DNSを深堀り：そのVPNサービス、実は偽装OpcJackerかもしれません

目次

要旨

インターネット閲覧の危険性が増すにつれ、サイバー脅威に対処するツールも増えてきています。例えば、データプライバシー侵害の増加を背景に、VPNサービスはいたるところで利用されるようになりました。では、VPNソフトウェアのインストーラと思われるものをダウンロードした結果マルウェアに感染してしまった場合はどうなるのでしょうか。

Trend Microが行ったOpcJackerの詳細な調査から、その答えがわかるかもしれません。OpcJackerはVPNソフトウェアのインストーラを偽装したマルウェアで、インストールされると、ハイジャックの目的でユーザーのキーストロークを記録し、スクリーンショットを撮り、機密のブラウザデータを盗み、追加の悪意あるモジュールをロードし、暗号通貨ウォレットのIDを置き換えます。

セキュリティ研究者のJaromir HorejsiとJoseph C. Chenは、33個のOpcJackerのセキュリティ侵害インジケーター（IoC）（30個のドメイン名と3個のIPアドレス）を特定しました。具体的には以下の通りです。

ドメイン名	IPアドレス
• alle13net1[.]com • alle13net2[.]com • comes1[.]com • comes2[.]com • gattri1[.]com • gattri2[.]com • installer-xvpn-g[.]site • installer-xvpn-h[.]site • installer-xvpn-k[.]site • installer-xvpn-n[.]site • irbxvpn[.]site • irexvpn[.]site • irfxvpn[.]site	• 185[.]163[.]45[.]36 • 94[.]158[.]244[.]118 • 206[.]188[.]197[.]199

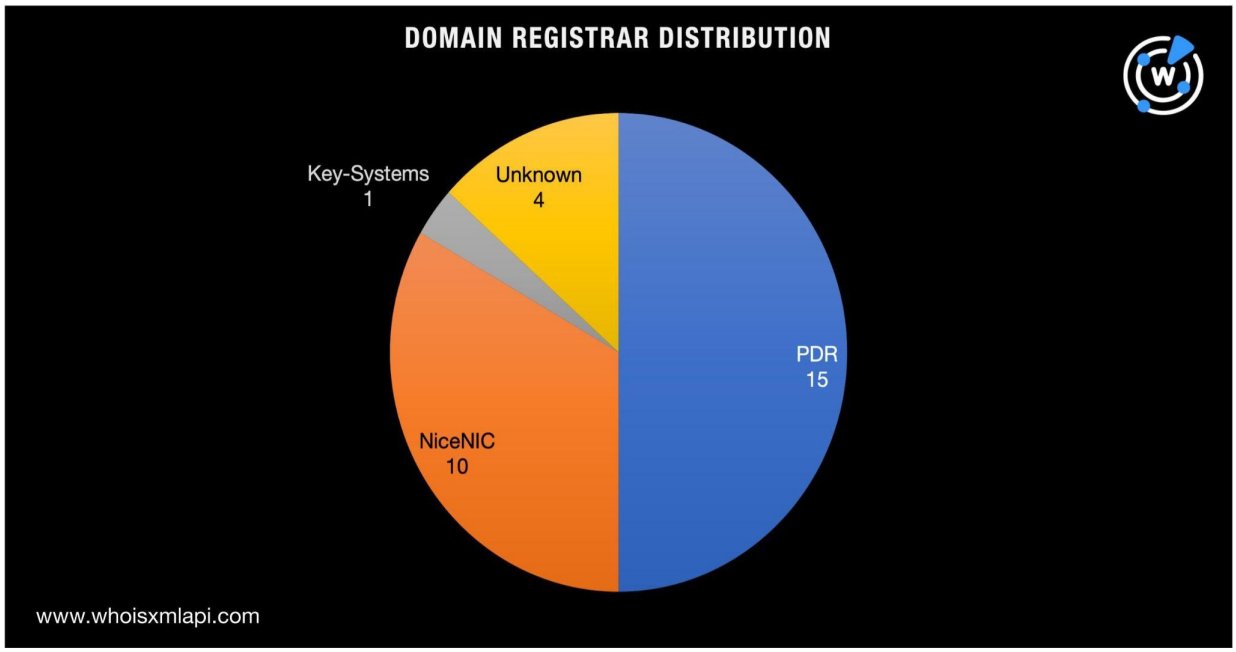
• irhxvpn[.]site • irixvpn[.]site • irkxvpn[.]site • irqxvpn[.]site • irtxvpn[.]site • iruxvpn[.]site • irwxvpn[.]site • manigiajabae32[.]com • manigiajabae35[.]com • neskrab1[.]com • neskrab2[.]com • nesupcli[.]com • she32rn1[.]com • she32rn2[.]com • uhcoxvpn[.]site • uzurtela1[.]com • uzurtela42[.]com	

