Genesis Marketインフラの裏側：DNSの徹底分析

目次

1. 要旨
2. 付録：アーティファクトとIoCの例

要旨

サイバー犯罪者が活動している限り、地下市場の数は増え続けます。Silk Roadのような最大級のマーケットが取り締まられても、市場の高い収益性を見込んで独自のマーケットプレイスを立ち上げようとするサイバー犯罪者が出てくるのです。

例えばGenesis Marketは、Silk Roadの閉鎖から4年後の2017年に運営を開始しました。しかし、米連邦捜査局（FBI）などの法執行機関によって2022年4月に閉鎖に追い込まれました。

WhoisXML APIの研究チームはこのたび、Genesis Marketのインフラが本当にダウンしているかどうかを確かめるべく、リサーチャーのDancho Danchevが収集したセキュリティ侵害インジケーター（IoC）（12個のメールアドレス）をもとに調査を展開しました。

この調査の結果、以下を検出することができました：

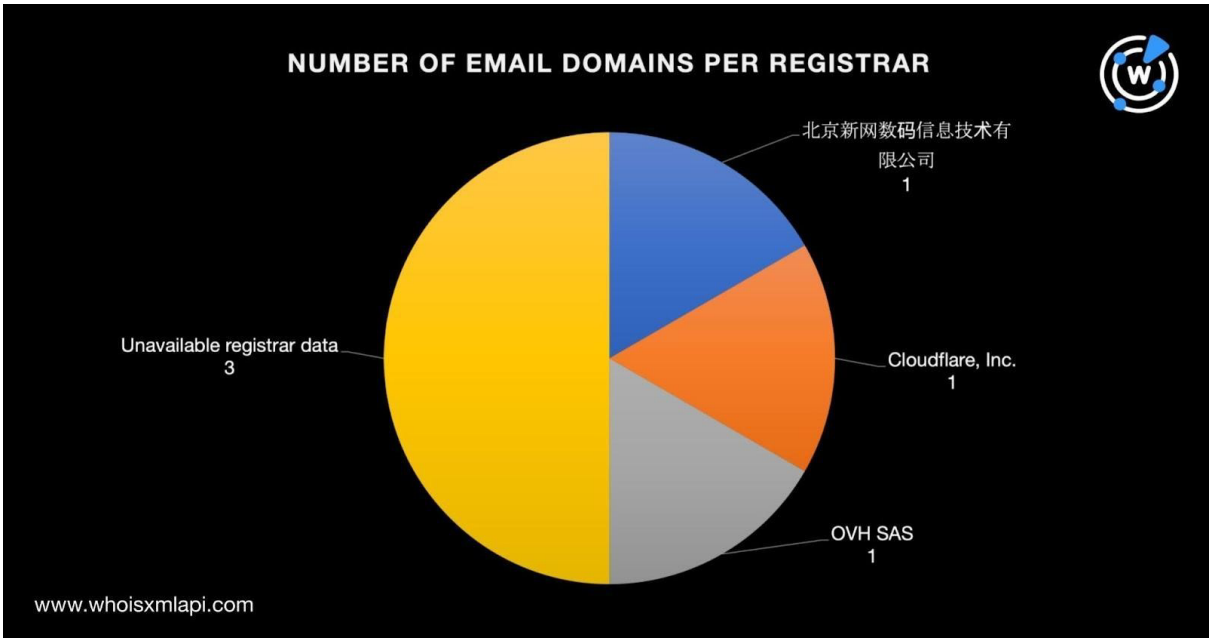
- 共通のメールアドレスを使用していたドメイン名28個
- IPアドレス5個
- 共通のIPアドレスを使用していたドメイン名2個
- 共通の文字列を含んだドメイン名2,417個。マルウェアチェックにより、そのうち3個は悪意あるドメイン名と判明

