Decoy Dog, Too Sly to Leave DNS Traces?

Table of Contents

Executive Report

Decoy Dog, a malware renowned for abusing the DNS, specifically by establishing command and control (C&C) via DNS queries, first reared its head most likely in early 2022. Given its sly nature, the DNS malware has been used to successfully steal data from organizations throughout Russia and other Eastern European nations.

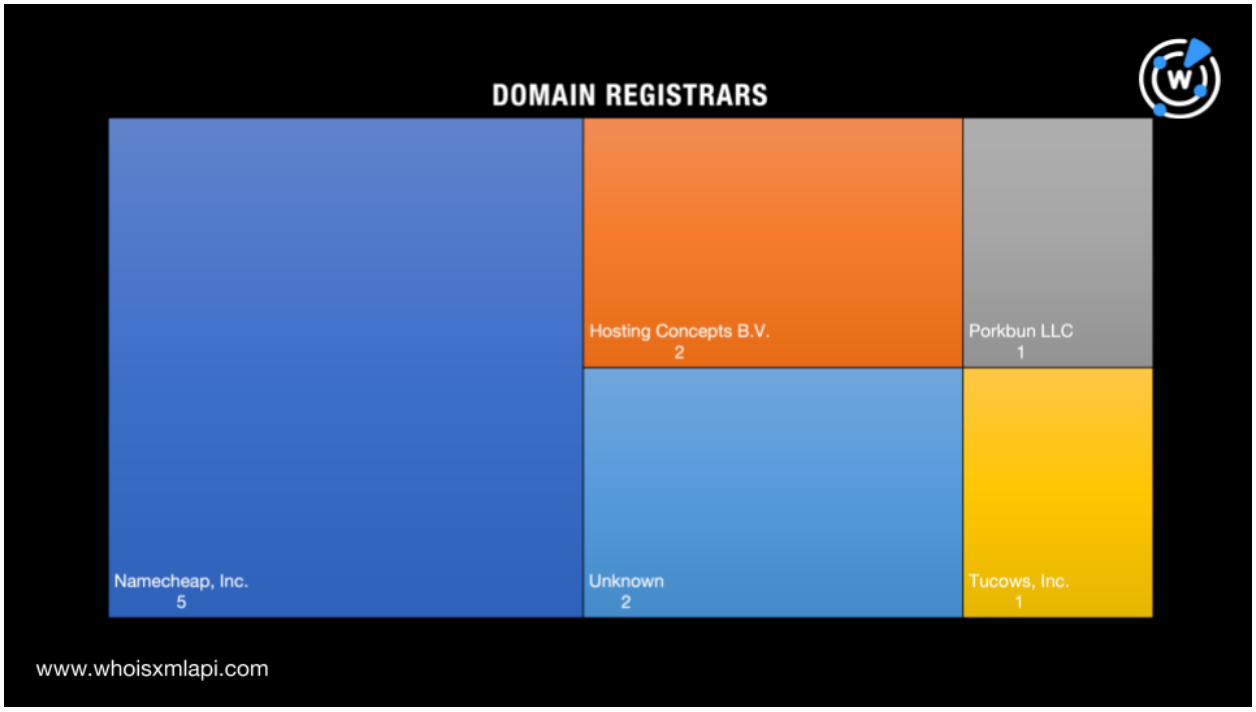
Infoblox published its in-depth analysis of the Decoy Dog infrastructure in April 2023, revealing 23 indicators of compromise (IoCs) comprising 11 domains and 12 IP addresses. To identify currently unidentified potential Decoy Dog threat vectors, WhoisXML API used the 23 IoCs as jump-off points for a DNS deep dive that led to the discovery of:

- Two IP address resolutions not on the Infoblox list that turned out to be malicious based on malware checks
- 90 domains hosted on five dedicated IP addresses identified as IoCs, four of which have been categorized as malicious by a bulk malware check
- 2,295 domains containing the strings **cbox4**, **ignorelist**, **claudfront**, **allowlisted**, **maxpatrol**, **atlas + upd**, **hsps**, **nsdps**, **ads + tm + glb**, and **hsdps** akin to 10 of the domains identified as IoCs, five of which turned out to be malware hosts based on a bulk malware check