WhoisXML APIの研究チームでは、上記のIoCリストを拡張してDNSを詳しく調べ、他の潜在的偽装VPNの脅威ベクトルを探し出すことにしました。その調査の結果、以下を発見しました。

- 一部のドメインIoCをホストしていたIPアドレスを新たに7個。そのうち3個は悪意あるIPアドレスと確認
- 一部のIPアドレスIoCを共用していたドメイン名を新たに441個。そのうち10個はマルウェアホストと確認
- ***vpn***という文字列を含む10,000個のドメイン名。そのうち12個は悪意あるドメイン名と確認

OpcJackerのIoCに関する事実

まず、IoCとされた30個のドメイン名をbulk WHOIS lookupで検索しました。その結果、26個のドメイン名のレジストラは公開情報から特定できました。具体的には、15個はPDR Ltd.、10個はNiceNIC International Group Co. Limited 、1個はKey-Systems GmbH がそれぞれ管理しているドメイン名でした。



30個のドメイン名は全て今年の2月に新規登録されたばかりのものでした。また、全てがロシアで登録されたドメイン名とわかりました。

3個のIPアドレスIoCをbulk IP geolocation lookupで検索した結果、3つの国（モルドバ、米国、オランダ）でそれぞれ登録されたものと判明しました。また、2つはMivoCloud SRL、残りの1つはBL Networksの管理下にありました。

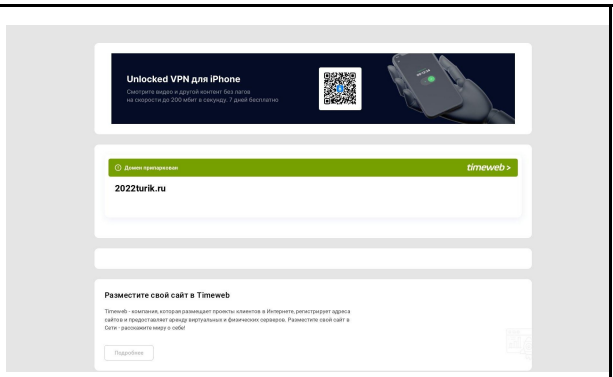
OpcJackerのIoCリストを拡張

IoCに関連している可能性のあるアーティファクトをさらに見つけるため、ドメインIoCをDNS lookupにかけました。その結果、5カ国に分散する7個のIPアドレスが新たに見つかりました。3個は地理的に米国にあり、そのほかドイツ、オランダ、ロシア、英国にそれぞれ1つずつ位置していました。

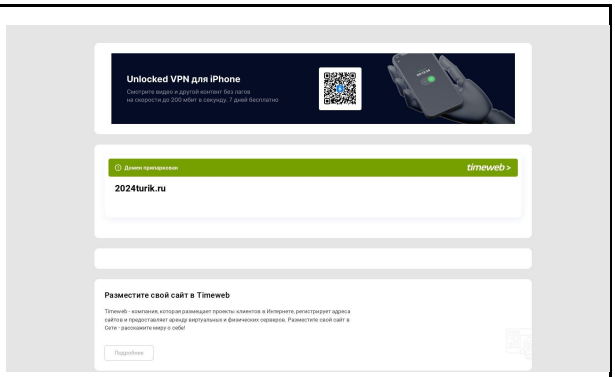
それらのIPアドレスは、2つをホストしていたDARL-TELECOMを筆頭に、6つのISPに分散していました。残りの5つのIPアドレスは、Hosting Technology Ltd.、TimeWeb Ltd.、BL Networks GB、Hostinger US、Hetzner Online GmbHに管理されていました。

