A DNS Deep Dive: That VPN Service May Be OpcJacker in Disguise

Table of Contents

Executive Report

The more dangerous browsing the Internet becomes, the more tools to address cyber threats emerge in the market. Virtual private network (VPN) service usage, for instance, gained ubiquity due to the ever-increasing number of data privacy intrusions. So what happens when you download a supposed VPN software installer but end up with a malware infection instead?

Trend Micro's in-depth OpcJacker investigation may tell you. The malware comes in the guise of a VPN software installer. When installed, it logs user keystrokes, takes screenshots, steals sensitive browser data, loads additional malicious modules, and replaces cryptocurrency wallet IDs for hijacking purposes.

Security researchers Jaromir Horejsi and Joseph C. Chen identified 33 OpcJacker indicators of compromise (IoCs)—30 domains and three IP addresses, namely:

DOMAINS	IP ADDRESSES
• 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

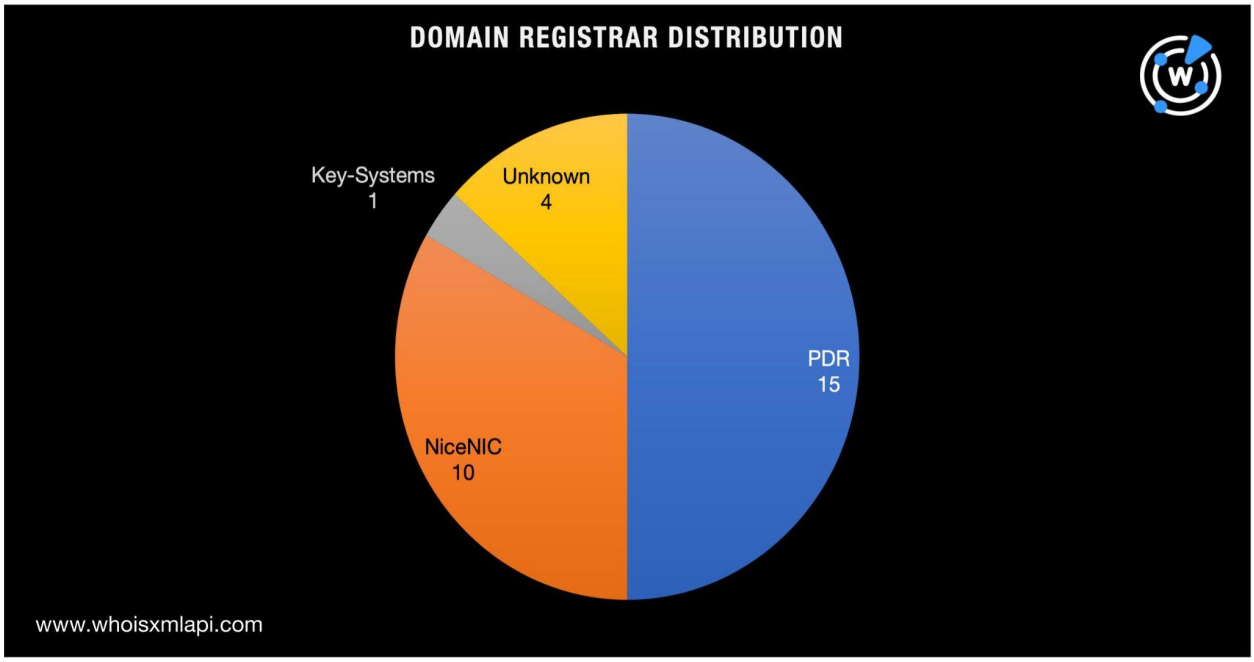
• irhxvpn[.]site • irixvpn[.]site • irkxvpn[.]site • irqxvpn[.]site • irtxvpn[.]site • iruxvpn[.]site • irwxvpn[.]site • manigiajabae32[.]com • manigiajabae35[.]com • neskrab1[.]com • neskrab2[.]com • nesupcli[.]com • she32rn1[.]com • she32rn2[.]com • uhcoxvpn[.]site • uzurtela1[.]com • uzurtela42[.]com	