DNSで浮かび上がるIoCの実像

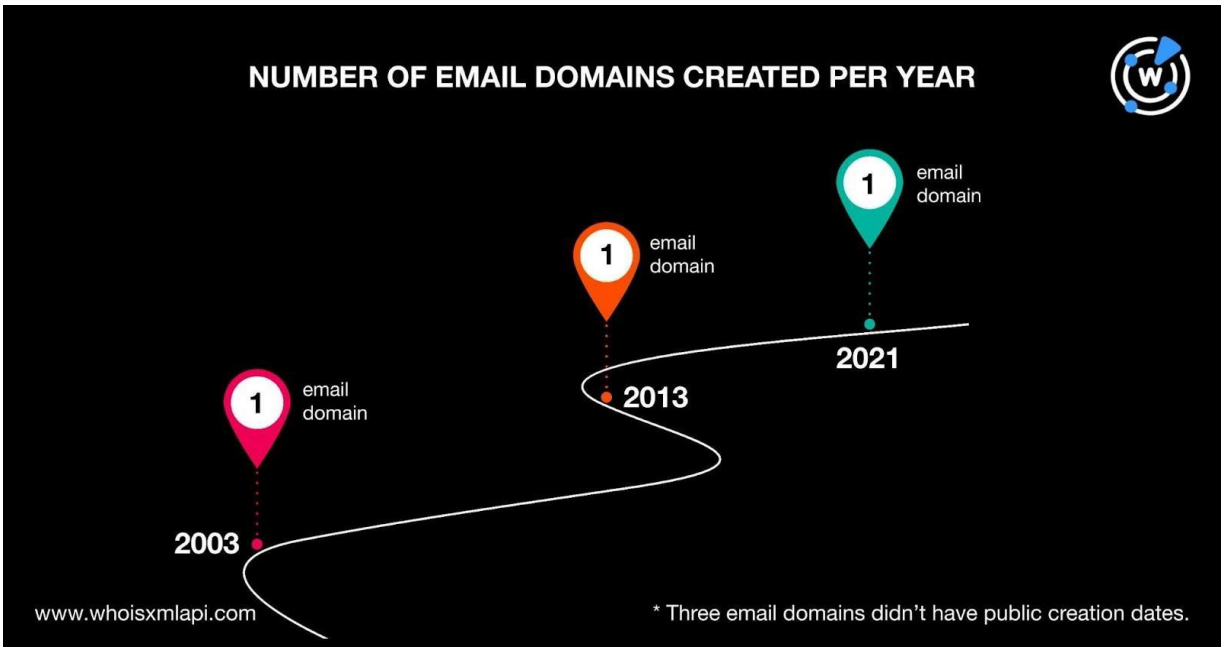
まず、IoCと特定された12個のメールアドレスについてそれぞれのドメイン名を確認し、カスタムメールドメインを持つ6個のメールアドレスに絞って分析を行うことにしました。それらはGenesis Marketの運用者が悪意あるキャンペーンのために特別に作成または不正アクセスした可能性があります。

調査結果の概要は以下の通りです：

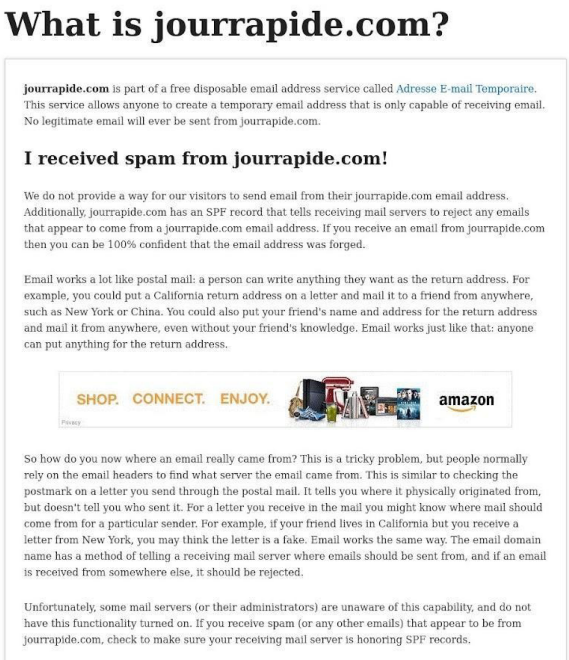
- 6個のIoCメールアドレスのドメイン名（以下「メールドメインIoC」）のうち3個については、WHOISにレジストラのデータが公開されていませんでした。残りの3個については、それぞれ北京新网数码信息技术有限公司（Beijing Xinwang Digital Information Technology Co., Ltd.）、Cloudflare, Inc.、OVH SASに管理されていました。