次に、10個のIPアドレス（IoCとして特定された3個と追加で見つかった7個）をreverse IP lookupsで検索しました。その結果441個のドメイン名が検出され、そのうち10個は悪意あるドメイン名でした。

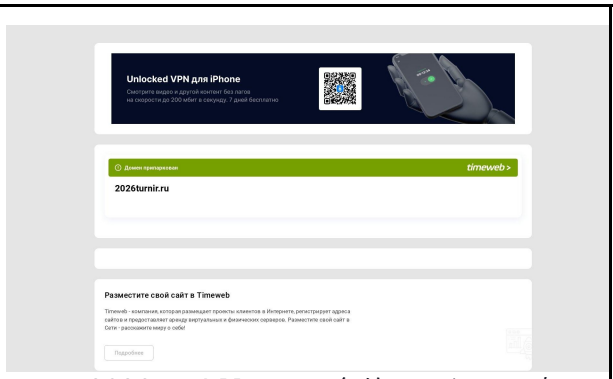
悪意あるページをScreenshot lookups にかけたところ、5つはアクセス可能でした。興味深いことにそれらのコンテンツは同一で、VPNソフトウェアのダウンロードページのようでした。



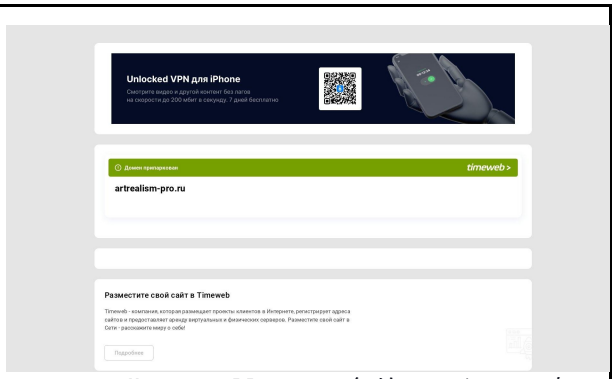
2022turik[.]ruのスクリーンショット



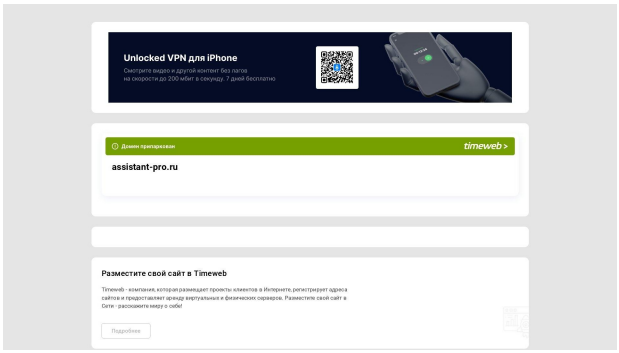
2024turik[.]ruのスクリーンショット



2026turnir[.]ruのスクリーンショット



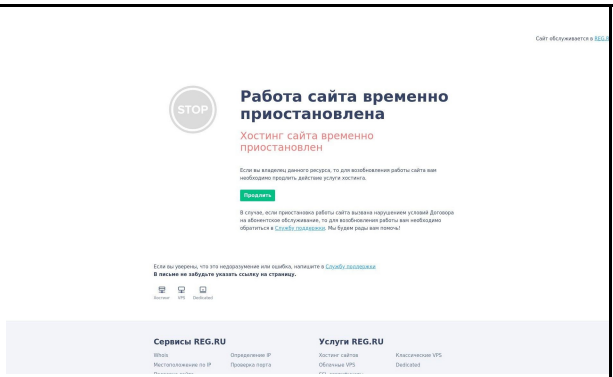
artrealism-pro[.]ruのスクリーンショット



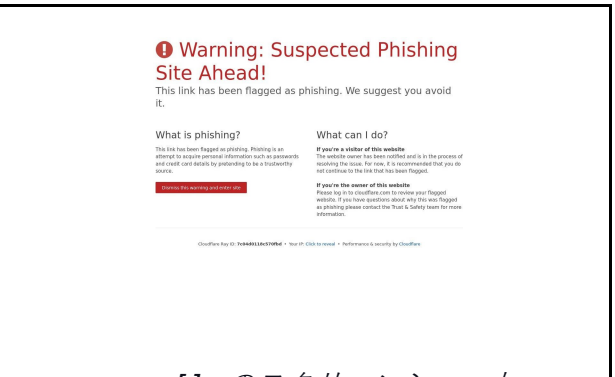
assistant-pro[.]ruのスクリーンショット

脅威アクターが偽のVPNソフトウェアを使用することから、OpcJackerと同様の攻撃に利用されるかもしれない***vpn***という文字列を含むドメイン名も調査しました。Domains & Subdomains Discoveryで検索した結果、10,000個のドメイン名が見つかりました。そのうち12個は悪意あるドメイン名と確認されました。12個のうち9個はマルウェアホストで、残りの3個はスパムに関与したものでした。

悪意あるドメイン名のうち10個は、本稿執筆時点で到達不能でした。あと2つは依然としてアクセス可能で、警告のページに到達しました。



1vpns[.]ruのスクリーンショット



vpnm[.]ruのスクリーンショット

次に、このページから VPNサービスプロバイダーのリストを入手しました。プロバイダーの公式ドメイン名を一括してWHOIS検索したところ、公開情報から登録者組織を特定できたものは10個しかありませんでした。 それらを***vpn***を含むドメイン名の登録者組織と照らし合わせた結果、リストにある正規のVPNサービスプロバイダーに属していることが確認できたドメイン名は、vpn[.]ac だけでした。