Jan 17 2024

NETMANAGEIT

Intelligence Report

Rimasuta New Variant Switches to ChaCha20 Encryption Algorithm

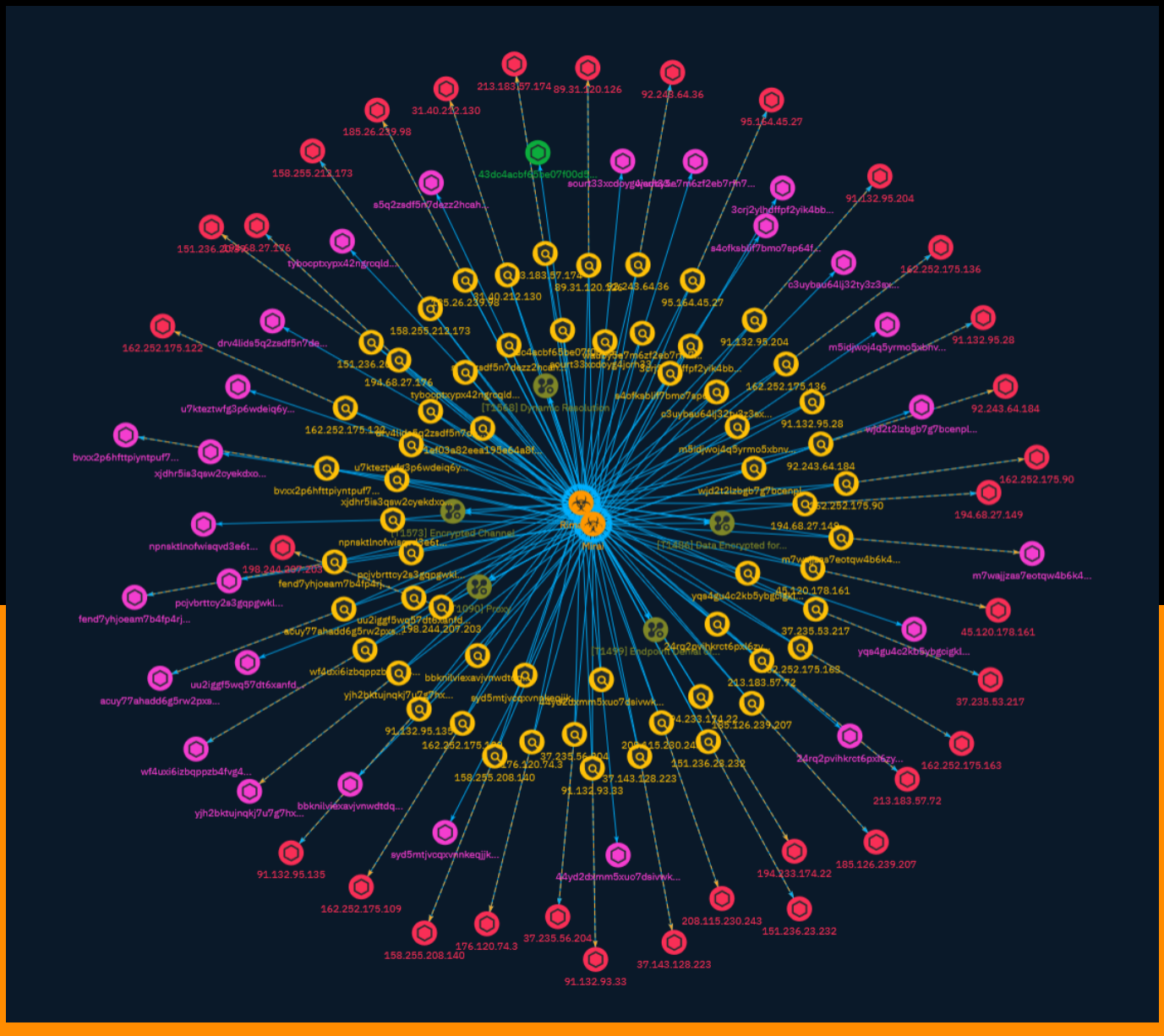

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new variant of the Mirai malware, known as Rimasuta, has recently resurfaced in samples captured by 360netlab in Japan, but has undergone a significant change in its encryption algorithm.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Encrypted Channel
ID
T1573
Description
Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.
Name
Proxy
ID
T1090
Description
Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection

through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Data Encrypted for Impact

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim

wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted. (Citation: Rhino S3 Ransomware Part 1)

