub[.]net
- redis[.]the7minutelife[.]com
- redis[.]hadaf[.]host
- redis[.]ndsboy[.]de
- redis[.]onlineradiop[.]com
- redis[.]ruzhbi[.]ru
- redis[.]dev-avos[.]com
- redis[.]hidatahub[.]com
- redis[.]techluxid[.]com
- redis[.]mediavoicemm[.]com
- redis[.]web-tef[.]my[.]id
- redis[.]runeclawgames[.]com
- redis[.]plugins[.]club
- redis[.]tekce[.]net[.]tr
- redis[.]dignative[.]cc
- redis[.]jange[.]de
- redis[.]quazgar[.]net
- redis[.]wallib[.]xyz
- redis[.]kainonly[.]com
- redis[.]elpsykongroo[.]com
- redis[.]305365[.]org
- redis[.]hc32dbwzn8e[.]cfd
- redis[.]barba[.]tech
- redis[.]learn4good[.]com
- redis[.]batesweb[.]tech
- redis[.]panghu[.]co
- redis[.]redwhiteanalytics[.]com
- redis[.]capitalenesti[.]com
- redis[.]innate[.]io
- redis[.]ugy9zrfdn[.]xyz
- redis[.]xarxa[.]interna

- redis[.]lfpconnect[.]io
- redis[.]0xff[.]xyz
- redis[.]vetrinas[.]ly
- redis[.]energynet[.]lol
- redis[.]yoga-zarydka[.]ru
- redis[.]mingyueguang[.]xyz
- redis[.]grupofocus[.]com[.]br
- redis[.]levvy[.]net
- redis[.]uptimesignal[.]com
- redis[.]bsi3y6tjd[.]xyz
- redis[.]hkdeepi[.]tech
- redis[.]kurento[.]org
- redis[.]confirmed[.]church
- redis[.]meyca[.]de
- redis[.]expressbyholidayinn[.]co
- redis[.]hiexpress[.]travel
- redis[.]sorice[.]info
- redis[.]danial23[.]com
- redis[.]gotivochka[.]pp[.]ua
- redis[.]bugatino[.]dev
- redis[.]securesa[.]co[.]za
- redis[.]gerhut[.]me
- redis[.]rdxt[.]com
- redis[.]axr[.]io
- redis[.]psymate[.]io
- redis[.]apselectric[.]com[.]br
- redis[.]tabbit[.]us
- redis[.]iwritesoftware[.]net
- redis[.]expectedgold[.]com
- redis[.]linion[.]net
- redis[.]xqz[.]pw
- redis[.]papercell[.]ir
- redis[.]uvensys[.]systems
- redis[.]binksma[.]de
- redis[.]cariuska[.]dev
- redis[.]crazedencoder[.]com
- redis[.]pet-test[.]work
- redis[.]sandos[.]cl
- redis[.]t3s[.]es
- redis[.]tandav[.]me
- redis[.]pintamundiboavista[.]com[.]br
- redis[.]riverlog[.]info
- redis[.]evy24[.]com
- redis[.]asanglobal[.]ir
- redis[.]zeepkist-gtr[.]com
- redis[.]redis[.]docker[.]stagewp[.]co
- redis[.]lexyourwebsitemaker[.]com
- redis[.]elevennerd[.]de
- redis[.]sciflow[.]net
- redis[.]wdboer[.]nl
- redis[.]playsmart[.]ir
- redis[.]neuai[.]cn
- redis[.]neighbourhoodnet[.]work
- redis[.]amoyensis[.]com
- redis[.]xea-twitcht[.]com
- redis[.]futuretravelplatform[.]com
- redis[.]sellinglive[.]com
- redis[.]tgrains[.]com
- redis[.]pafcode[.]cloud
- redis[.]jinchen[.]cloud
- redis[.]moonsolution[.]ru
- redis[.]unixy[.]net
- redis[.]pnwhatsapp[.]online
- redis[.]x22[.]io
- redis[.]holyhub[.]xyz
- redis[.]hubedev[.]com
- redis[.]muzeapp[.]io
- redis[.]catallact[.]com
- redis[.]quancy[.]com[.]sg
- redis[.]sdsrv01[.]ch
- redis[.]twisted-rope[.]com
- redis[.]vbuckstool[.]pw
- redis[.]xoffx[.]com
- redis[.]baobeinihao[.]com
- redis[.]cfgglobal[.]co[.]nz
- redis[.]devopsculture[.]ca
- redis[.]fabiofava[.]com
- redis[.]fantuan[.]ca
- redis[.]freeriding[.]us
- redis[.]gamequitters[.]com