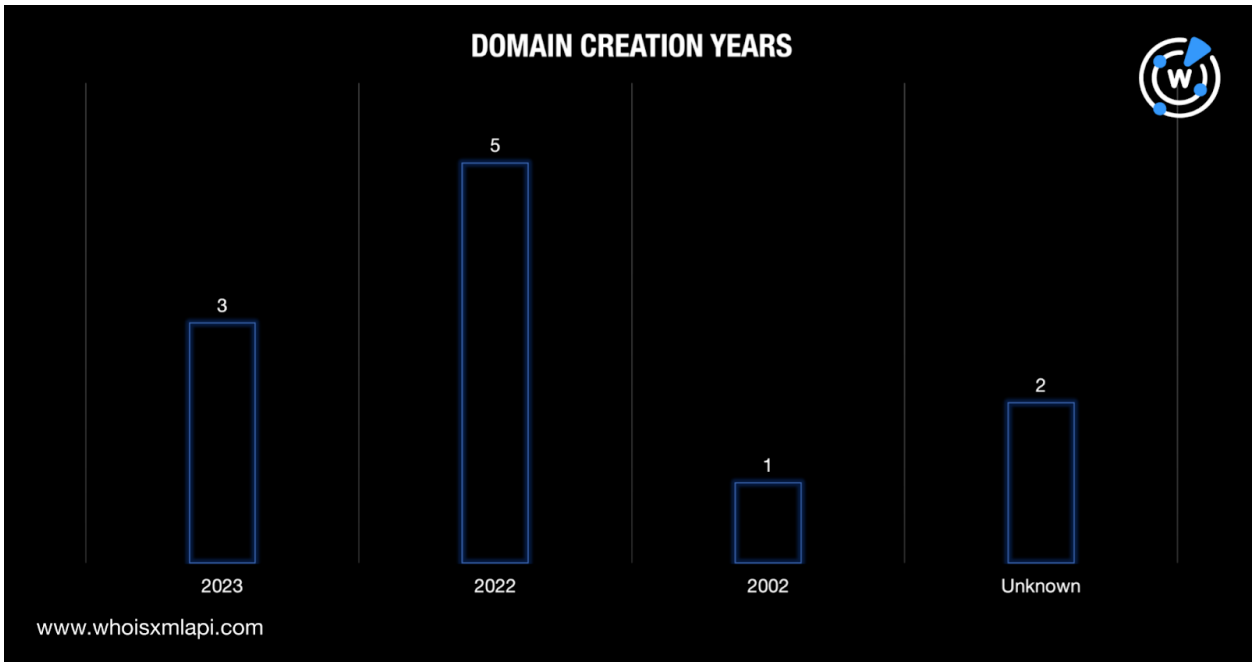
Tracing Decoy Dog's DNS Roots

As our first step, we subjected the 11 domains identified as IoCs to a bulk WHOIS lookup. Note that two of the IoCs—hsps[.]cc and rcmsf100[.]net—didn't have active WHOIS records. We listed our findings for the nine remaining domains on our list.