Name

Endpoint Denial of Service

ID

T1499

Description

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014) An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries can target various layers of the application stack that is hosted on the system used to provide the service. These layers include the Operating Systems (OS), server applications such as web servers, DNS servers, databases, and the (typically web-based) applications that sit on top of them. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. A DoS attack may be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform DoS attacks against endpoint resources, several aspects apply to multiple methods, including IP address spoofing and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an

attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016) In cases where traffic manipulation is used, there may be points in the global network (such as high traffic gateway routers) where packets can be altered and cause legitimate clients to execute code that directs network packets toward a target in high volume. This type of capability was previously used for the purposes of web censorship where client HTTP traffic was modified to include a reference to JavaScript that generated the DDoS code to overwhelm target web servers.(Citation: ArsTechnica Great Firewall of China) For attacks attempting to saturate the providing network, see [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

Name

Dynamic Resolution

ID

T1568

Description

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

Indicator

Name

95.164.45.27

Description

- **Zip Code:** N/A - **ISP:** Stark Industries Solutions - **ASN:** 44477 - **Organization:** Stark Industries Solutions - **Is Crawler:** False - **Timezone:** Europe/Paris - **Mobile:** False - **Host:** vm1917284.stark-industries.solutions - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** FR - **Region:** le-de-France - **City:** Paris - **Latitude:** 48.83229828 - **Longitude:** 2.40750003

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.164.45.27']

Name

194.233.174.22

Description

- **Zip Code:** N/A - **ISP:** Akamai Connected Cloud - **ASN:** 63949 - **Organization:** Akamai Connected Cloud - **Is Crawler:** False - **Timezone:** Europe/Berlin - **Mobile:** False - **Host:** 194-233-174-22.ip.linodeusercontent.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** DE - **Region:** Hesse - **City:** Frankfurt am Main - **Latitude:** 50.11880112 - **Longitude:** 8.68430042

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.233.174.22']

Name

37.235.56.204

Description

- **Zip Code:** N/A - **ISP:** EDIS GmbH - **ASN:** 57169 - **Organization:** EDIS GmbH - **Is Crawler:** False - **Timezone:** Europe/Vienna - **Mobile:** False - **Host:** 204.56.235.37.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** AT - **Region:** Vienna - **City:** Vienna - **Latitude:** 48.20489883 - **Longitude:** 16.36619949

Pattern Type

stix

Pattern

[ipv4-addr:value = '37.235.56.204']

Name

194.68.27.149

Description

- **Zip Code:** N/A - **ISP:** EDIS GmbH - **ASN:** 9009 - **Organization:** EDIS GmbH - **Is Crawler:** False - **Timezone:** Asia/Tokyo - **Mobile:** False - **Host:** 149.27.68.194.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** JP - **Region:** Tokyo - **City:** Tokyo - **Latitude:** 35.68930054 - **Longitude:** 139.68989563

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.68.27.149']

Name

45.120.178.161

Description

- **Zip Code:** N/A - **ISP:** Stark Industries Solutions - **ASN:** 44477 - **Organization:** Stark Industries Solutions - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** sharduem.asiwaju.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** Drenthe - **City:** Meppel - **Latitude:** 52.69589996 - **Longitude:** 6.18470001

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.120.178.161']

Name

3crj2ylhdffpf2yik4bb2hn32xey2bdhcpykxfezb4sq53eelglp3sqd.onion

Pattern Type

stix

Pattern

[domain-name:value = '3crj2ylhdffpf2yik4bb2hn32xey2bdhcpykxfezb4sq53eelglp3sqd.onion']

Name

s4ofksblif7bmo7sp64f56gij6xzh7sznvrn46m6daup2hwdmwbiabqd.onion

Pattern Type

stix

Pattern

[domain-name:value = 's4ofksblif7bmo7sp64f56gij6xzh7sznvrn46m6daup2hwdmwbiabqd.onion']

Name

162.252.175.90

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 90.175.252.162.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Florida - **City:** Miami - **Latitude:** 25.76889992 - **Longitude:** -80.19460297

Pattern Type

stix

Pattern

[ipv4-addr:value = '162.252.175.90']

Name

yqs4gu4c2kb5ybgcigkl5gcsqbjuk5n2su2pozpsw4ojav2op5gddkid.onion

Pattern Type

stix

Pattern

[domain-name:value = 'yqs4gu4c2kb5ybgcigkl5gcsqbjuk5n2su2pozpsw4ojav2op5gddkid.onion']

