Behind the Genesis Market Infrastructure: An In-Depth DNS Analysis

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts and IoCs

Executive Report

As long as cybercriminals remain in business, so will the number of underground marketplaces grow. And despite the crackdown on the biggest markets like Silk Road, cybercriminals will continue to strive to put up their own marketplaces, probably given their profitability.

Case in point? The Genesis Market began operating in 2017, four years after Silk Road closed shop. Like its predecessor, though, the Federal Bureau of Investigation (FBI) and other law enforcement agencies took the Genesis Market down last April.

The WhoisXML API research team sought to find out if Genesis Market's infrastructure is truly down and out. We expanded a list of indicators of compromise (IoCs)—12 email addresses to be exact—researcher Dancho Danchev collated.

Our Genesis Market DNS deep dive led to the discovery of:

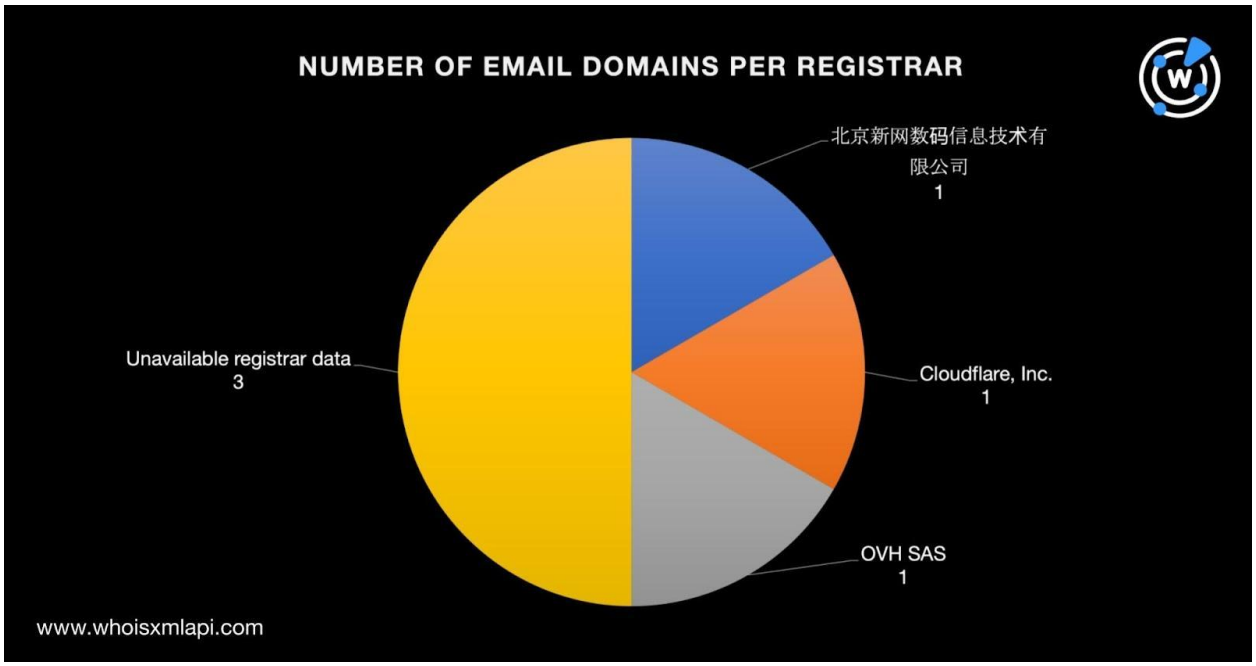
- 28 email-connected domains
- Five IP addresses
- Two IP-connected domains
- 2,417 string-connected domains, three of which turned out to be malicious based on malware checks

