Decoy DogはDNSに痕跡を残さないほど狡猾か？

目次

要旨

DNSクエリを介してコマンド＆コントロール（C&C）を確立することで有名なマルウェア「Decoy Dog」がその姿を現したのは、おそらく2022年初頭のことです。Decoy Dogは、その狡猾な性質により、ロシアを含む東欧諸国の組織からデータを盗み出すことに成功しています。

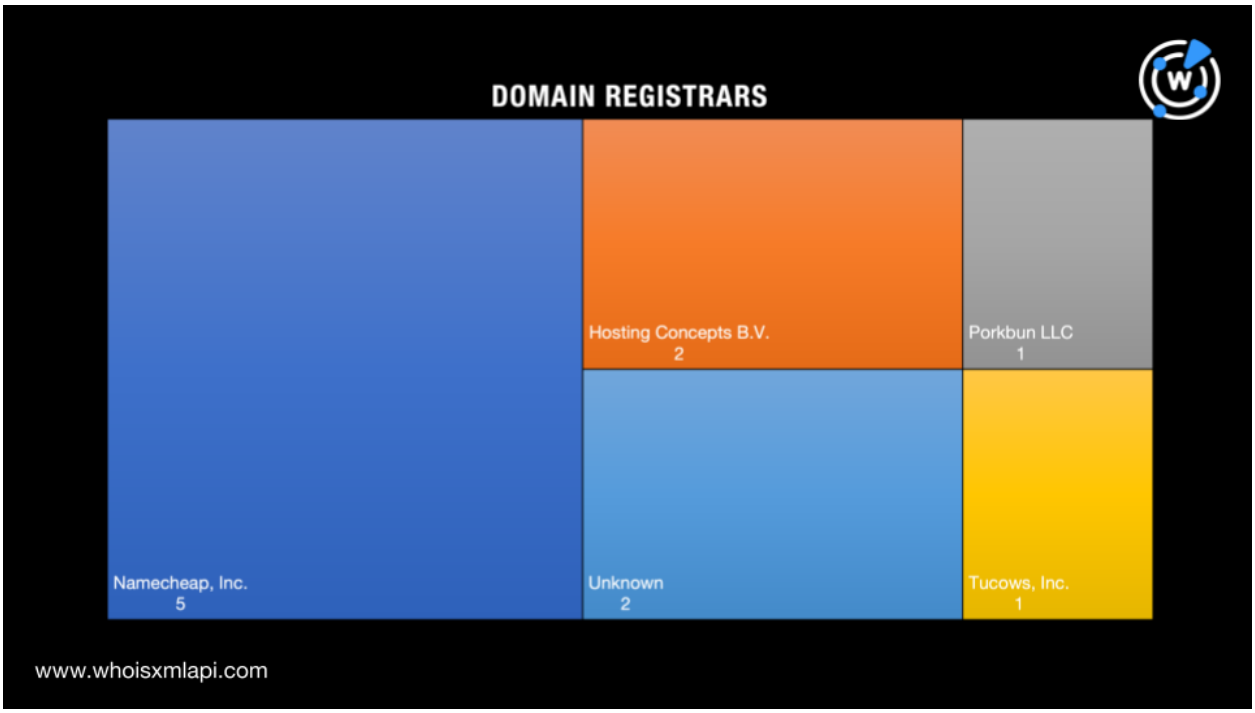
2023年4月、InfobloxがDecoy Dogインフラの詳細な分析を発表し、11個のドメイン名と12個のIPアドレスからなる合計23個のセキュリティ侵害インジケーター（IoC）を明らかにしました。WhoisXML APIではこれを受け、未確認のDecoy Dogの脅威ベクトルを特定するべく、InfobloxのIoCをもとにDNSを徹底的に調べました。そして、このほど以下を発見しました。