- redis[.]iad-engage[.]tk
- redis[.]j4u[.]su
- redis[.]lockstate[.]com
- redis[.]xfantasy[.]tv
- redis[.]youmine[.]xyz
- redis[.]zxcs[.]nl
- redis[.]vuebit[.]com
- redis[.]web-production[.]pl
- redis[.]zeemi[.]tv
- redis[.]pizket[.]com
- redis[.]reeves[.]one
- redis[.]roadreadyapp[.]com
- redis[.]youqianlaile[.]com
- redis[.]jihuayu[.]site
- redis[.]lalizas[.]gr
- redis[.]sessionlinkpro[.]com
- redis[.]shuttlestage[.]com
- redis[.]spankbang[.]site
- redis[.]devnet[.]rs
- redis[.]tengtoo[.]com
- redis[.]planos[.]dev
- redis[.]softagon[.]app
- redis[.]mektoube[.]fr
- redis[.]1473[.]cn
- redis[.]3lados[.]com[.]br
- redis[.]clomp-spirion[.]com
- redis[.]8o0[.]cc
- redis[.]camelwifi[.]cn
- redis[.]bitcoingameapps[.]com
- redis[.]playground-spirion[.]com
- redis[.]us1home[.]com
- redis[.]fx55bj5[.]cn
- redis[.]dreamwidth[.]org
- redis[.]wilcodeboer[.]me
- redis[.]sledge[.]fr
- redis[.]obotai[.]com
- redis[.]promedik[.]com
- redis[.]paine[.]nyc
- redis[.]asppj[.]top
- redis[.]bitloops[.]net
- redis[.]automovers[.]us
- redis[.]boxee[.]sh
- redis[.]villain[.]school
- redis[.]lufuhu[.]com
- redis[.]moveitpro[.]com
- redis[.]videosave[.]xyz
- redis[.]abangkito[.]xyz
- redis[.]robertocastan[.]com
- redis[.]tommyngo[.]co[.]nz
- redis[.]nomic[.]cloud
- redis[.]fruit-cloud[.]de
- redis[.]musiccord[.]cloud
- redis[.]remenxs[.]com
- redis[.]zamzam[.]dev
- redis[.]bmdlapp[.]com
- redis[.]luckystore[.]com[.]sg
- redis[.]sendchamp[.]live
- redis[.]wxfggzs[.]com
- redis[.]proctorio[.]com
- redis[.]hqjltech[.]com
- redis[.]letgo[.]com
- redis[.]poullailerduburck[.]fun
- redis[.]thijn[.]ovh
- redis[.]mode14[.]io
- redis[.]marsh[.]gg
- redis[.]hlx[.]co
- redis[.]wxp-2[.]nl
- redis[.]chiphosting[.]org
- redis[.]astoundvideo[.]net
- redis[.]increev[.]com
- redis[.]starclass[.]academy
- redis[.]geekyco[.]de
- redis[.]nbfc[.]io
- redis[.]vmt[.]ir
- redis[.]tinymarshmallow[.]dev
- redis[.]eternalbits[.]net
- redis[.]futwebapp[.]tk
- redis[.]cshisan[.]com
- redis[.]attractive[.]media
- redis[.]creationspl[.]com

