A DNS Deep Dive into New Crypto Threat "Hidden Risk"

Table of Contents

Executive Report

As of 2024, more than 560 million people own cryptocurrencies worldwide, which could translate to more than half a million potential cyber attack victims. This widespread adoption may explain the emergence of threats like Hidden Risk, a malicious campaign that uses fake crypto news to distribute the RustBucket malware.

SentinelLabs published an in-depth investigation of the Hidden Risk campaign and identified 86 indicators of compromise (IoCs) related to the payload—RustBucket.

The attack began with phishing attempts targeting crypto-related businesses. Victims were tricked into downloading a dropper with RustBucket as a payload. The SentinelLabs researchers believed the campaign began as early as July 2024 and used fake news about cryptocurrency-related topics.

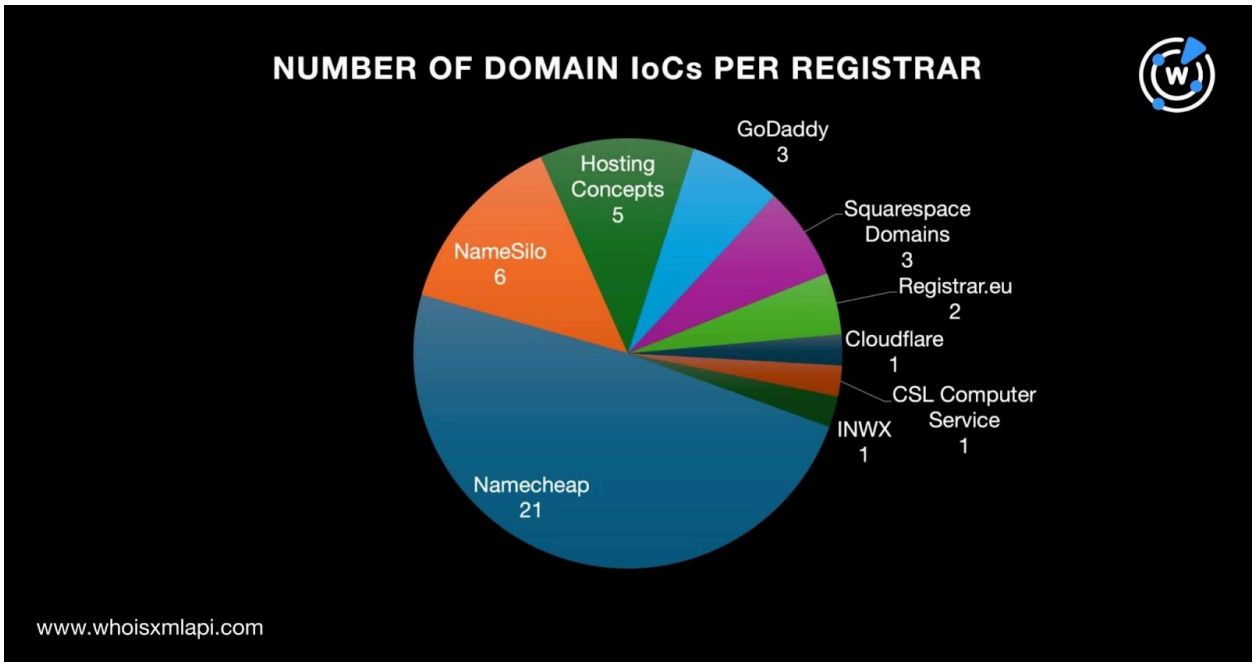
The WhoisXML API research team handpicked 81 of the IoCs, specifically 44 domains, 27 subdomains, and 10 IP addresses, for an expansion analysis. Our DNS deep dive led to the discovery of:

- 40 email-connected domains
- 14 additional IP addresses, 13 of which turned out to be malicious
- Six IP-connected domains
- 1,685 string-connected domains, three of which turned out to be malicious
- Five string-connected subdomains