このドメイン名は実際、VPN.acというルーマニアのVPNサービスプロバイダーの公式なサイトアドレスでした。共通の文字列を含む残りの9,999個のドメイン名は、偽のVPNソフトウェアのインストールページに使われている可能性があります。

—

当社が行ったIoCリスト拡張により、OpcJackerのインフラの一部かもしれない10の偽VPNダウンロードページを発見できました。それらは一部のIoCと同じIPアドレスを使っていました。また、***vpn***という文字列を含む他の12個のドメインも見つかりました。これらはすでに同様の悪意あるキャンペーンに関与した可能性があります。

同様の調査をご希望のお客様、または本調査のデーター式をご希望のお客様は、こちらまでお気軽にお問い合わせください。

付録：アーティファクトとIoCの例

IoCとして特定されたドメイン名をホストしていたIPアドレスの例

- 176[.]124[.]216[.]31
- 37[.]1[.]211[.]16
- 92[.]53[.]118[.]39
- 45[.]61[.]138[.]73

悪意あるIPホストの例

- 176[.]124[.]216[.]31
- 92[.]53[.]118[.]39

一部のIoCのIPホストを共用していたドメイン名の例

- a-sharik[.]ru
- a1trashandjunkoflincoln[.]com
- aa[.]best-prices-today[.]site
- aatt45[.]ru
- ab-pereplanirovka[.]ru
- abcdesigngroup[.]com
- academy51[.]ru
- acc[.]nbgiba[.]site
- acc[.]noticias-hoy1[.]site
- accex[.]ru
- acro[.]su
- acw-2022[.]tw1[.]ru
- ad-foru[.]ru
- ad[.]air-appvela[.]site
- ad[.]best-prices-today[.]site
- ad[.]good-prices-for[.]site
- adaptivvrn[.]ru
- adelante[.]ru
- adfplata[.]ru
- adi-avadhuta[.]ru