- WHOISデータの作成日がわかるメールドメインIoCは6個のうち3個のみで、それぞれ2003年、2013年、2021年でした。



- 2個のメールドメインIoCは登録者の国の情報が公開されており、それぞれ、スペインと米国でした。
- マルウェアチェックの結果、1個（jourrapide[.]com）は悪意あるドメイン名と判明しました。このドメイン名についてScreenshot Lookupを実行したところ、本稿執筆時点で依然としてアクセス可能な状態とわかりました。



What is jourrapide.com?

jourrapide.com is part of a free disposable email address service called Adresse E-mail Temporaire. This service allows anyone to create a temporary email address that is only capable of receiving email. No legitimate email will ever be sent from jourrapide.com.

I received spam from jourrapide.com!

We do not provide a way for our visitors to send email from their jourrapide.com email address. Additionally, jourrapide.com has an SPF record that tells receiving mail servers to reject any emails that appear to come from a jourrapide.com email address. If you receive an email from jourrapide.com then you can be 100% confident that the email address was forged.

Email works a lot like postal mail: a person can write anything they want as the return address. For example, you could put a California return address on a letter and mail it to a friend from anywhere, such as New York or China. You could also put your friend's name and address for the return address and mail it from anywhere, even without your friend's knowledge. Email works just like that: anyone can put anything for the return address.

So how do you now where an email really came from? This is a tricky problem, but people normally rely on the email headers to find what server the email came from. This is similar to checking the postmark on a letter you send through the postal mail. It tells you where it physically originated from, but doesn't tell you who sent it. For a letter you receive in the mail you might know where mail should come from for a particular sender. For example, if your friend lives in California but you receive a letter from New York, you may think the letter is a fake. Email works the same way. The email domain name has a method of telling a receiving mail server where emails should be sent from, and if an email is received from somewhere else, it should be rejected.

Unfortunately, some mail servers (or their administrators) are unaware of this capability, and do not have this functionality turned on. If you receive spam (or any other emails) that appear to be from jourrapide.com, check to make sure your receiving mail server is honoring SPF records.

悪意あるメールドメインIoCであるjourrapide[.]comのスクリーンショット

DNSの調査結果

Genesis Marketが閉鎖後に残したかもしれない痕跡をDNSから探し出すため、IoCと特定された12個のメールアドレスをReverse WHOIS Searchを使って検索しました。すると、1個のメールアドレスが28個のドメイン名の現在のWHOISレコードに表示されました。

次に、その28個のドメイン名をDNS Lookupで検索したところ、5個のユニークなIPアドレスに名前解決することがわかりました。

そのうち4個のアドレスは専用と思われ、合計で6個のドメイン名をホストしていました。そこから重複と共通のメールアドレスを使っているドメイン名を取り除いた結果、共用されているIPアドレスとして2個が残りました。

同じメールアドレスまたはIPアドレスを共用しているドメイン名についてさらに精査した結果、Genesis Marketが悪意あるキャンペーンに使うために選んだと思われる22種類の固有の文字列（以下）を特定できました：

- **eactexpo**
- **gobaza**
- **grandscape**
- **hymg.**
- **korkpay**
- **nsr.**
- **qcgk.**
- **silk-road**
- **udhg.**
- **wsreli**
- **xj118114**
- **xj96596**
- **xjei.**
- **xjghwy**
- **xjhjtx**
- **xjitv**
- **xjkokse**
- **xjmuseum**
- **xjrccb**
- **xjsgj**
- **xjxnw**
- **xjyh.**