The WhoisXML API research team expanded the list of IoCs to determine other potential fake VPN threat vectors. Our closer look at the DNS uncovered:

- Seven additional IP addresses that played host to some of the domains identified as IoCs, three of which turned out to be malicious
- 441 additional domains that shared some of the IoCs' IP hosts, 10 of which turned out to be malware hosts
- 10,000 domains that contained the string ***vpn***, 12 of which have been dubbed malicious

Facts about the OpcJacker IoCs

We began our in-depth study with a bulk WHOIS lookup for the 30 domains identified as IoCs. Twenty-six of the domains' registrars were publicly visible. They were spread across three registrars—15 with PDR Ltd., 10 with NiceNIC International Group Co. Limited, and one with Key-Systems GmbH.



All 30 domains were newly registered, specifically just this February. They were also registered in a single country—Russia.

A bulk IP geolocation lookup, meanwhile, for the three IP addresses showed they were geolocated in three distinct countries—Moldova, the U.S., and the Netherlands. Two of them were managed by MivoCloud SRL while the remaining was under BL Networks.

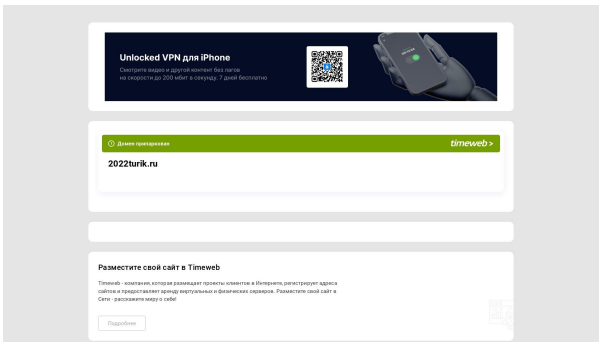
OpcJacker IoC List Expansion Findings

To find all other potentially connected artifacts, we subjected the domains identified as IoCs to DNS lookups. That led to the discovery of seven additional IP addresses spread across five countries. Three were geolocated in the U.S. and one each in Germany, the Netherlands, Russia, and the U.K.

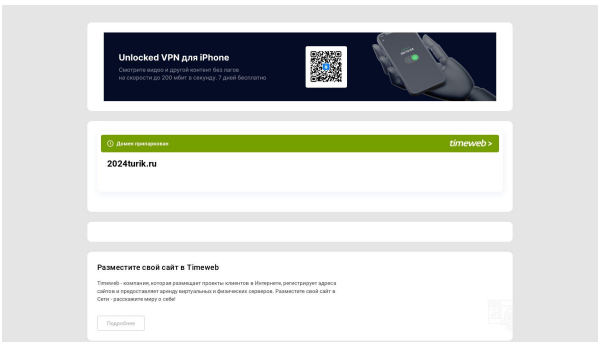
The IP addresses were distributed among six ISPs led by DARL-TELECOM, which accounted for two of the hosts. The remaining five IP addresses were managed by Hosting Technology Ltd., TimeWeb Ltd., BL Networks GB, Hostinger US, and Hetzner Online GmbH.

Next, reverse IP lookups for the 10 IP addresses—three identified as IoCs and seven additional hosts—allowed us to uncover 441 domains, 10 of which turned out to be malicious.

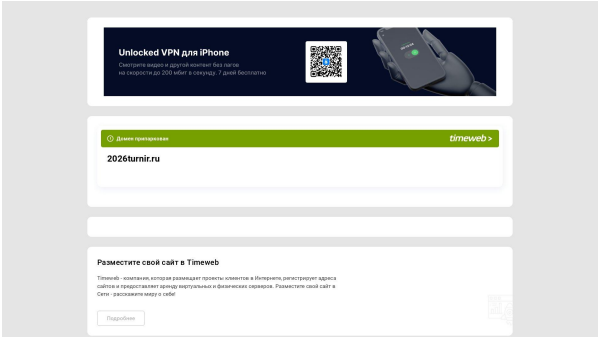
Screenshot lookups for the malicious pages showed that five remained accessible. What was, however, more interesting was that they had the same content, a supposed VPN software download page.