- adihic[.]com
- adihic[.]ru
- adkstudio[.]ru
- adrialux[.]ru
- ads-kindile[.]site
- ads[.]air-appvela[.]site
- ads[.]best-prices-today[.]site
- ads[.]good-prices-for[.]site
- ads[.]noticias-hoy1[.]site
- advf1[.]ru
- advocat-lukyanov[.]ru
- advocativanova[.]ru
- advokatburnaev[.]com
- advokatsterlitamak[.]ru
- advsphere[.]ru
- adygeya-yurist-konsultaciya[.]ru
- aerocosmos[.]su
- afalina-tour[.]ru
- africainhermitage[.]ru
- agency-1[.]ru
- agid[.]su
- agonist[.]studio
- agro-star[.]net
- agrogradt[.]com
- agvilon[.]ru
- aicutting[.]com
- aider-halil[.]ru
- aif-profi[.]ru
- aigeos[.]ru
- aimara-mara[.]ru

共通のIPアドレスを共用していた悪意あるドメイン名の例

- 2022turik[.]ru
- 2024turik[.]ru
- 2024turik[.]site
- 2026turnir[.]ru
- 2026turnir[.]site
- 2027turnir[.]site

*vpn*という文字列を含むドメイン名の例

- vpnvpnvpnvpnvpnvpnvpn[.]tk
- vpnvpnvpnvpn[.]tk
- vpnvpnvpn[.]cf
- vpnvpnvpn[.]ru
- vpnvpnvpn[.]tk
- vpnvpnvpn[.]com
- vpnvpnvpn[.]top
- vpnvpnvpn[.]xyz
- vpn-vpn-vpn[.]ml
- vpnvpn[.]us
- vpnvpn[.]tw
- vpnvpn[.]cn
- vpn-vpn-vpn[.]com
- vpnvpn[.]ml
- vpnvpn[.]de
- vpnvpn[.]tk
- vpnvpn[.]ru
- vpn-vpn-vpn[.]top
- vpnvpn[.]kr
- vpnvpn[.]me
- vpnvpn[.]co
- vpnvpn[.]ga
- vpnvpn[.]cc
- vpnvpnvpnllc[.]com
- vpnovpn[.]tk
- vpnvpn[.]vip
- vpn-vpn[.]ru
- vpn1vpn[.]tk
- vpnvpn[.]xyz
- vpn-vpn[.]cn
- vpnvpn[.]com
- vpnbvpn[.]tk
- vpnvpn[.]xin
- vpn-vpn[.]tk

- vpnvpn[.]top
- vpn2vpn[.]tk
- bvpnvpn[.]ml
- vpn4vpn[.]tk
- vpnvpn[.]app
- vpnvpn[.]org
- vpnivpn[.]tk
- vpnvpn[.]net
- vpn-vpn[.]ml
- vpnfcvpn[.]in
- vpnvpnf[.]icu
- vpnlvpn[.]com
- vpn-vpn[.]com
- ovpnovpn[.]pw
- vpn-vpns[.]tk
- 88vpnvpn[.]cn
- vpn4vpn[.]com
- vpn2vpn[.]top
- hdvpnvpn[.]cc
- vpnvpn[.]mobi
- vpnvpn[.]info
- vpnxvpn[.]com
- vpn-vpnn[.]tk
- vpnvpn[.]work
- 91vpnvpn[.]cn
- vpnfcvpn[.]pw
- vpn3vpn[.]com
- vpnvpn2[.]xyz
- vpn2vpn[.]com
- vpn1vpn[.]com
- vpnvpn[.]site
- vpnvpn[.]live
- vpnvpn[.]club
- vpn7vpn7[.]tk
- vpnvpn1[.]com
- vpnvpns[.]com
- upspeedvpnvpnvpn[.]tk
- upspeedvpnvpnvpn[.]ml
- esvpnvpn[.]com
- 91vpnvpn[.]ltd
- vpnvpn[.]co[.]kr
- vpnvpnnv[.]top
- vpnvpnas[.]com
- vpn2vpn1[.]top
- vpntvvpn[.]com
- fcvpnsvpn[.]pw
- vpnvsvpn[.]com
- 91vpnvpn[.]com
- vpnasvpn[.]com
- vpnvpn[.]gives
- vpntvvpn[.]org
- vpnvpn[.]store
- vpnvpn[.]pe[.]kr
- 88vpnvpn[.]com
- bsvpnvpn[.]com
- vpn2vpn[.]info
- vpnvpncn[.]com
- vpntovpn[.]top
- 56vpnvpn[.]com
- vpntovpn[.]com
- vpn2vpn2[.]top
- vpn-xvpn[.]com
- vpn0vpn[.]site
- vpnvpn[.]online
- vpnforvpn[.]com
- gocvpnvpn[.]com
- mymjvpnvpn[.]tk
- vpnas-vpn[.]org
- vpnvpn[.]com[.]ph
- vpntvvpn[.]info
- purevpnvpn[.]co
- vpntorvpn[.]com
- vpnnordvpn[.]ru
- vpn12vpn[.]buzz
- vpnforvpn[.]xyz
- vpnovervpn[.]com
- vpnbestvpn[.]net
- vpnforvpn[.]shop
- vpnbestvpn[.]com
- vpnfreevpn[.]org