上記の22種類の文字列を検索語とし、Domains & Subdomains Discoveryの**Contains**パラメータを用いて過去データを検索したところ、条件に合致するドメイン名を12,442個収集することができました。誤検出の数を減らすために、文字列**nsr.**の検索結果（10,000個あまりのドメイン名に出現）、重複およびメールアドレスまたはIPアドレスを共用していることを確認済みのドメイン名を取り除きました。その結果、2,417個のドメイン名が残りました。

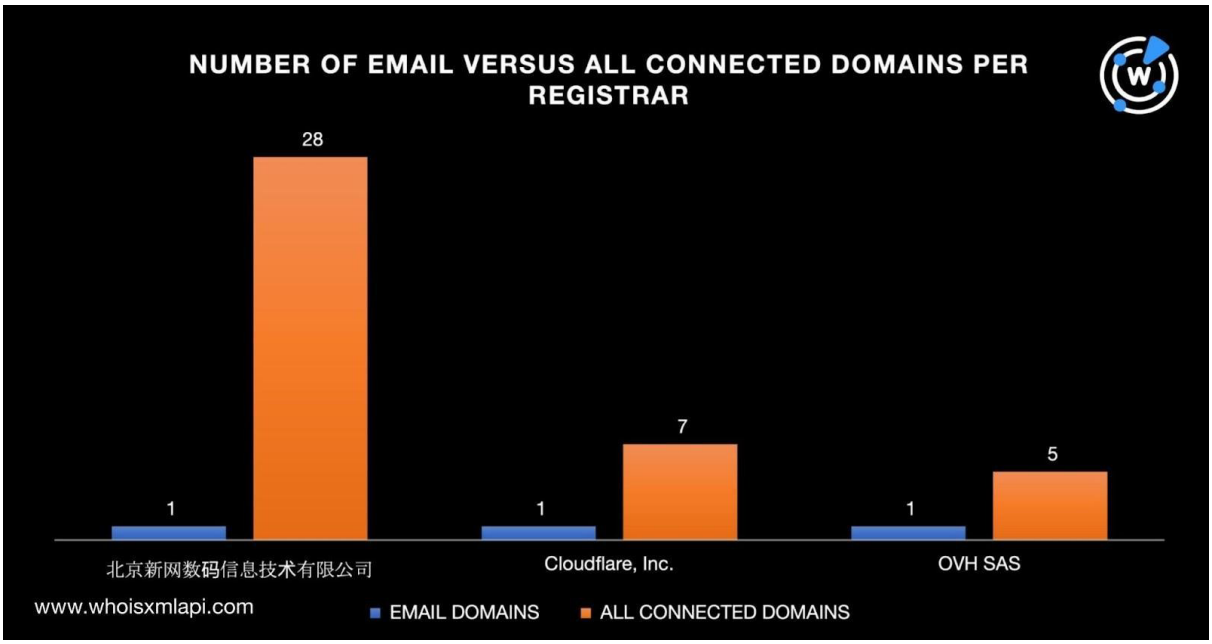
その2,417個をマルウェアの一括チェックにかけたところ、3個はすでに悪意あるドメイン名と判定されていました。その3個についてScreenshot Lookupを実行した結果、1個（silk-road[.]xyz）はその時点でもアクセス可能でしたが、エラーページに誘導されました。このドメイン名には、**silk-road**という文字列が含まれています。Silk Roadは、2011年に立ち上げられた最初のダークネット市場です。