- InfobloxのIoCリストに含まれていない2つのIPアドレスへの名前解決。どちらもマルウェアチェックにより悪意のあるアドレスであることが判明
- IoCとして特定された5個の専用IPアドレスを使用していた90個のドメイン名。そのうち 4個は、マルウェアの一括チェックで悪意あるドメイン名と確認
- IoCと特定されたドメイン名のうち10個と同じく**cbox4**、**ignorelist**、**claudfront**、**allowlisted**、**maxpatrol**、**atlas + upd**、**hsps**、**nsdps**、**ads + tm + glb**または**hsdps**という文字列を含む2,295個のドメイン名。そのうち5個はマルウェアの一括チェックによりマルウェアホストと判明

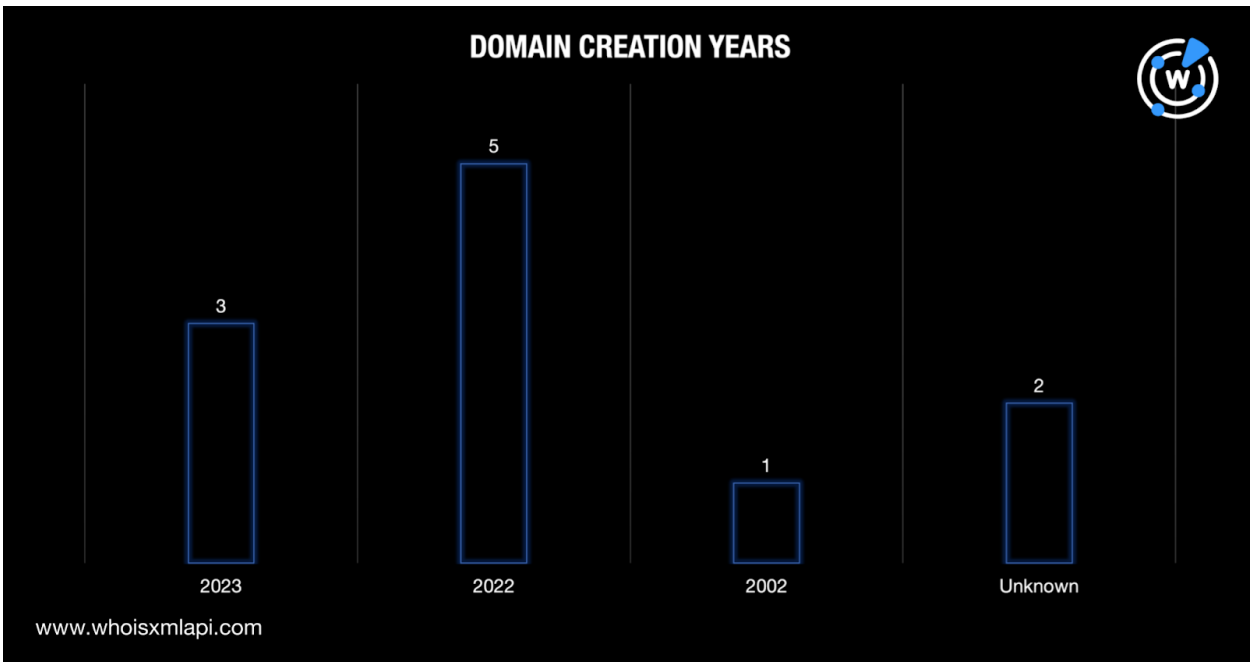
Decoy DogのDNSのルーツ

まず、InfobloxによってIoCと特定された11個のドメイン名をBulk WHOIS Lookupにかけました。その結果、2個（hsps[.]ccとrcmsf100[.]net）はアクティブなWHOISレコードを持っていないことがわかりました。以下は、WHOISレコードを参照できた残り9個に関する調査の結果です。