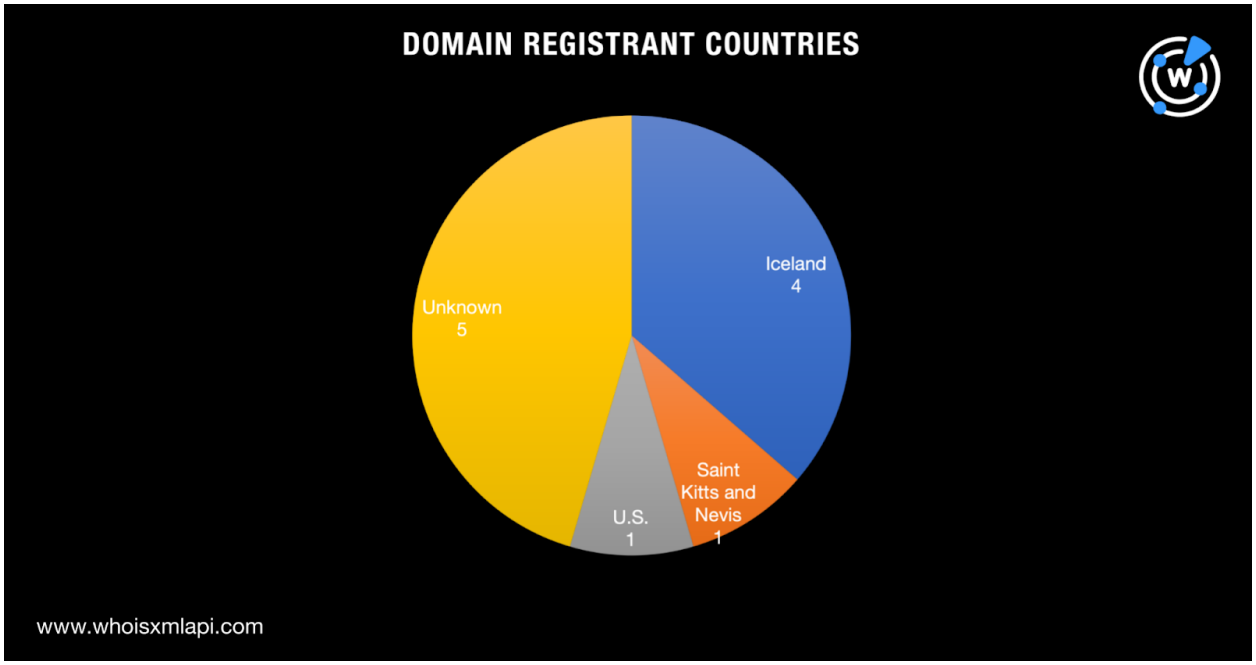
- More than half of the IoCs (five out of nine) were registered under Namecheap, Inc. The remaining four domains were spread across three other registrars—Hosting Concepts B.V. (two domains) and Porkbun LLC and Tucows, Inc. (one domain each).



- Five of the domains were created in 2022. They were probably used in the first Decoy Dog attacks. Three of the IoCs were created just this year, which could hint at forthcoming attacks. It's also interesting to note that one of the domains was aged—created way back in 2002.