悪意あるドメイン名silk-road[.]xyzのスクリーンショット

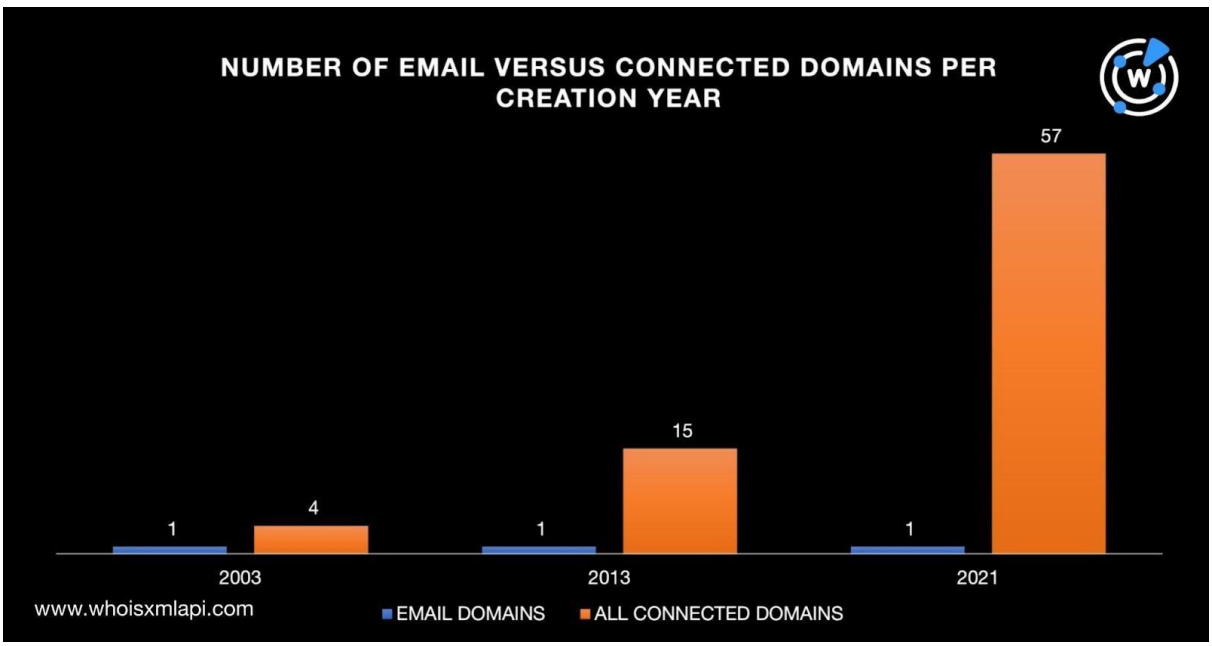
IoCと関連ドメイン名の共通点

これまでに特定された関連ドメイン名とGenesisMarketのIoCを詳細に分析した結果、いくつかの共通点が見られました：

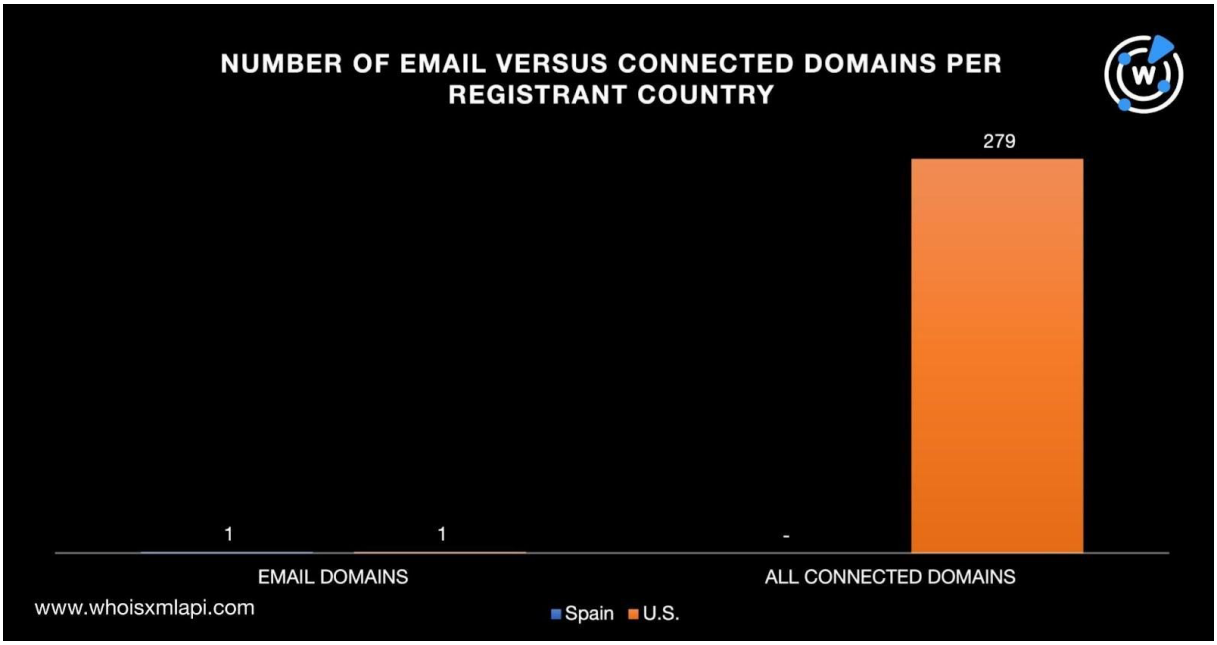
- 40個の関連ドメイン名（共通のメールアドレス、IPアドレスまたはテキスト文字列を持つもの）は、メールドメインIoCと同じレジストラを使っていました。具体的には、北京新网数码信息技术有限公司が28個、Cloudflare, Inc.が7個、OVH SASが5個の関連ドメイン名を管理していました。1,640個の関連ドメイン名のWHOISレコードにはレジストラの情報がありませんでした。残りの561個は、他のレジストラによって管理されていました。



- 4個、15個、57個の関連ドメイン名は、それぞれ2003年、2013年、2021年に新規登録されたものでした。これはメールドメインIoCと共通しています。また、1,634個の関連ドメイン名にはWHOISデータの作成日がなかった一方、734個は1995～2002年、2004～2012年、2022～2023年のいずれかの年に新規登録されたものでした。



- 関連ドメイン名のうちスペインで登録されたものはありませんでしたが、279個はメールドメインIoCと同様に米国で登録されていました。



—

今回Genesis MarketのIoCを出発点として行ったDNS調査で、同IoCに関連する2,452個のアーティファクトが発見されました。また、IoCに関連するドメイン名のうち40個の管理レジストラ、76個の新規登録年、279個の登録国がメールドメインIoCと同じでした。

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

Genesis MarketのIoCとして特定されたメールアドレス

- cmi*****@mpi-klsb[.]mpg[.]de
- c*****@vianw[.]pt
- co*****@gmail[.]com
- *****@aol[.]com
- gerben_h*****@163[.]com
- ghe*****@gherasim[.]net
- *****@webcontrolmultimedia[.]com
- michellewmo*****@jourrapide[.]com
- put[.]a[.]feud[.]pike0*****@gmail[.]com
- working_su*****@163[.]com
- x*****@xj163[.]cn
- ykc*****@163[.]com

上記のメールアドレスを使用して登録されたドメイン名の例

- eactexpo[.]com[.]cn
- gobaza[.]cn
- grandscape[.]com[.]cn
- hymg[.]cn
- korkpay[.]com[.]cn
- nsr[.]tel
- qcgk[.]com[.]cn
- silk-road[.]net[.]cn
- udhg[.]com[.]cn
- wsreli[.]cn
- xj118114[.]cn
- xj96596[.]cn
- xj96596[.]com[.]cn
- xjei[.]cn
- xjghwy[.]com[.]cn