Name

37.235.53.217

Description

- **Zip Code:** N/A - **ISP:** Comvive Servidores S.L. - **ASN:** 39020 - **Organization:** Speedify VPN - **Is Crawler:** False - **Timezone:** Europe/Madrid - **Mobile:** False - **Host:** 217.53.235.37.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** ES - **Region:** Andalusia - **City:** Seville - **Latitude:** 37.38410187 - **Longitude:** -5.97049999

Pattern Type

stix

Pattern

[ipv4-addr:value = '37.235.53.217']

Name

91.132.95.28

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Europe/London - **Mobile:** False - **Host:** 28.95.132.91.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** GB - **Region:** England - **City:** Poplar - **Latitude:** 51.50640106 - **Longitude:** -0.02

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.132.95.28']

Name

syd5mtjvcqxvnnkeqjjkdm2oz2jzl6swrfhnvliiemxtgiqvcbm26nyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'syd5mtjvcqxvnnkeqjjkdm2oz2jzl6swrfhnvliiemxtgiqvcbm26nyd.onion']

Name

158.255.212.173

Description

- **Zip Code:** N/A - **ISP:** EDIS - **ASN:** 57169 - **Organization:** EDIS - **Is Crawler:** False - **Timezone:** Europe/Vienna - **Mobile:** False - **Host:** 173.212.255.158.in-addr.arpa - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** AT - **Region:** Vienna - **City:** Vienna - **Latitude:** 48.20489883 - **Longitude:** 16.36619949

Pattern Type

stix

Pattern

[ipv4-addr:value = '158.255.212.173']

Name

162.252.175.109

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 109.175.252.162.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Florida - **City:** Miami - **Latitude:** 25.76889992 - **Longitude:** -80.19460297

Pattern Type

stix

Pattern

[ipv4-addr:value = '162.252.175.109']

Name

1ef03a82eea195e64a8f193fe0a50c5b78e0801f

Description

mirai_rimasuta proxy client

Pattern Type

yara

Pattern

rule mirai_rimasuta { meta: description = "mirai_rimasuta proxy client" author = "xlab" date = "2023-11-22" strings: $str_seed = {BE BA 49 48} $chacha20key = {8F EA E2 F1 84 F6 B2 A3 D8 BF F0 E9 9E F7 B2 FB} condition: all of them }

Name

m7wajjzas7eotqw4b6k4aei5q4zijdal3spsec7wsfmf2xqjhmydjiyd.onion

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** m7wajjzas7eotqw4b6k4aei5q4zijdal3spsec7wsfmf2xqjhmydjiyd.onion - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[domain-name:value = 'm7wajjzas7eotqw4b6k4aei5q4zijdal3spsec7wsfmf2xqjhmydjiyd.onion']

Name

213.183.57.174

Description

- **Zip Code:** N/A - **ISP:** Melbikomas UAB - **ASN:** 56630 - **Organization:** Speedify VPN - **Is Crawler:** False - **Timezone:** Europe/Moscow - **Mobile:** False - **Host:** 174.57.183.213.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. -

Country Code: RU - **Region:** Moscow - **City:** Moscow - **Latitude:** 55.74829865 - **Longitude:** 37.61709976

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.183.57.174']

Name

u7kteztwfg3p6wdeiq6y7zidxx3xtto4gmm2vwz42mzd6s4ixgvpgxyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'u7kteztwfg3p6wdeiq6y7zidxx3xtto4gmm2vwz42mzd6s4ixgvpgxyd.onion']

Name

fend7yhjoeam7b4fp4rj5oobphuvmhjbovhtvporusjex4nyoiamgdyd.onion

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** fend7yhjoeam7b4fp4rj5oobphuvmhjbovhtvporusjex4nyoiamgdyd.onion - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[domain-name:value = 'fend7yhjoeam7b4fp4rj5oobphuvmhjbovhtvporusjex4nyoiamgdyd.onion']

Name

acuy77ahadd6g5rw2pxsuejskirjmxaoj37ck7fvj4h4kc36a3uwirqd.onion

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** acuy77ahadd6g5rw2pxsuejskirjmxaoj37ck7fvj4h4kc36a3uwirqd.onion - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[domain-name:value = 'acuy77ahadd6g5rw2pxsuejskirjmxaoj37ck7fvj4h4kc36a3uwirqd.onion']

Name

31.40.212.130

Description

- **Zip Code:** N/A - **ISP:** BrainStorm Network - **ASN:** 136258 - **Organization:** ZoogVPN - **Is Crawler:** False - **Timezone:** America/Argentina/Buenos_Aires - **Mobile:** False - **Host:** 31.40.212.130 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** AR - **Region:** Buenos Aires F.D. - **City:** Buenos Aires - **Latitude:** -34.61759949 - **Longitude:** -58.38090134