- vpnfreevpn[.]com
- vpn2019vpn[.]net
- vpnfreevpn[.]net
- vpn2019vpn[.]com
- freevpnvpn[.]com
- openvpnvpn[.]net
- vpnistavpn[.]xyz
- vpniranvpn[.]com
- vpn-xfxvpn[.]com
- vpnforvpn[.]site
- vpnbestvpn[.]top
- nordvpnvpn[.]com
- vpnlivevpn[.]com
- vpnchinavpn[.]com
- vpnnordvpn[.]zone
- vpnforvpn[.]store
- vpnroom1-vpn[.]ga
- vpnovpn[.]website
- vpnkoreavpn[.]com
- beibeivpnvpn[.]cn
- fcvpn-fcvpn[.]top
- vpnroom1-vpn[.]gq
- vpn[.]ng
- vpn[.]st
- vpn[.]gr
- vpn[.]sn
- vpn[.]ug
- vpn[.]xn--czr694b
- vpn[.]si
- vpn[.]ua
- vpn[.]ge
- vpn[.]to
- vpn[.]id
- vpn[.]fi
- vpn[.]se
- vpn[.]nu
- vpn[.]by
- tomvpn-vpn-7[.]fm
- vpn[.]ai
- vpn[.]me
- vpn[.]vn
- vpn[.]no
- vpn[.]xn--kprw13d
- vpn[.]ms
- vpn[.]fm
- vpn[.]kz
- vpn[.]gl
- vpn[.]pe
- vpn[.]bi
- vpn[.]cc
- vpn[.]sy
- vpn[.]at
- vpn[.]in
- vpn[.]xn--3ds443g
- vpn[.]sg
- vpn[.]bz
- vpn[.]sh
- vpn[.]uy
- vpn[.]ph
- vpn[.]pw
- vpn[.]is
- vpn[.]ke
- vpn[.]cm
- vpn[.]xn--6frz82g
- vpn[.]su
- vpn[.]cl
- vpn[.]cz
- vpn[.]tt
- vpn[.]tn
- vpn[.]ma
- vpn[.]im
- vpn[.]pt
- vpn[.]rs
- vpn[.]ie
- vpn[.]lc
- vpn[.]nz
- vpn[.]tf
- vpn[.]ro
- vpn[.]ca
- vpn[.]so