IPアドレスの例

- 117[.]190[.]16[.]8
- 117[.]190[.]227[.]10
- 170[.]106[.]48[.]231

共通のIPアドレスを使用していたドメイン名の例

- grandscape[.]cn

共通の文字列を含むドメイン名の例

- 0mudhg[.]cn
- 0qcgk[.]ph
- 0qcgk[.]tk
- 0udhg[.]tk
- 0udhg[.]xyz
- 0y6qcgk[.]icu
- 1vq3j0e6m10ud8npaj0i70c5j81ludhg[.]uk
- 1wxjei[.]top
- 1xjei[.]cn
- 2020uqcgk[.]work
- 2gobazaar[.]com
- 2gobazar[.]com
- 2lewsreliableheat[.]com
- 2uwqcgk[.]club
- 31xjyh[.]cyou
- 3cxjxnwyyxb2szj3674q-po9bd3-d48d5d130-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxb2szj3suea-picqty-fab1ee7a7-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxb2szjjc3na-py07kh-34624ce48-clientnsv4-s[.]akamaihd[.]net

- 3cxjxnwyyxb2szku4a4q-pooxh4-ed1342183-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxb2szkvfvtq-pubs1v-1f586d634-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxb3czkkbywq-pmsm1f-f24167f2d-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxbrazkt6v2a-p9rpdy-58c919fcb-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxbzezj7ykfa-pylrms-20b1e575a-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxbzezjnp7da-pnfy18-3d575b6e9-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxbzezjqcmaa-pdsqci-921281921-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxbzezjxf3wq-p177r8-3590f12b7-clientnsv4-s[.]akamaihd[.]net
- 3cxjxnwyyxbzezku6i6a-p7hf3r-d0a569abd-clientnsv4-s[.]akamaihd[.]net
- 3hymg[.]tk
- 3xjyh[.]tk
- 42qnllatwn5qse3bnvrgzcxjyh[.]com
- 48qcgk[.]ga
- 4a8j9n8iudhg[.]club
- 4hymg[.]tk
- 4lewsreliableheat[.]com
- 4pawsrelief[.]com
- 4qcgk[.]life
- 51silk-road[.]com
- 58silk-road[.]com
- 5hymg[.]tk
- 5ugcxjyh[.]tw
- 5y8hymg[.]cn
- 5yxjei[.]tw
- 68xjyh[.]cn
- 68xjyh[.]top
- 6hymg[.]tk
- 6hymg[.]top
- 6khymg[.]top
- 6qcgk[.]tk
- 6r5982hymg[.]skin
- 6txjyh[.]cn
- 6xjyh[.]tk
- 7g5micme-i59udhg[.]com
- 7nhymg[.]cyou
- 7xjyh[.]com
- 7xjyh[.]tk
- 8mjsxjei[.]com
- 8xjei[.]com
- 91xjyh[.]cc
- 99cmqcgk[.]top
- 9dqcgk[.]cn
- 9x4xjei[.]work
- a557xjei[.]xyz
- a9rsxjei[.]com
- abexjitvie[.]cf
- adflnomudhg[.]xyz
- adudhg[.]xyz
- afuegobazar[.]com[.]ar
- agaligobazaar[.]com
- agogobazaar[.]com
- agogobazar[.]com
- ahcudhg[.]top
- ahymg[.]com
- ailqudhg[.]cf
- ailqudhg[.]ga
- aipxjyh[.]cn
- aircargobazaar[.]com
- ajudhg[.]com
- ak-silk-road[.]com
- akudhg[.]cn
- alalwkwqudhg[.]site
- algobazaar[.]com
- algobazar[.]com
- all-silk-road-tours[.]com
- als-silk-road[.]com
- amagobazar[.]com

- amazing-silk-road[.]com
- ambassador-silk-road-drive[.]com
- americangrandscape[.]com
- americangrandscape[.]net
- americangrandscape[.]org
- amgobazar[.]com
- amigobazaar[.]cyou
- amigobazar[.]com
- amxjei[.]com
- amxjsgjyl[.]com
- amxjsgjyl003[.]cn
- amxjsgjyl004[.]cn
- amxjyh[.]com
- anarchymg[.]com
- andrewsreliableconcrete[.]com

共通の文字列を含む悪意あるドメイン名の例

- silk-road[.]xyz
- wtqcgk[.]ga