IoC DNS Revelations

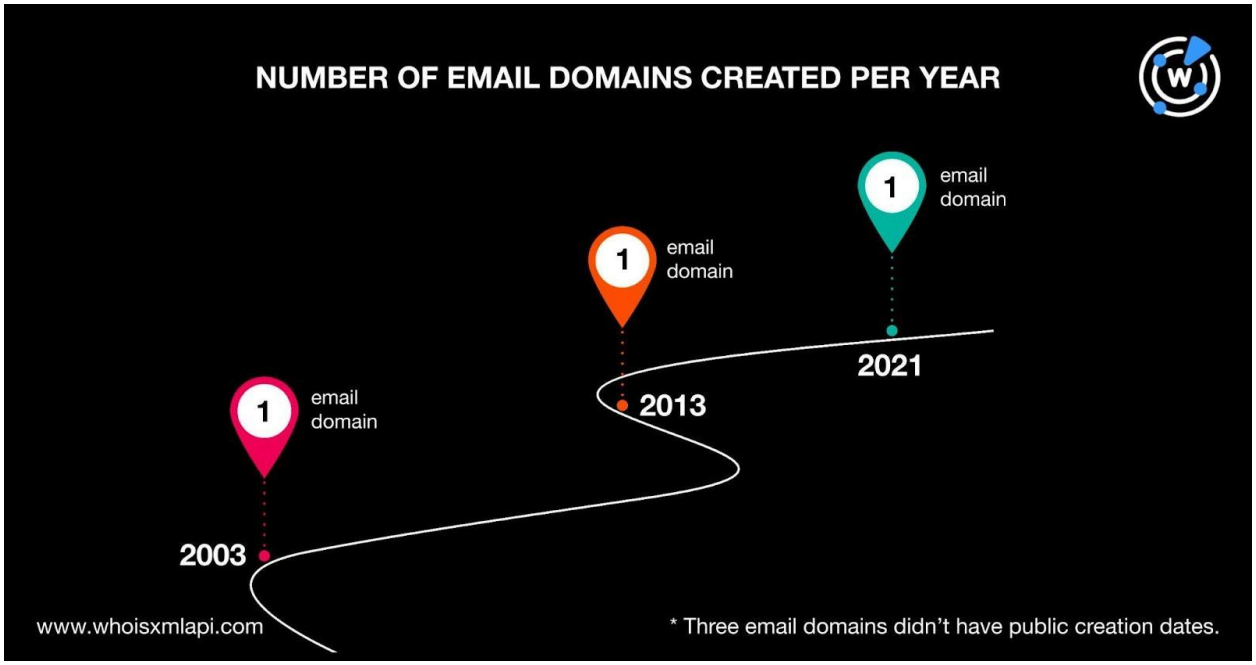
First off, we sought to find more information on the 12 email addresses identified as IoCs by looking more closely at their domains. We decided to focus our analysis on the six email addresses with custom email domains, as the Genesis Market operators may have specially crafted or compromised them for their malicious campaigns.

Here's a summary of our findings:

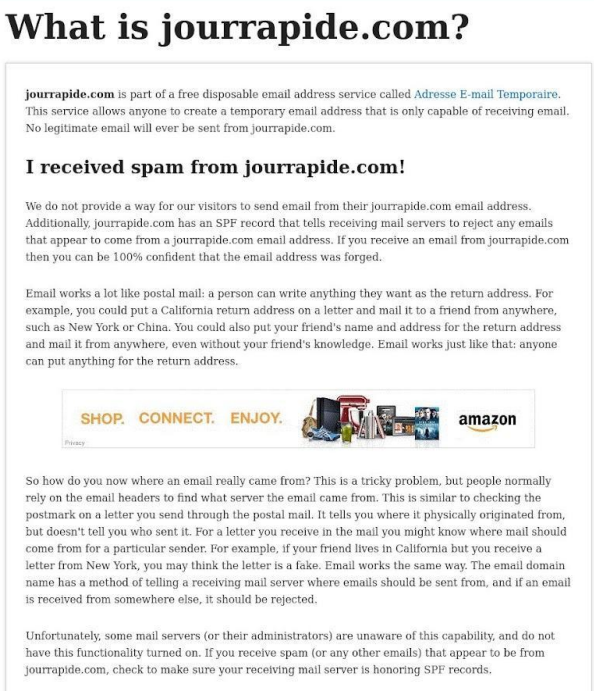
- Three of the six email domains didn't have current public registrar data. One each was administered by 北京新网数码信息技术有限公司 (which translates to Beijing Xinwang Digital Information Technology Co., Ltd.); Cloudflare, Inc.; and OVH SAS.