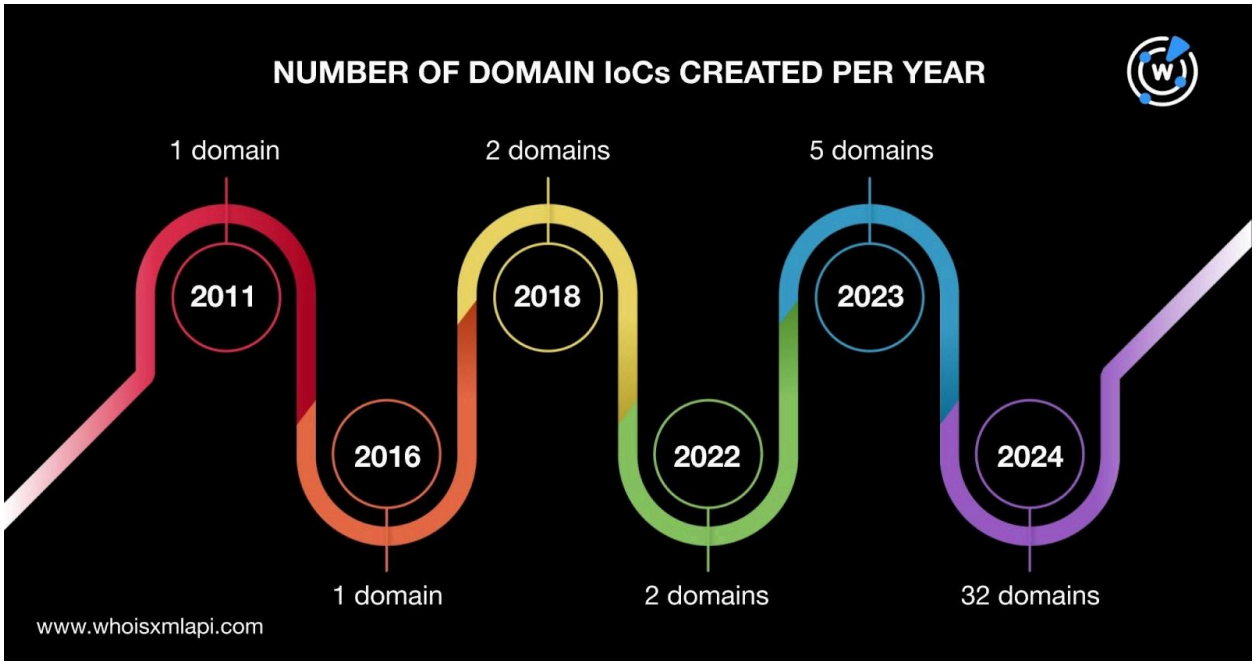
About the Hidden Risk IoCs

We began our analysis with a bulk WHOIS lookup for the 44 domains tagged as IoCs, which found that:

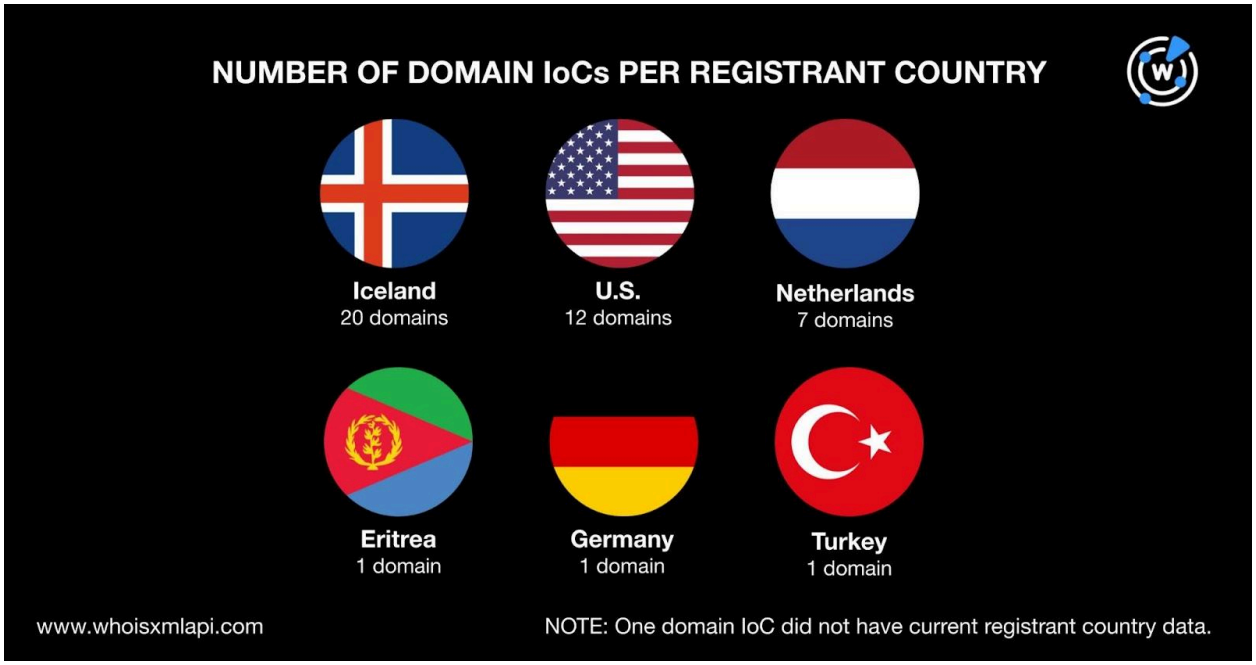
- Only 43 of them had current WHOIS records.
- The 43 domain IoCs with current WHOIS data were administered by nine registrars led by Namecheap, which accounted for 21 domains. The rest of the registrars were NameSilo with six domains; Hosting Concepts with five; GoDaddy and Squarespace Domains with three each; Registrar.eu with two; and Cloudflare, CSL Computer Service, and INWX with one each.



- The 43 domain IoCs with current WHOIS data were created between 2011 and 2024, with most (74%) being newly created.



- The domain IoCs with current WHOIS data were registered in six different countries led by Iceland, which accounted for 20 domains. The remaining registrant countries were the U.S. with 12 domains; the Netherlands with seven; and Eritrea, Germany, and Turkey with one each. One domain IoC did not have current registrant country data.