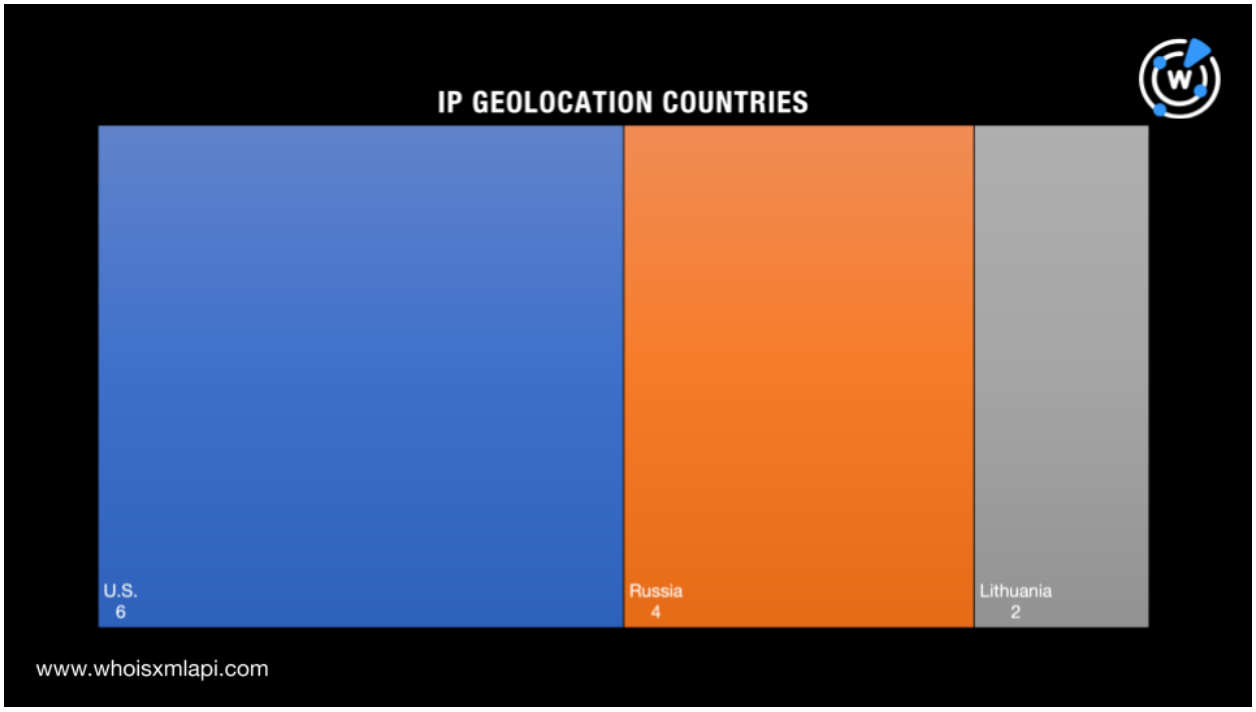


- Six of the IoCs were registered across three countries—four in Iceland and one each in Saint Kitts and Nevis and the U.S. Apart from hsps[.]cc and rcmsf100[.]net that we noted earlier for not having active WHOIS records, the owners of the three other domains—hsdps[.]cc, j2update[.]cc, and nsdps[.]cc—had redacted countries.

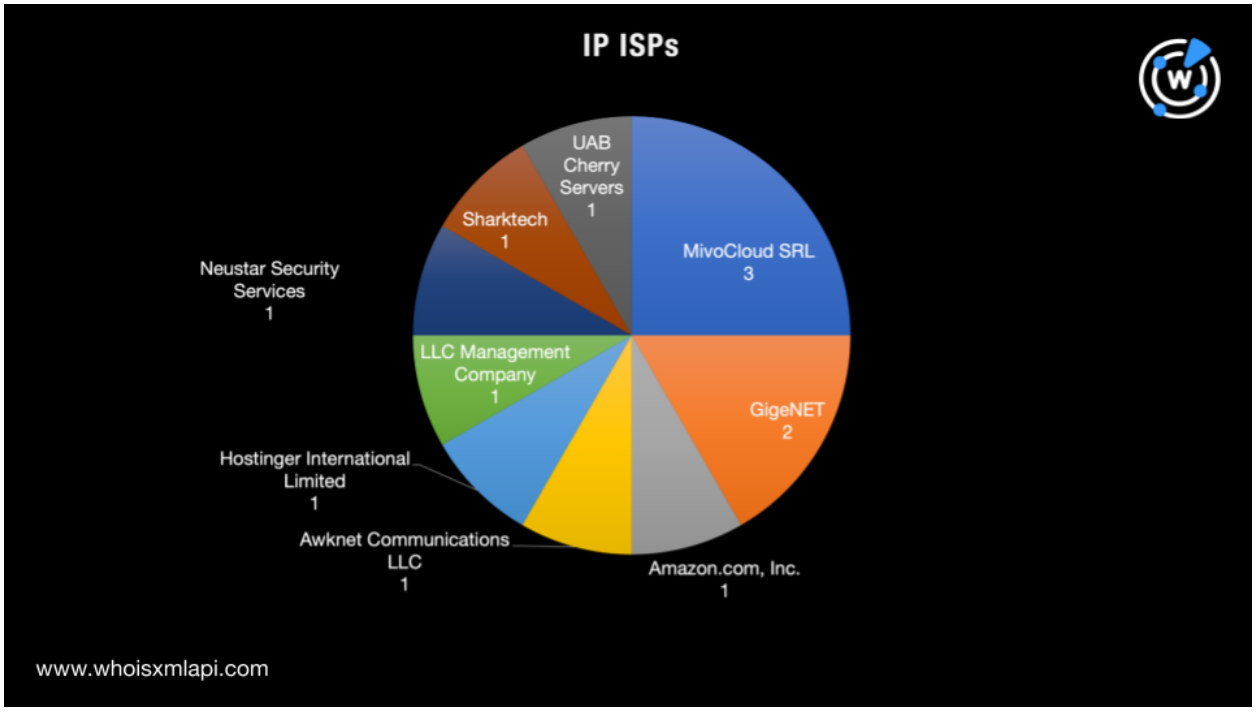


Next, a bulk IP geolocation lookup for the 12 IP addresses identified as IoCs showed that:

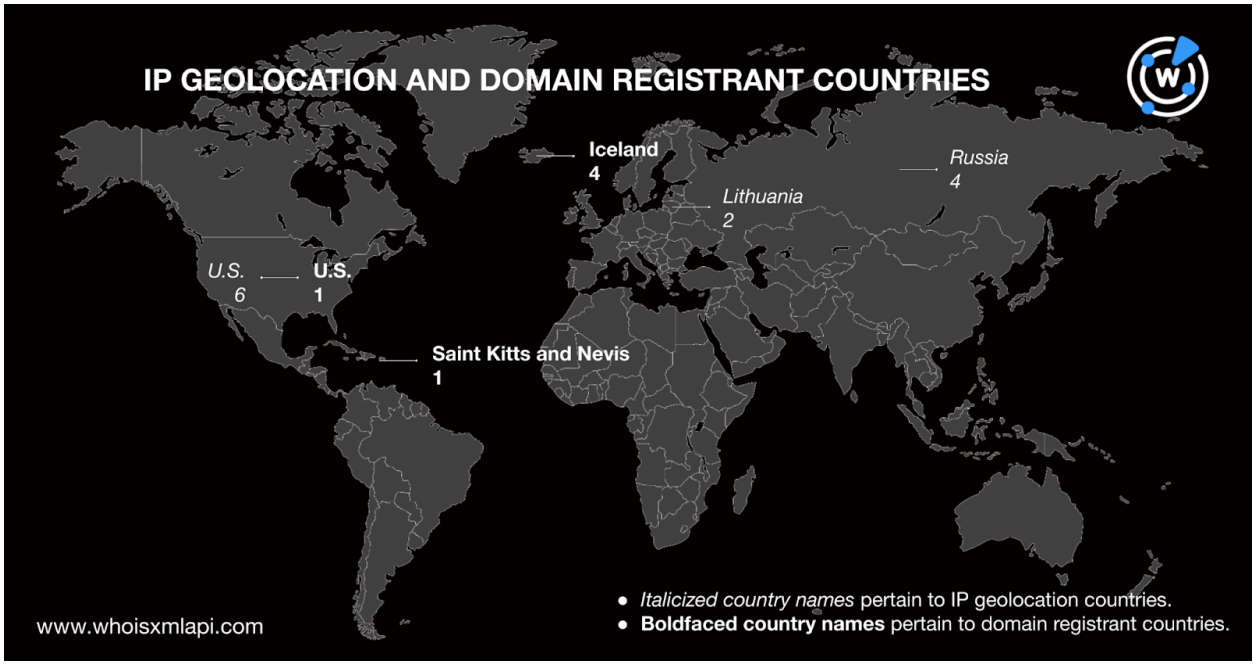
- The IP addresses originated from three countries led by the U.S. (six IP addresses). Russia accounted for four of the IoCs and Lithuania for the remaining two.



- The IP addresses were scattered across nine Internet service providers (ISPs) led by MivoCloud SRL, which accounted for three of the IoCs. GigeNET with two IP addresses took second place.



Interestingly, a comparison of the registrant and IP geolocation countries revealed that the IoCs only had the U.S. in common.