- Only three of the six email domains had current public creation dates. One each was registered in 2003, 2013, and 2021.



- Two of the six email domains had current public registrant country information. One each was registered in Spain and the U.S.
- Based on the results of malware checks, one of the email domains—jourrapide[.]com—turned out to be malicious. A screenshot lookup for the malicious email domain showed that it remained accessible as of this writing.



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.

Screenshot of malicious email domain jourrapide[.]com

DNS Deep Dive Findings

To scour the DNS for traces that Genesis Market may have left behind after its takedown, we performed reverse WHOIS searches for the 12 email addresses identified as IoCs. Only one of the email addresses appeared in the current WHOIS records of 28 domains.

Next, we subjected the 28 email-connected domains to DNS lookups. We discovered that they resolved to five unique IP addresses.

Four of the IP addresses were seemingly dedicated. Altogether, they hosted six domains. After removing duplicates and the email-connected domains, we were left with two IP-connected domains.

Further scrutiny of the email- and IP-connected domains allowed us to collate a list of 22 unique strings that Genesis Market may have specifically chosen to use for their malicious campaigns. These text strings were:

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

Using the 22 strings above as Domains & Subdomains Discovery historical search terms enabled us to collate 12,442 string-connected domains using the **Contains** parameter. To reduce the number of false positives, we filtered out the results for **nsr.** (which appeared in 10,000+ domains), along with duplicates and the domains already classified as email- and IP-connected domains. That left us with 2,417 string-connected domains.

A bulk malware check for the 2,417 string-connected domains revealed that three of them were already categorized as malicious. Screenshot lookups showed that one of the malicious domains—silk-road[.]xyz—remained accessible even if it led to an error page. Note the

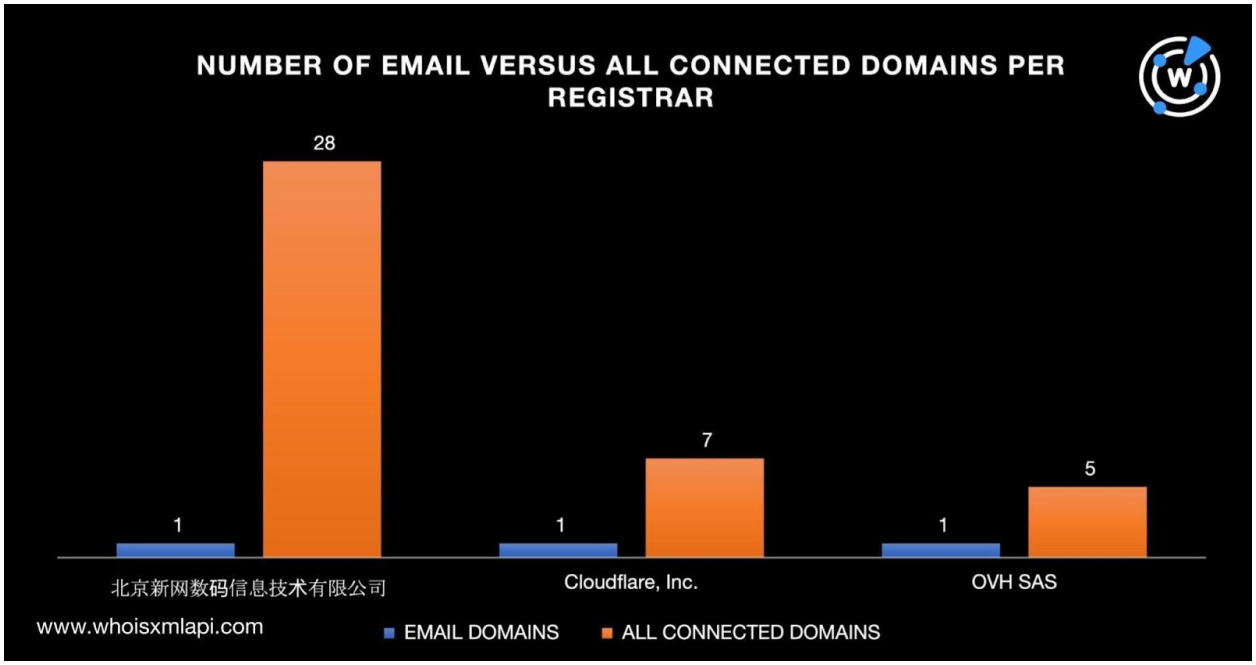
appearance of the string **silk-road** in the domain, too. Silk Road was the first darknet market established in 2011.