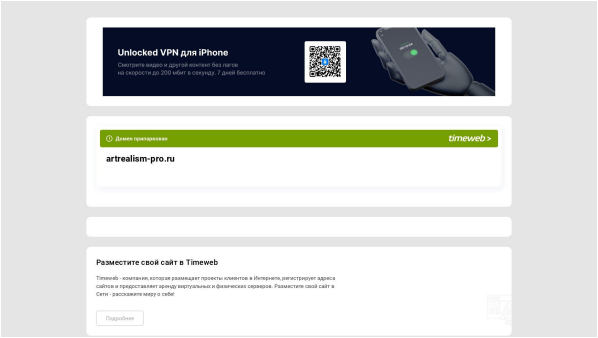
Screenshot of 2022turik[.]ru



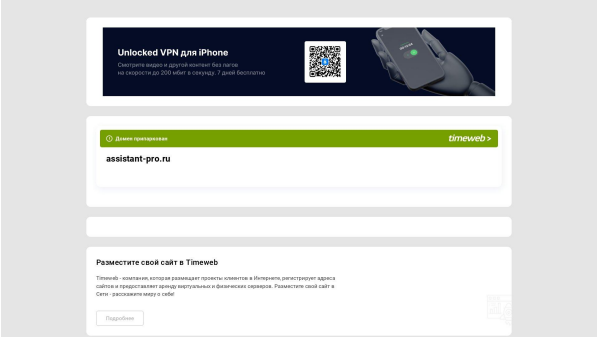
Screenshot of 2024turik[.]ru



Screenshot of 2026turnir[.]ru



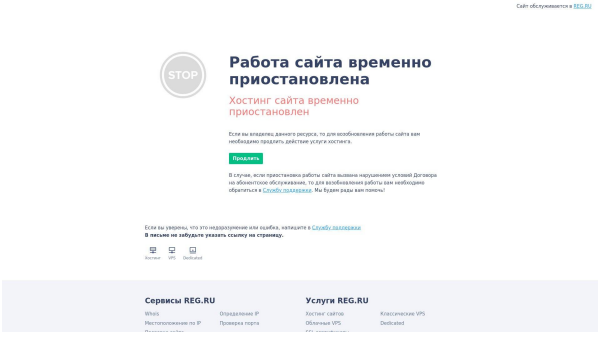
Screenshot of artrealism-pro[.]ru



Screenshot of assistant-pro[.]ru

Due to the threat actors' use of fake VPN software, we also scoured the DNS for domains that contained the string ***vpn***, which could be utilized maliciously for attacks similar to the OpcJacker campaign. Domains & Subdomains Discovery gave us 10,000 domain names, 12 of which turned out to be malicious. Specifically, nine of them were malware hosts while the remaining three were involved in spamming.

A majority of the malicious domains (10 to be exact) were unreachable as of this writing. The other two, which remained accessible, meanwhile, led to warning pages.



Screenshot of 1vpns[.]ru

Screenshot of vpnm[.]ru

Next, we obtained a list of VPN service providers from this page. A bulk WHOIS lookup for their official domains showed that only 10 had publicly viewable registrant organizations. Comparing them with the registrant organizations of the ***vpn***-containing domains revealed that only one—vpn[.]ac—could be publicly attributed to the legitimate VPN service providers on our list. It is, in fact, Romania-based VPN service provider VPN.ac's official site address. The remaining 9,999 string-connected domains could serve as hosts to fake VPN software installer pages.

—

Our IoC list expansion analysis led to the discovery of 10 fake VPN download pages that could be part of the OpcJacker infrastructure since they shared some of the IoCs' IP hosts. It also uncovered 12 other domains that contained the string ***vpn***, which may have already figured in similar malicious campaigns.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample IP Addresses That Played Host to the Domains Identified as IoCs

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

Sample Malicious IP Hosts

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

Sample Domains That Shared Some of the IoCs' IP Hosts

- 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

Sample Malicious IP-Connected Domains

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

Sample Domains That Contained the String *vpn*

- 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

Sample Malicious String-Connected Domains

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