- redis[.]g-by-g[.]kr
- redis[.]onursay[.]com
- redis[.]opencard[.]us
- redis[.]vivinatura[.]site
- redis[.]kevingyorick[.]com
- redis[.]lendfusiondemo[.]com
- redis[.]d4win[.]net
- redis[.]ededi[.]si
- redis[.]investidea[.]tech
- redis[.]test-avos[.]com
- redis[.]wowpowers[.]com
- redis[.]rackspace[.]com
- redis[.]g7ut8arhj6[.]xyz
- redis[.]guildwars2[.]com
- redis[.]micro-tech[.]com[.]vn
- redis[.]thingdustdata[.]com
- redis[.]housepartyfun[.]com
- redis[.]scalegrid[.]io
- redis[.]funarcade[.]io
- redis[.]cbgroup[.]biz
- redis[.]0x007[.]me
- redis[.]broadband[.]deals
- redis[.]nft500[.]io
- redis[.]magitek[.]no
- redis[.]bookholidayinns[.]com
- redis[.]candlewoodsuites[.]asia
- redis[.]mozumder[.]net
- redis[.]mexzona[.]xyz
- redis[.]webuscomms[.]com
- redis[.]fallensword[.]com
- redis[.]inovan[.]do
- redis[.]makomaki[.]ru
- redis[.]donavanaldrich[.]com
- redis[.]charismabi[.]com
- redis[.]filmofilia[.]com
- redis[.]moneyfan[.]ru
- redis[.]partywizz[.]com
- redis[.]qtalents[.]co
- redis[.]aedashomes[.]com
- redis[.]maunu[.]group
- redis[.]cpcloud[.]nl
- redis[.]xebok[.]net
- redis[.]softur[.]com[.]ar
- redis[.]my-jewellery[.]business
- redis[.]noblecollection[.]ca
- redis[.]pypiptech[.]ir
- redis[.]leadingpath[.]com
- redis[.]smartloyalty[.]vn
- redis[.]homescriptone[.]com
- redis[.]jugru[.]team
- redis[.]kt-pulse[.]dev
- redis[.]evotide[.]com
- redis[.]zerwin[.]me
- redis[.]riso[.]lol
- redis[.]nabytek-natali[.]cz
- redis[.]noisepalace[.]co[.]uk
- redis[.]rectelework[.]com
- redis[.]vrizead[.]com
- redis[.]onlinepos[.]me
- redis[.]kurer-sreda[.]ru
- redis[.]rh-trader[.]com
- redis[.]fastvelocity[.]com
- redis[.]tulbure[.]net
- redis[.]postcodes[.]fi
- redis[.]tocomsorte[.]com[.]br
- redis[.]aagc[.]xyz
- redis[.]qa-carris-cloud[.]ga
- redis[.]0sy1s[.]com
- redis[.]conectivax[.]uk
- redis[.]brocorp[.]site
- redis[.]coolops[.]cn
- redis[.]developcloud[.]ml
- redis[.]heliospal[.]net
- redis[.]linuxcrypt[.]cn
- redis[.]30kan[.]com
- redis[.]maximustest[.]ru
- redis[.]aboalarm[.]de
- redis[.]squash-app[.]win
- redis[.]mojetestovacidomena[.]cz
- redis[.]hackyhack[.]net