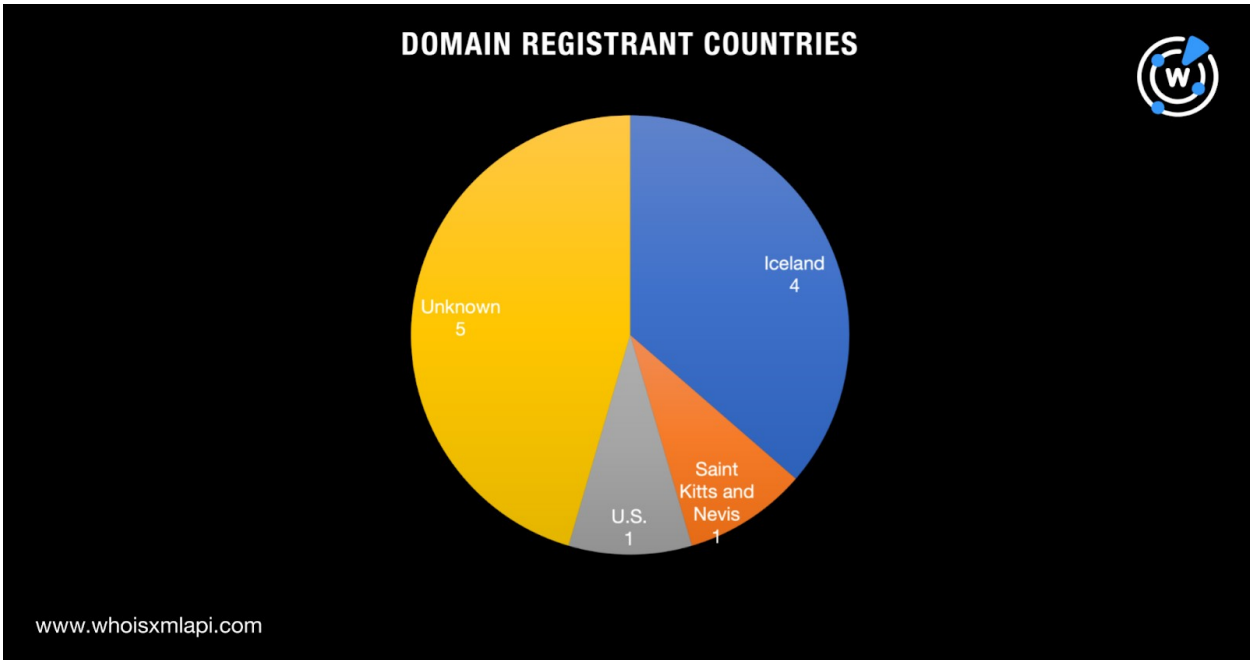
- 最も多くのドメイン名を管理していたレジストラはTucows（5個）でした。これに、Hosting Concepts（2個）、Porkbun LLC（1個）、Tucows, Inc.（1個）が続きます。



- 5個のIoCドメイン名は2022年に新規登録されました。これらはおそらく最初のDecoy Dog攻撃で使用されたものでしょう。3個は2023年に登録されたばかりで、近日中の攻撃を示唆している可能性があります。また、1個は2002年に登録された古いドメイン名でした。