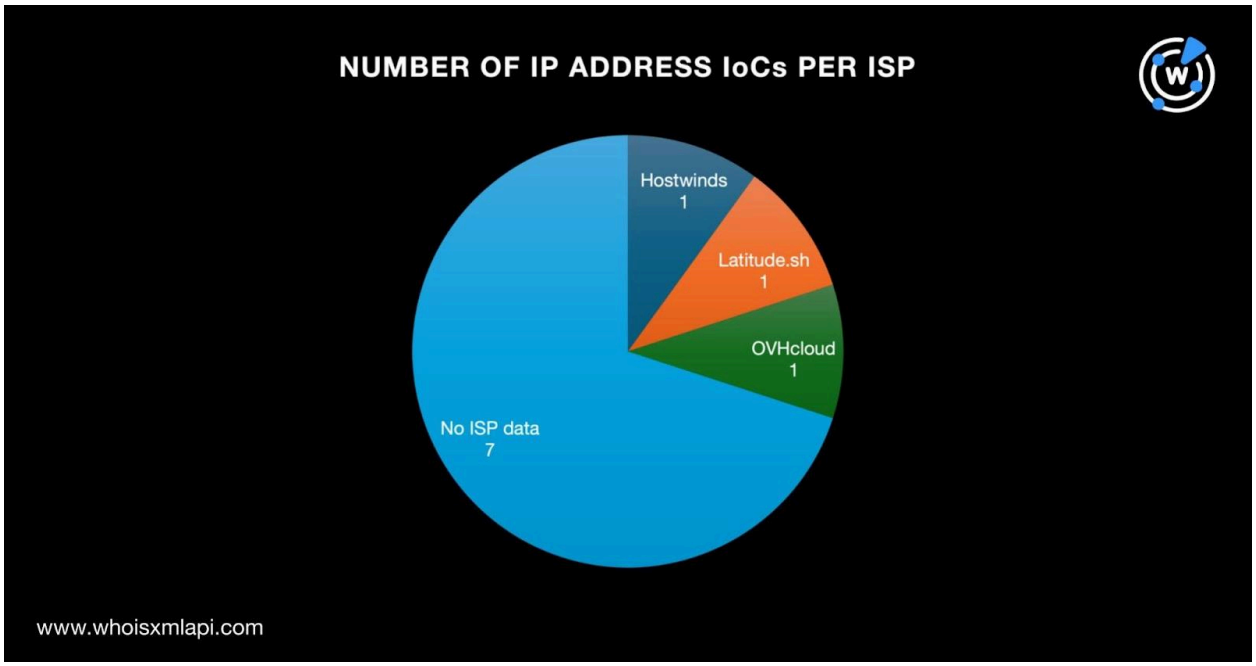


A query on DNS Chronicle API for the 44 domains tagged as IoCs showed that 34 had resolved to at least one IP address in the past. Overall, they resolved to 537 IP addresses between 2019 and 2024. Here are five examples with historical DNS data.

DOMAIN IoC	START DATE	END DATE	NUMBER OF IP ADDRESSES
ankanimatoka[.]com	22 March 2024	28 August 2024	14
buy2x[.]com	23 April 2020	9 July 2024	27
caladan[.]video	30 October 2024	30 October 2024	1
delphidigital[.]org	3 April 2024	20 October 2024	9
evalaskatours[.]com	23 October 2019	15 November 2024	3

A bulk IP geolocation lookup for the 10 IP addresses tagged as IoCs yielded these results:

- They were geolocated in two countries—nine in the U.S. and one in Singapore.
- While seven IP addresses did not have ISP data, one IP address each was administered by Hostwinds, Latitude.sh, and OVHcloud.



A query on DNS Chronicle API for the 10 IP addresses tagged as IoCs revealed that all resolved at least two domains in the past. Overall, they resolved 1,717 domains between 2019 and 2024. Take a look at three examples below.

IP ADDRESS IoC	START DATE	END DATE	NUMBER OF DOMAINS
139[.]99[.]66[.]103	26 September 2020	30 August 2023	1,000
216[.]107[.]136[.]10	27 March 2024	21 October 2024	10
45[.]61[.]128[.]122	4 September 2023	20 October 2024	19

Hidden Risk IoC List Expansion Analysis Findings

We began our search for connected threat artifacts with a WHOIS History API query for the 44 domains tagged as IoCs. The results showed that they had 30 email addresses in their historical WHOIS records. Seven of the email addresses were public.

A Reverse WHOIS API query for the seven public email addresses yielded results for four although one may belong to a domainer, given the large number of connected domains. Excluding results for that potential domainer, we obtained 40 email-connected domains after filtering out duplicates and the IoCs.

Next, a DNS Lookup API query for the 44 domains tagged as IoCs provided us with 14 additional IP addresses after removing duplicates and the IoCs.