Screenshot of the malicious string-connected domain silk-road[.]xyz

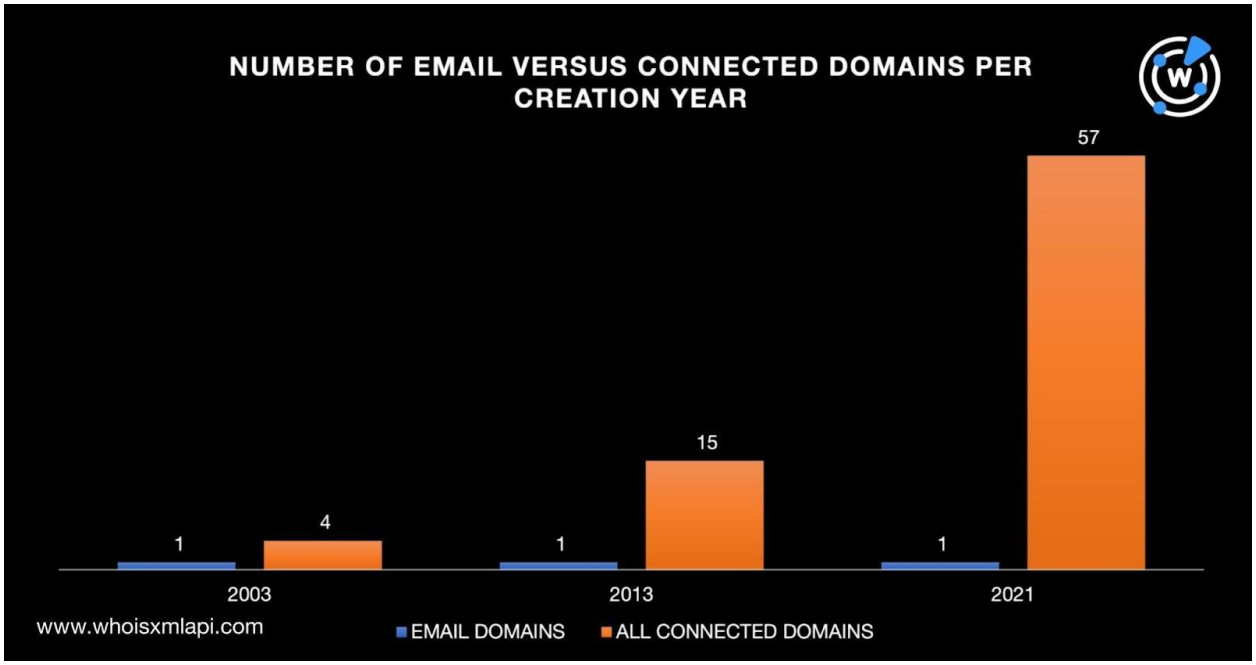
Uncovering Similarities between the IoCs and Connected Domains

Our in-depth analysis of the Genesis Market IoCs and connected domains also showed some similarities, namely:

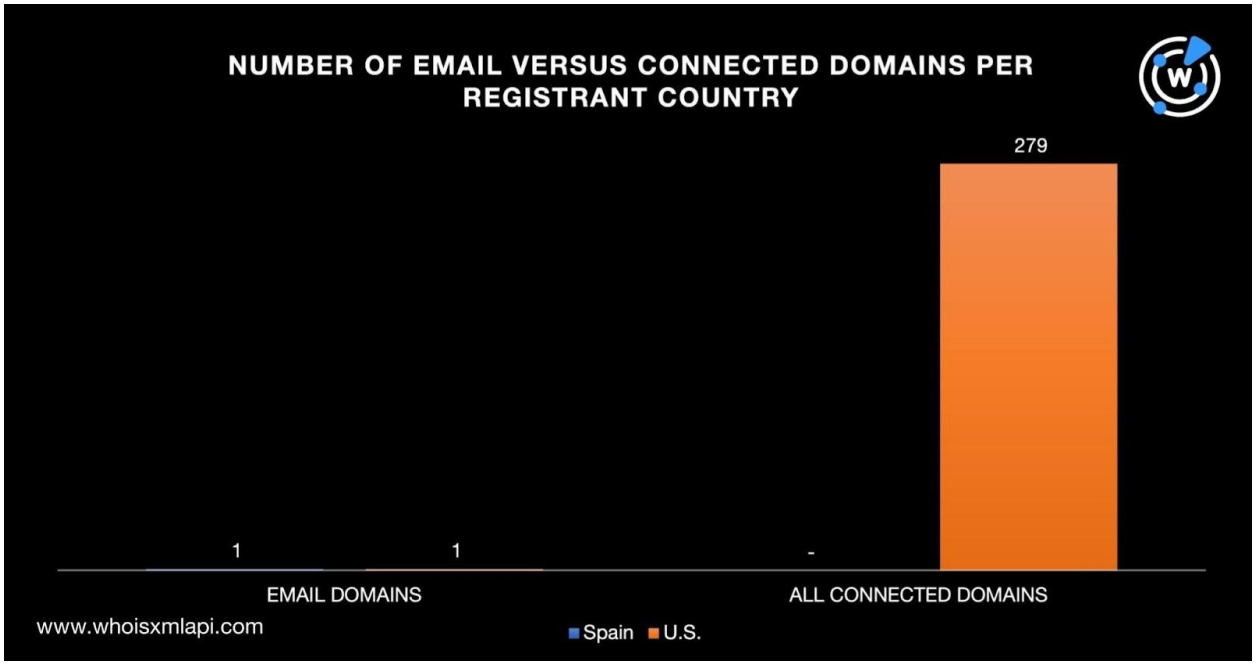
- Forty connected domains (via email address, IP address, and text string) shared the email domains' registrars. Specifically, 北京新网数码信息技术有限公司 administered 28 connected domains. Seven and five connected domains, meanwhile, were administered by Cloudflare, Inc. and OVH SAS, respectively. While 1,640 connected domains didn't have current public registrar data, 561 were distributed among several other registrars.



- Four, 15, and 57 connected domains were created in 2003, 2013, and 2021, respectively, akin to the email domains. While 1,634 connected domains didn't have current public creation dates, 734 were created in 1995–2002, 2004–2012, and 2022–2023.



- While none of the connected domains were registered in Spain, 279 were registered in the U.S. like one of the email domains.



—

Our DNS deep dive into the Genesis Market IoCs led to the discovery of 2,452 potentially connected artifacts. We also found that 40 connected domains shared the email domains' registrars, 76 shared the email domains' creation years, and 279 shared the email domains' registrant countries.

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

Email Addresses Identified as Genesis Market IoCs

- 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

Sample Email-Connected Domains

- 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

Sample IP Addresses

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

Sample IP-Connected Domain

- grandscape[.]cn

Sample String-Connected Domains

- 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

Sample Malicious String-Connected Domains

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