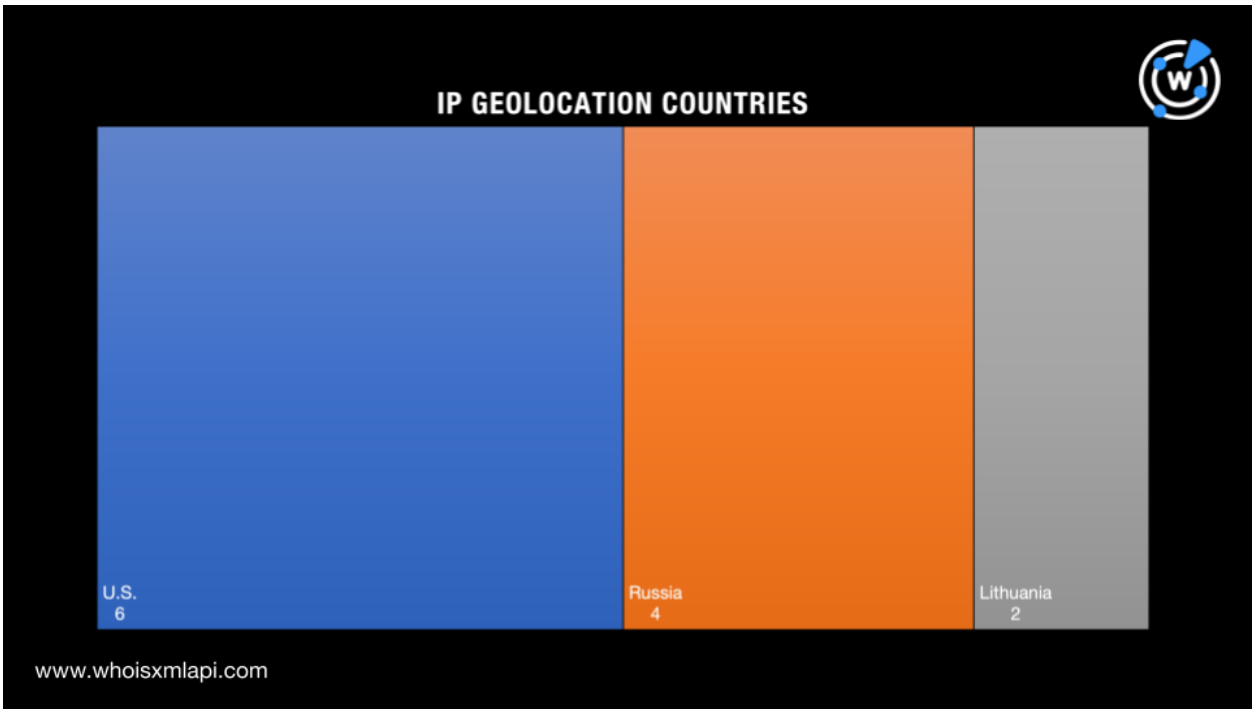


- 6個のIoCドメイン名は3カ国で登録されていました（アイスランド4個、セントクリストファーネービス1個、米国1個）。前述のWHOISレコードがなかった2個（hsps[.]ccとrcmsf100[.]net）に加え、3個のドメイン名（hsdps[.]cc、j2update[.]cc、nsdps[.]cc）の登録者は、国名を非公開にしていました。