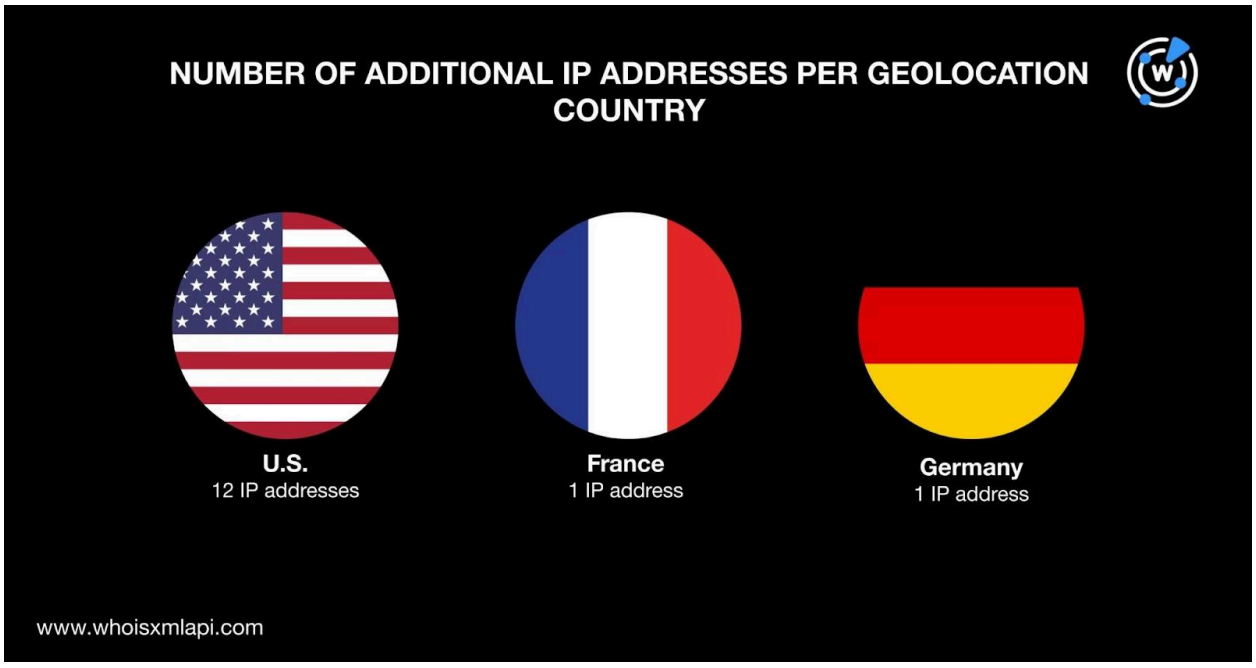
A Threat Intelligence API query for the 14 additional IP addresses revealed that 13 have already figured in malicious campaigns. Here are three examples.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT TYPES
13[.]248[.]213[.]45	Attack Command and control (C&C) Generic Malware Phishing Spam Suspicious
76[.]223[.]67[.]189	Attack C&C

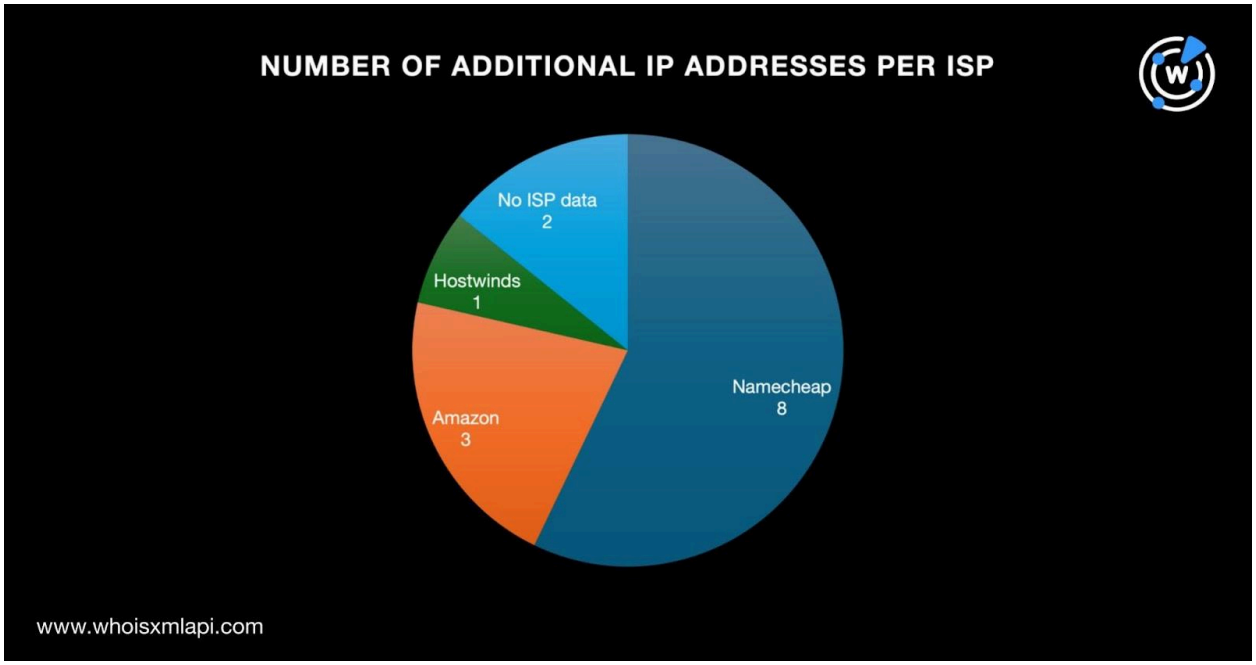
	Generic Malware Phishing Spam Suspicious
91[.]195[.]240[.]12	Attack C&C Generic Malware Phishing Spam Suspicious