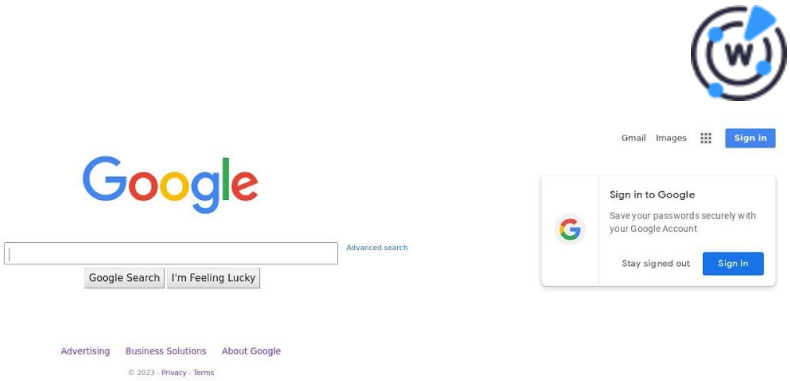
Identifying Potential Decoy Dog Attack Vectors

To determine if the domains identified as IoCs resolved to IP addresses that weren't part of the Infoblox list yet, we subjected them to DNS lookups, which led to the discovery of two web properties—192[.]64[.]119[.]51 and 15[.]197[.]130[.]221 that turned out to be malicious according to malware checks.

IP geolocation lookups for the two IP addresses further revealed they hailed from the U.S., similar to six of the IoCs. One of them—15[.]197[.]130[.]221—was administered by Amazon.com, Inc. like the IoC 13[.]248[.]169[.]48.

We then performed reverse IP lookups for the 14 IP addresses in total—12 from the Infoblox IoC list and the two we obtained from our DNS lookups earlier. We found that five of them were dedicated, altogether hosting 90 unique domains. A bulk malware check revealed that four of the IP-connected domains were classified as malicious.

Two of the four malicious IP-connected domains—darknode[.]net and settepani[.]net—continued to point to live content. Darknode[.]net proved noteworthy in that it redirected to a Google search page.



Screenshot of darknode[.]net (redirecting to google[.]com)

A bulk WHOIS lookup for the IP-connected domains allowed us to see some similarities between them and the IoCs as well, including:

- 35 domains shared the IoCs' four registrars—30 for Namecheap, Inc.; three for Porkbun LLC; and one each for Hosting Concepts B.V. and Tucows, Inc.
- 34 connected domains shared two of the IoCs' creation years—16 for 2023 and eight for 2022
- 53 IP-connected domains shared two of the IoCs' registrant countries—29 for Iceland and 24 for the U.S.

A closer look at the domains identified as IoCs allowed us to identify these 10 strings that appeared in 2,295 other possibly connected artifacts based on Domains & Subdomains Discovery searches:

- **cbox4**
- **ignorelist**
- **claudfront**
- **allowlisted**
- **maxpatrol**
- **atlas + upd**
- **hsps**
- **nsdps**
- **ads + tm + glb**
- **hsdps**

A bulk malware check for the string-connected domains categorized five of them as malicious.

—

Our in-depth analysis of the Decoy Dog IoCs uncovered more than 3,000 possibly connected web properties, a couple of which may have already figured in malicious campaigns. It also showed a number of similarities between the newly discovered artifacts and the IoCs Infoblox already made public.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts and IoCs

Decoy Dog IoCs Infoblox Identified

- cbox4[.]ignorelist[.]com
- claudfront[.]net
- allowlisted[.]net
- maxpatrol[.]net
- atlas-upd[.]com
- hsps[.]cc
- nsdps[.]cc
- j2update[.]cc
- ads-tm-glb[.]click
- hsdps[.]cc
- rcmsf100[.]net
- 13[.]248[.]169[.]48
- 156[.]154[.]132[.]200
- 194[.]31[.]55[.]85
- 5[.]199[.]173[.]4
- 5[.]252[.]176[.]63
- 5[.]252[.]176[.]22
- 5[.]252[.]179[.]18
- 67[.]220[.]81[.]190
- 69[.]65[.]50[.]194
- 69[.]65[.]50[.]223
- 70[.]39[.]97[.]253
- 83[.]166[.]240[.]52