- vpn[.]hn
- vpn[.]sk
- vpn[.]mx
- vpn[.]mn
- vpn[.]kr
- vpn[.]es
- vpn[.]pl
- vpn-xvpn[.]online
- huajunvpnvpn[.]cn
- vpn[.]xn--55qx5d
- vpn[.]pm
- vpn[.]tv
- vpn[.]bh
- vpn[.]nl
- vpn[.]de
- vpn[.]mg
- vpn[.]cn
- vpn[.]xn--io0a7i
- vpn[.]sb
- vpn[.]ws
- vpn[.]tw
- vpn[.]ru
- vpnyourvpn[.]club
- vpn[.]tj
- vpn[.]uz
- vpn[.]sr
- vpn[.]tk
- vpn[.]am
- vpn[.]lt
- vpn[.]md
- vpn[.]gg
- vpn[.]vg
- vpn[.]lk
- vpn[.]la
- vpn[.]jp
- vpn[.]eu
- vpn[.]fo
- vpn[.]je
- vpn[.]hr
- vpn[.]mk
- vpn[.]ee
- vpn[.]vc
- vpn[.]ba
- vpn[.]gw
- vpn[.]hk
- vpn[.]xn--qxam
- vpn[.]cy
- vpn[.]us
- vpnopenvpn[.]zone
- vpnroom1-vpn[.]ml
- vpnroom1-vpn[.]tk
- nordvpn-vpn[.]com
- vpn[.]vu
- vpn[.]ci
- vpn[.]ir
- vpn[.]co
- vpn[.]dk
- vpn[.]ch
- vpn[.]fr
- vpn[.]ac
- vpn[.]tl
- vpn[.]ae
- vpn[.]et
- vpn[.]be
- vpn[.]io
- vpn[.]wf
- vpn[.]uk
- vpn[.]af
- vpn[.]tc
- vpn[.]lv
- vpn[.]it
- vpn[.]gy
- vpn[.]my
- vpn[.]ao
- vpn[.]sc
- xn--vp-0ja[.]se
- vpn[.]cx
- vpn[.]gs
- vpn[.]ht
- vpn[.]gd

- vpn[.]bg
- vpn[.]al
- vpnouvpn[.]website
- vpnformacvpn[.]com
- vpniovpn[.]website
- vpnreviewvpn[.]net
- norordvpnvpn[.]com
- vpnreviewvpn[.]com
- huajunvpnvpn[.]com
- freevpnbyvpn[.]org
- fcvpn-fcvpn1[.]top
- vpnversusvpn[.]com
- vpnserversvpn[.]tk
- fcvpn-fcvpn2[.]top
- vpnforvpn[.]online
- vpnoivvpn[.]website
- vpnthebestvpn[.]com
- vpnnetflixvpn[.]com
- vpnoiovpn[.]website
- nordvpnopenvpn[.]ga
- vpncandelavpn[.]com
- expressvpnvpn[.]com
- speedvpntovpns[.]tk
- vpn2[.]co
- dvpn[.]pw
- qvpn[.]tk
- vpnu[.]in
- tvpn[.]in
- vpno[.]cc
- mvpn[.]pl
- vvpn[.]pl
- dvpn[.]ch
- ovpn[.]tw
- vpn[.]fan
- yvpn[.]tk
- vpne[.]tk
- vpn[.]nrw
- pvpn[.]kr
- vpn[.]app
- vpnx[.]io
- vpny[.]cc
- ovpn[.]gr
- mvpn[.]kr
- rvpn[.]ga
- xvpn[.]in
- vpnz[.]ru
- vpn[.]gdn
- ovpn[.]co
- rvpn[.]ml
- zvpn[.]cf
- vpnc[.]eu
- vpnx[.]ru
- cvpn[.]me
- vpng[.]fr
- mvpn[.]cf
- vpns[.]it
- rvpn[.]me
- 2vpn[.]tk
- vpn[.]how
- cvpn[.]ga
- jvpn[.]xn--node
- ovpn[.]nl
- ovpn[.]cn
- cvpn[.]ph
- vpnw[.]de
- avpn[.]ml
- 3vpn[.]vg
- vpnp[.]es
- vpns[.]us
- vpn[.]srl
- dvpn[.]ws
- hvpn[.]uk
- tvpn[.]pl
- dvpn[.]ru
- vpn4[.]cn
- mvpn[.]cn
- mvpn[.]ru
- mvpn[.]nl
- dvpn[.]ir
- ivpn[.]tw