A bulk IP geolocation lookup for the 14 additional IP addresses showed that:

- They were geolocated in three different countries led by the U.S., which accounted for 12 IP addresses. One IP address each was geolocated in France and Germany.



- While two IP addresses did not have ISP data, the rest were administered by three different entities. Namecheap administered eight IP addresses, Amazon managed three, and Hostwinds handled one.



A Reverse IP API query for the 24 IP addresses in total (i.e., the 10 IoCs and 14 additional IP addresses) showed that nine of them could be dedicated hosts. All in all, they hosted six new IP-connected domains after filtering out duplicates, the IoCs, and the email-connected domains.

As the final step, we trooped to Domains & Subdomains Discovery to uncover string-connected web properties. While we looked for potential connections for all strings present in the domain IoCs, only the text strings and parameters below yielded results.

DOMAIN SEARCH STRINGS AND PARAMETERS	SUBDOMAIN SEARCH STRINGS AND PARAMETERS
Starts with **cardiagnostic.**	Contains **doc** and **solanalab**
Starts with **cmt.**	Contains **info** and **customer-app**
Starts with **customer-app.**	Contains **meeting** and **zoom-client**
Starts with **delphidigital.**	Contains **xu10** and **1056**
Starts with **dns.**	
Starts with **dourolab.**	
Starts with **drogueriasanjose.**	

Starts with **edwardcaputo.**	
Starts with **frameworks.**	
Starts with **hananetwork.**	
Starts with **happyz.**	
Starts with **hostwindsdns.**	
Starts with **huspot.**	
Starts with **kevinaraujo.**	
Starts with **maelstromfund.**	
Starts with **maelstroms.**	
Starts with **matuaner.**	
Starts with **panda95sg.**	
Starts with **pixelmonmmo.**	
Starts with **presentations.**	
Starts with **prismlab.**	
Starts with **selinicapital.**	
Starts with **sendmailed.**	
Starts with **sendmailer.**	
Starts with **solanalab.**	
Starts with **zoom-client.**	

We found a total of 1,685 string-connected domains after removing duplicates, the IoCs, and the email- and IP-connected domains. Three of them turned out to be malicious according to Threat Intelligence API. An example is cmt[.]ro, which was associated with phishing.

We also discovered five string-connected subdomains.

—

Our DNS deep dive into Hidden Risk led to the discovery of 1,750 connected artifacts comprising 40 email-connected domains, 14 additional IP addresses, six IP-connected domains, 1,685 string-connected domains, and five string-connected subdomains. Sixteen of them have already figured in various malicious campaigns.