Additional IP Addresses That Played Host to Domains Identified as IoCs

- 192[.]64[.]119[.]51
- 15[.]197[.]130[.]221

Sample IP-Connected Domains

- 2[.]houtworm[.]name
- allsafeInsurance[.]com
- auditline[.]eu[.]com
- barein[.]ch
- beautyhouse[.]eu[.]org
- capdonx[.]online
- cmd0[.]net
- darknode[.]net
- diamondpartyrentalsaz[.]com
- dns1[.]namecheaphosting[.]com
- dns1[.]registrar-servers[.]com
- dns1[.]web-hosting[.]com
- dns3[.]namecheaphosting[.]com
- dns3[.]registrar-servers[.]com
- dns5[.]registrar-servers[.]com
- dsg-edv[.]net
- ezshaping[.]pw
- freediscordbots[.]online
- freegameservers[.]online
- fueled[.]byhamsters[.]net

Sample Malicious IP-Connected Domains

- darknode[.]net
- settepani[.]net

Sample String-Connected Domains

- cbox4u[.]tk
- cbox4u[.]com
- ocbox4u[.]com
- whcbox4[.]com
- cbox4u[.]co[.]uk
- cbox4you[.]com
- musicbox4[.]cf
- locbox44[.]com
- xecbox48[.]loan
- musicbox4u[.]de
- ignorelist[.]ga
- ignorelist[.]co
- ignorelist[.]ru
- ignorelist[.]ws
- ignorelist[.]ml
- ignorelist[.]tk
- ignorelist[.]de
- ignorelist[.]xn--fiqs8s
- ignorelist[.]xyz
- ignorelist[.]com
- claudfront[.]gq
- claudfront[.]ml
- claudfronts[.]site
- allowlisted[.]io
- allowlisted[.]com
- allowlisted[.]xyz
- allowlisted[.]app
- londonrp-allowlisted[.]co[.]de
- allowlistedinstruments[.]net
- londonrp-allowlisted[.]co[.]uk
- maxpatrol[.]de
- maxpatrol[.]it
- maxpatrol[.]kz
- maxpatrol[.]ru
- maxpatrol[.]me
- maxpatrol[.]eu
- maxpatrol[.]com
- tmaxpatrol[.]com
- maxpatrolus[.]com
- maxpatrol[.]support
- atlasupdate[.]com
- atlasgroupdc[.]com
- atlasgroupdxb[.]com
- atlasgroupdev[.]com

- theatlasupdate[.]com
- atlasgroupdrons[.]com
- atlasgroupdrones[.]com
- atlassianupdates[.]com
- atlasgroupdagitim[.]com
- atlascopcoupdates[.]com
- hsps[.]hr
- hsps[.]se
- hsps[.]cz
- hsps[.]dk
- hsps[.]cf
- hsps[.]tk
- hsps[.]us
- hsps[.]sk
- hsps[.]de
- hsps[.]fr
- nsdps[.]cn
- nsdps[.]com
- nsdps[.]top
- rnsdps[.]in
- rnsdps[.]xyz
- rnsdps[.]com
- nsdpsei[.]cn
- lnsdps[.]com
- jnsdpsd[.]cn
- jnsdps[.]com
- nsdps[.]info
- wnsdps[.]xyz
- rnsdps[.]org
- ynsdps[.]com
- znsdps[.]club
- gansdps[.]com
- masonsdps[.]xn--kprw13d
- nsdpsis[.]site
- unsdpsh[.]info
- glbtmobileads[.]com
- hsdps[.]cn
- bhsdps[.]cn
- ihsdps[.]ws
- ihsdps[.]us
- hsdps[.]com
- nhsdps[.]com
- bhsdps[.]top
- shsdps[.]com
- ahsdpsp[.]cn
- ihsdps[.]net
- qhsdps[.]win
- ihsdps[.]com
- hsdpsc[.]com
- zhsdps[.]com
- ihsdpsq[.]us
- bhsdps[.]xyz
- hhsdps[.]win
- uhsdpsp[.]cn
- chsdps[.]com
- hsdpsi[.]icu

Sample Malicious String-Connected Domains

- mhspsp[.]eu
- uhsps[.]mom
- usp-ghspss[.]us