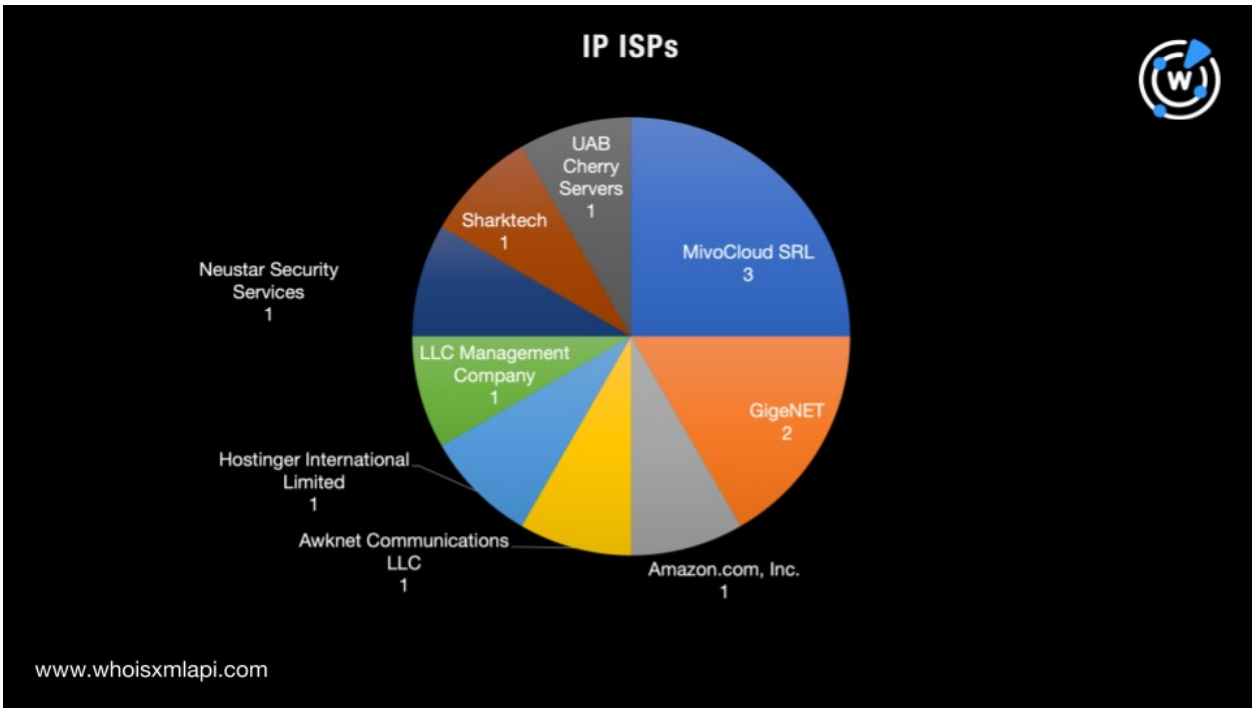


次に、IoCとして特定された12個のIPアドレスをBulk IP Geolocation Lookupで検索しました。その結果、以下が判明しました。

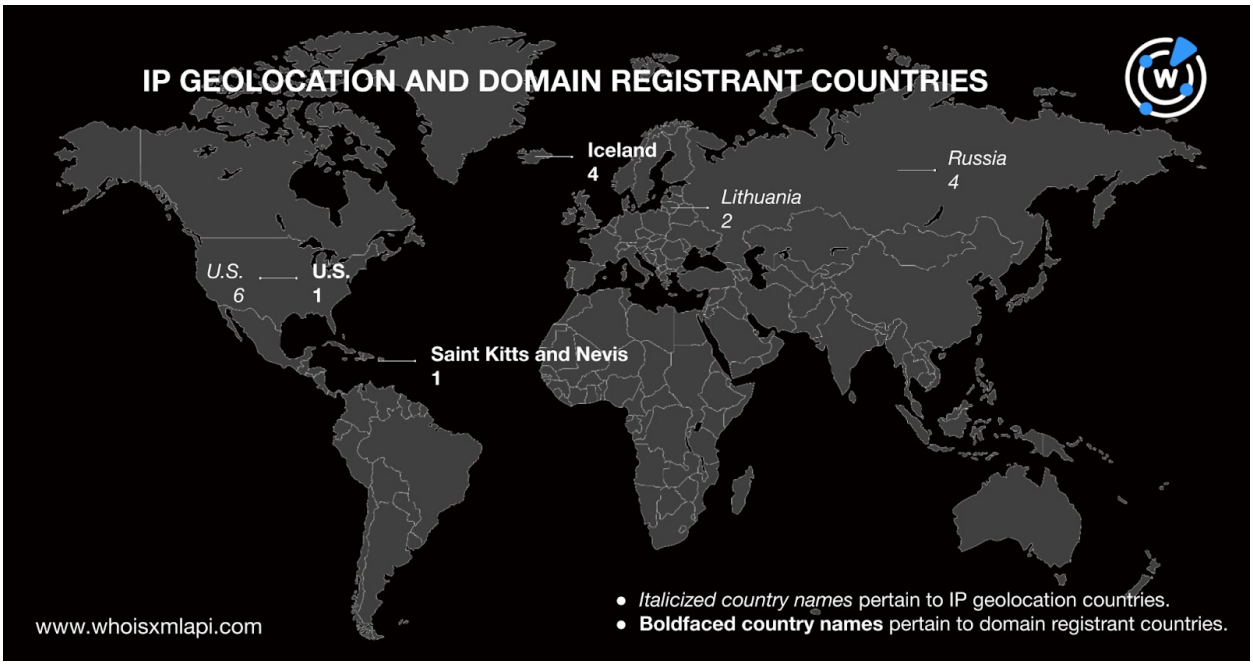
- 6個は地理的に米国に位置していました。また、4個はロシア、2個はリトアニアにありました。