If you wish to 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

Sample Email-Connected Domains

- aaftindia[.]com
- analysislawfirmllp[.]asia
- avjbusinesspark[.]org
- bulkemaildelhiindia[.]com
- cmc-tcsnoida[.]biz
- crayon4[.]biz
- dotaeventos[.]com
- emdeewelfaresociety[.]biz
- estatebull[.]com
- fincaraizluzdarygomez[.]com
- fundacionayudanosaayudar[.]com
- gdjpcancertrust[.]com
- gyanayurveda[.]com
- holidayhaat[.]com
- ittinndelhi[.]com
- jyotishisk[.]com
- mteducare[.]biz
- nimbusadcom[.]com
- nimbusbpo[.]com
- nimbusdigitech[.]com

Sample Additional IP Addresses

- 13[.]248[.]213[.]45
- 142[.]11[.]230[.]202
- 162[.]255[.]119[.]113
- 162[.]255[.]119[.]169
- 162[.]255[.]119[.]225
- 162[.]255[.]119[.]28
- 172[.]246[.]49[.]109
- 192[.]64[.]119[.]119

Sample IP-Connected Domains

- 0pensea-io[.]com
- dal-dns-1[.]hostwinds[.]net
- ns1[.]masterns[.]com

Sample String-Connected Domains

- cardiagnostic[.]app
- cardiagnostic[.]at
- cardiagnostic[.]be
- cardiagnostic[.]bg
- cardiagnostic[.]ca
- cardiagnostic[.]ch
- cmt[.]ac
- cmt[.]ac[.]cn
- cmt[.]academy
- cmt[.]adult
- cmt[.]adv[.]br
- customer-app[.]asia
- customer-app[.]com
- customer-app[.]io
- customer-app[.]online
- customer-app[.]services
- delphidigital[.]ai
- delphidigital[.]app
- delphidigital[.]at
- delphidigital[.]ca
- delphidigital[.]co
- dns[.]5g[.]in
- dns[.]6g[.]in
- dns[.]ac
- dns[.]ac[.]cn
- dns[.]ac[.]nz
- dourolab[.]com
- dourolab[.]pt
- drogueriasanjose[.]com
- drogueriasanjose[.]com[.]co
- drogueriasanjose[.]com[.]mx
- drogueriasanjose[.]site
- drogueriasanjose[.]space
- edwardcaputo[.]com
- frameworks[.]academy
- frameworks[.]ae
- frameworks[.]africa
- frameworks[.]agency
- frameworks[.]ai
- hananetwork[.]biz
- hananetwork[.]co
- hananetwork[.]co[.]kr
- hananetwork[.]com
- hananetwork[.]live
- happyz[.]app
- happyz[.]be
- happyz[.]cc
- happyz[.]cf
- happyz[.]club
- hostwindsdns[.]co
- huspot[.]com
- huspot[.]com[.]my
- huspot[.]de
- huspot[.]my
- huspot[.]net
- kevinaraujo[.]co[.]uk
- kevinaraujo[.]com
- maelstromfund[.]com
- maelstroms[.]belau[.]pw
- maelstroms[.]business
- maelstroms[.]ca
- maelstroms[.]ch
- maelstroms[.]co[.]uk
- matuaner[.]autos
- matuaner[.]boats
- matuaner[.]cfd
- matuaner[.]cn
- matuaner[.]hair
- panda95sg[.]co
- panda95sg[.]com
- panda95sg[.]live
- panda95sg[.]net
- panda95sg[.]online
- pixelmonmmo[.]com
- pixelmonmmo[.]org
- presentations[.]academy

- presentations[.]agency
- presentations[.]ai
- presentations[.]app
- presentations[.]at
- presentations[.]audio
- prismlab[.]cc
- prismlab[.]cn
- prismlab[.]co
- prismlab[.]co[.]kr
- prismlab[.]com
- selinicapital[.]ae
- selinicapital[.]com
- sendmailed[.]net
- sendmailed[.]site
- sendmailed[.]website
- sendmailed[.]xyz
- sendmailer[.]cf
- sendmailer[.]ch
- sendmailer[.]cloud
- sendmailer[.]club
- sendmailer[.]co
- solanalab[.]com
- solanalab[.]eu
- solanalab[.]info
- solanalab[.]net
- solanalab[.]nl
- zoom-client[.]ru
- zoom-client[.]us

Sample String-Connected Subdomains

- customer-applied-pepekinfo[.]unyqxfiorc[.]com
- docs-solanalabs-com[.]translate[.]goog
- qxu1001810562[.]my3w[.]com