- ovpn[.]im
- vvpn[.]cc
- fvpn[.]gq
- lvpn[.]tk
- vpnf[.]cf
- uvpn[.]in
- vpnt[.]pl
- nvpn[.]kr
- ivpn[.]fi
- vpnz[.]tk
- zvpn[.]pl
- ivpn[.]cn
- vpnf[.]ga
- ovpn[.]cz
- ivpn[.]me
- evpn[.]ga
- uvpn[.]es
- vpn[.]ski
- xvpn[.]ca
- bvpn[.]io
- vpn[.]pub
- ovpn[.]sx
- vpno[.]de
- zvpn[.]us
- vpnc[.]ru
- xvpn[.]us
- vpnh[.]cn
- 8vpn[.]cc
- vpn[.]sbs
- ovpn[.]es
- dvpn[.]io
- vpnd[.]cn
- vpnd[.]gq
- vpnn[.]ws
- gvpn[.]ru
- 1vpn[.]pl
- vpn1[.]cc
- vpn[.]tax
- vpns[.]tv
- svpn[.]eu
- kvpn[.]de
- tvpn[.]vg
- vpnu[.]nl
- vpn2[.]nl
- vpn2[.]ga
- svpn[.]us
- 8vpn[.]ru
- vpn[.]dtt
- vpnu[.]us
- vpnn[.]tk
- mvpn[.]eu
- vpn2[.]eu
- vpnv[.]cc
- zvpn[.]tw
- bvpn[.]cf
- mvpn[.]se
- vpnz[.]io
- kvpn[.]se
- lvpn[.]uk
- vpnl[.]pw
- vpns[.]ws
- uvpn[.]tk
- vpny[.]cf
- vpnx[.]ir
- wvpn[.]eu
- evpn[.]cn
- 1vpn[.]ga
- 9vpn[.]co
- tvpn[.]pw
- hvpn[.]de
- ivpn[.]ca
- xvpn[.]cc
- uvpn[.]io
- vpnm[.]ru
- bvpn[.]co
- nvpn[.]cc
- tvpn[.]ru
- ovpn[.]uk
- hvpn[.]me
- mvpn[.]it

- ovpn[.]to
- jvpn[.]me
- vpn2[.]cz
- vpng[.]io
- vpnc[.]cn
- vpnc[.]de
- vpns[.]ca
- vpn6[.]cn
- uvpn[.]de
- vpn[.]win
- vpnb[.]de
- 1vpn[.]us
- vpnn[.]ga
- vpng[.]us
- vpnz[.]us
- vpn[.]bid
- vpnm[.]cf
- uvpn[.]us
- zvpn[.]cn
- 2vpn[.]cn
- vpne[.]se
- nvpn[.]se
- lvpn[.]us
- vpnf[.]tk
- vpns[.]su
- vpnm[.]ml
- mvpn[.]pw
- qvpn[.]me
- 7vpn[.]kr
- ovpn[.]tk
- vpnz[.]vg
- vvpn[.]uk
- vpn8[.]cf
- evpn[.]ru
- evpn[.]us
- vpnr[.]cn
- avpn[.]io
- mvpn[.]ga
- 0vpn[.]ga
- vpn[.]mom
- kvpn[.]kr
- hvpn[.]tk
- uvpn[.]ru
- vpns[.]pw
- vpne[.]ws
- fvpn[.]ga
- ivpn[.]co
- vpnb[.]xn--fiqz9s
- qvpn[.]vg
- vpns[.]fr
- 4vpn[.]de
- vpns[.]nl
- vpnd[.]io
- vpnl[.]cc
- vpny[.]cn
- xvpn[.]gq
- evpn[.]eu
- vpn[.]run
- 0vpn[.]xn--fiqz9s
- 1vpn[.]io
- gvpn[.]us
- vpnx[.]nl
- vpn[.]bio
- ivpn[.]de
- xvpn[.]cn
- svpn[.]ru

共通の文字列を含む悪意あるドメイン名の例

- vpnvpn[.]me
- vpnm[.]ru
- gvpn[.]us
- vpn[.]lol
- advpn[.]tk
- 1vpns[.]ru