- 9社のISPが特定されました。最も多くのアドレスを管理していたのはMivoCloud SRL（3個）で、次に多かったのはGigeNET（2個）です。



興味深いことに、登録者の国とIPアドレスのジオロケーションを照らし合わせたところ、両方の条件に該当した国は米国だけでした。



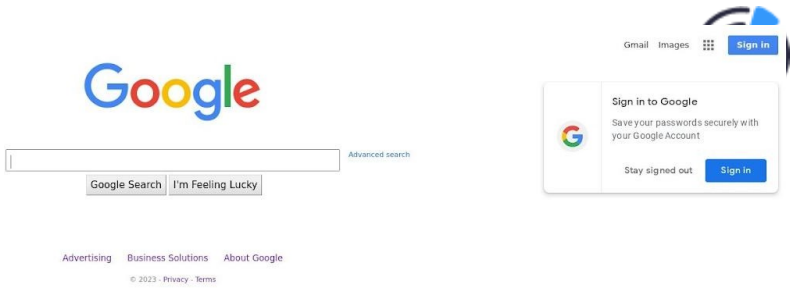
Decoy Dogの潜在的攻撃ベクトルを特定

IoCのドメイン名がIoCリストにないIPアドレスに名前解決するかどうかを確認するため、IoCのドメイン名をDNS Lookupにかけました。その結果、2個のIPアドレス（192[.]64[..]119[...]51と15[...]197[...]130[...]221）が新たに検出されました。そして、マルウェアチェックにより、どちらのIPアドレスにも悪意があることが判明しました。

その2個のIPアドレスをIP Geolocation Lookupで検索したところ、IoCとして特定されている6個のIPアドレスと同様に米国に位置していることがわかりました。2個のうちの1個、すなわち15[.]197[.]130[.]221の管理ISPは、IoCである13[.]248[.]169[.]48と同じAmazon.com, Incでした。

次に、IoCリストの12個と上記の検索で検出した2個を合わせた14アドレスについてReverse IP Lookupを実行しました。その結果、5個のIPアドレスは専用アドレスであること、そしてその5個が合計で90個のユニークなドメイン名をホストしていたことが判明しました。その90個に対してマルウェアの一括チェックを行ったところ、4個が悪意あるドメイン名に分類されました。

その4個のドメイン名のうち2個（darknode[.]netとsettepani[.]net）は、有効なコンテンツを指していました。darknode[.]netは、Googleの検索ページにリダイレクトしました。



darknode[.]net （google[.]comにリダイレクト）のスクリーンショット

上述の90個のドメイン名についてWHOISで一括検索を実行したところ、IoCとの共通点がいくつか見つかりました。主な共通点は以下の通りです。

- 35個のドメイン名のレジストラは、IoCドメイン名のレジストラのうち4社と同じ：Namecheap（30個）、Porkbun LLC（3個）、Hosting Concepts B.V.（1個）、Tucows, Inc.（1個）
- 34個のドメイン名の新規登録年は、2個のIoCドメイン名の新規登録年と同じ：2023年（16個）、2022年（8個）
- 53個のドメイン名は、IoCドメイン名の登録国として判明した2カ国で登録：アイスランド（29個）、米国（24個）

さらに、IoCのドメイン名を詳しく調べ、以下の10個の文字列を特定しました。そして、Domains & Subdomains Discoveryでこれらを検索したところ、関連性が疑われる別の2,295個のドメイン名にも含まれていることがわかりました。

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

その2,295個のドメイン名に対する一括マルウェアチェックでは、5個が悪意あるドメイン名に分類されました。

—

Decoy DogのIoCを徹底的に分析したことで、Decoy Dogとの関連が疑われるウェブプロパティを3,000個あまり発見できました。そのうちのいくつかは、すでに悪意あるキャンペーンで使われた可能性があります。また、Infobloxが公開したIoCと今回検出したプロパティの間に多くの共通点があることもわかりました。

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

Infobloxが特定したDecoy DogのIoC

- 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

IoCのドメイン名をホストしていたIPアドレス（今回の調査で発見）

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

共通のIPアドレスを使っていたドメイン名の例

- 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

共通のIPアドレスを使っていた悪意あるドメイン名の例

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

共通の文字列を含むドメイン名の例

- 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

共通の文字列を含む悪意あるドメイン名の例

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