- redis[.]astawmind[.]se
- redis[.]dev-pulsemi[.]com
- redis[.]truespider[.]com
- redis[.]ugr[.]es
- redis[.]welltycoon[.]dev
- redis[.]yeradonkey[.]com
- redis[.]digitalopera[.]io
- redis[.]contender[.]com
- redis[.]deepbrain[.]net[.]cn
- redis[.]deliverakis[.]chat
- redis[.]flum[.]pw
- redis[.]freeform[.]ca
- redis[.]huhsp[.]org[.]br
- redis[.]jimmytest[.]nl
- redis[.]mygomel[.]com
- redis[.]myhubapp[.]net
- redis[.]rezervacesluzeb[.]cz
- redis[.]sbuntu[.]com
- redis[.]shuttlerock[.]org
- redis[.]silly[.]horse
- redis[.]soinge[.]ga
- redis[.]thecatapult[.]io
- redis[.]bluepix[.]cz
- redis[.]chaturbate[.]com
- redis[.]felixlabs[.]xyz
- redis[.]gamemonitoring[.]net
- redis[.]21tec[.]cn
- redis[.]asprl[.]com
- redis[.]btclear[.]io
- redis[.]communick[.]com
- redis[.]douglaspinheiro[.]dev
- redis[.]lavanderia60minutos[.]com[.]br
- redis[.]leonardschuetz[.]ch
- redis[.]medopps[.]org
- redis[.]reelead[.]com
- redis[.]tongsong[.]top
- redis[.]weidaibaobei1[.]com
- redis[.]xuanthulab[.]net
- redis[.]majunwei[.]com
- redis[.]peterkeyser[.]ca
- redis[.]kaarix[.]work
- redis[.]becard[.]me
- redis[.]szkt[.]cc
- redis[.]bestmixer[.]online
- redis[.]peachtreedir[.]com
- redis[.]flolio[.]com
- redis[.]evoluumlab[.]com[.]br
- redis[.]itmm[.]ru
- redis[.]pvu[.]one
- redis[.]dshibainu[.]com
- redis[.]knowhowcommunity[.]org
- redis[.]niezalezneforum[.]pl
- redis[.]34353[.]org
- redis[.]ismdeep[.]com
- redis[.]hardrize[.]tk
- redis[.]mayanserver[.]com
- redis[.]xea-rewardsprime[.]com
- redis[.]zerobugware[.]com
- redis[.]blogg[.]click
- redis[.]nightowl[.]name
- redis[.]port80[.]ch
- redis[.]toan[.]one
- redis[.]strelkov[.]net
- redis[.]sogam[.]org
- redis[.]mukabrasil[.]com[.]br
- redis[.]yly[.]plus
- redis[.]personio-internal[.]de
- redis[.]kkri[.]cn
- redis[.]fernandescontabilidade[.]com
- redis[.]newspink[.]top
- redis[.]joopyo[.]design
- redis[.]tameliorate[.]com
- redis[.]saspe[.]com[.]br
- redis[.]anuto[.]net
- redis[.]babyready[.]io
- redis[.]lexul[.]dev
- redis[.]iraki[.]net
- redis[.]opinaka[.]co
- redis[.]hushuaikang[.]top

- redis[.]autodarts[.]io
- redis[.]warmhealth[.]com
- redis[.]ktc[.]de
- redis[.]orixdev[.]xyz
- redis[.]jxpanda[.]com
- redis[.]enimaloc[.]fr
- redis[.]revrebel[.]cloud
- redis[.]capsilon[.]com
- redis[.]showmefit[.]app
- redis[.]treebal[.]green
- redis[.]devawaken[.]com
- redis[.]rassvet-nf[.]ru
- redis[.]producttutor[.]net
- redis[.]primafrance[.]com
- redis[.]lotusit[.]ba
- redis[.]gs-demo[.]net
- redis[.]hayuq[.]com
- redis[.]dobro[.]website
- redis[.]transang[.]me
- redis[.]raweonline[.]com
- redis[.]vitalized[.]co[.]uk
- redis[.]adcm[.]uk
- redis[.]amli[.]cloud
- redis[.]quick123[.]net
- redis[.]april[.]com[.]br
- redis[.]mb[.]com[.]br
- redis[.]golfballs[.]com
- redis[.]yooi[.]io
- redis[.]weotaku[.]space
- redis[.]bcloud[.]ca
- redis[.]ittailors[.]net
- redis[.]05007com[.]site
- redis[.]quip[.]com
- redis[.]skyonbook[.]com
- redis[.]oiio[.]media
- redis[.]cplus[.]com[.]br
- redis[.]rdrct[.]eu
- redis[.]wedodata[.]de
- redis[.]preparedformore[.]ca
- redis[.]bgorgeous[.]asia
- redis[.]score[.]study
- redis[.]bemcuidartech[.]com[.]br
- redis[.]divvy[.]co
- redis[.]krumpled[.]com
- redis[.]mysoft[.]re
- redis[.]learnserver[.]online
- redis[.]tradenest[.]in

Redisのブランド名を含む悪意あるサブドメインの例

- redis[.]redis[.]typhoon-s1[.]ru
- redis[.]leha-vnuk[.]online
- redis[.]soolo[.]tools