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.40.212.130']

Name

pcjvbrttcy2s3gqpgwklgsco4u4bskr5xhvdzs4pzqqcrfllkwe437id.onion

Pattern Type

stix

Pattern

[domain-name:value = 'pcjvbrttcy2s3gqpgwklgsco4u4bskr5xhvdzs4pzqqcrfllkwe437id.onion']

Name

43dc4acbf65be07f00d53e6b2c65b572e4b43f30227aa42438e34d21ecc50acd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '43dc4acbf65be07f00d53e6b2c65b572e4b43f30227aa42438e34d21ecc50acd']

Name

158.255.208.140

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** Slick VPN - **Is Crawler:** False - **Timezone:** Asia/Hong_Kong - **Mobile:** False - **Host:** 140.208.255.158.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** HK - **Region:** Kwai Tsing - **City:** Ha Kwai Chung - **Latitude:** 22.35390091 - **Longitude:** 114.13420105

Pattern Type

stix

Pattern

[ipv4-addr:value = '158.255.208.140']

Name

bbknilviexavjvnwdtdqmhsexqcokfwgdqthxexvuwzlwgaggddaahxn.onion

Pattern Type

stix

Pattern

[domain-name:value = 'bbknilviexavjvnwdtdqmhsexqcokfwgdqthxexvuwzlwgaggddaahxn.onion']

Name

92.243.64.36

Description

- **Zip Code:** N/A - **ISP:** M247 Europe SRL - **ASN:** 9009 - **Organization:** M247 Europe SRL - **Is Crawler:** False - **Timezone:** America/Toronto - **Mobile:** False - **Host:** 36.64.243.92.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** CA - **Region:** Quebec - **City:** Montreal - **Latitude:** 45.49940109 - **Longitude:** -73.57029724

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.243.64.36']

Name

37.143.128.223

Description

- **Zip Code:** N/A - **ISP:** BrainStorm Network - **ASN:** 136258 - **Organization:** BrainStorm Network - **Is Crawler:** False - **Timezone:** America/Santiago - **Mobile:** False - **Host:** 37.143.128.223 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. -

Country Code: CL - **Region:** Santiago Metropolitan - **City:** Santiago - **Latitude:** -33.45209885 - **Longitude:** -70.6536026

Pattern Type

stix

Pattern

[ipv4-addr:value = '37.143.128.223']

Name

s5q2zsdf5n7dezz2hcah23iodsrn6gpyv6f2dxv62ikp7idntmlecvqd.onion

Pattern Type

stix

Pattern

[domain-name:value = 's5q2zsdf5n7dezz2hcah23iodsrn6gpyv6f2dxv62ikp7idntmlecvqd.onion']

Name

162.252.175.163

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 163.175.252.162.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Florida - **City:** Miami - **Latitude:** 25.76889992 - **Longitude:** -80.19460297

Pattern Type

stix

Pattern

[ipv4-addr:value = '162.252.175.163']

Name

91.132.95.135

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Europe/London - **Mobile:** False - **Host:** 135.95.132.91.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** GB - **Region:** England - **City:** Poplar - **Latitude:** 51.50640106 - **Longitude:** -0.02

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.132.95.135']

Name

151.236.20.39

Description

- **Zip Code:** N/A - **ISP:** M247 Europe SRL - **ASN:** 9009 - **Organization:** M247 Europe SRL - **Is Crawler:** False - **Timezone:** Asia/Hong_Kong - **Mobile:** False - **Host:** 39.20.236.151.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** HK - **Region:** Hong Kong - **City:** Hong Kong - **Latitude:** 22.28552055 - **Longitude:** 114.15769196

Pattern Type

stix

Pattern

[ipv4-addr:value = '151.236.20.39']

Name

176.120.74.3

Description

- **Zip Code:** N/A - **ISP:** Stark Industries Solutions - **ASN:** 44477 - **Organization:** Stark Industries Solutions - **Is Crawler:** False - **Timezone:** Europe/Madrid - **Mobile:** False - **Host:** vm1819705.stark-industries.solutions - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** ES - **Region:** Madrid - **City:** Madrid - **Latitude:** 40.41630173 - **Longitude:** -3.69339991

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.120.74.3']

Name

uu2iggf5wq57dt6xanfdmwq3rvxqorkb43bh2eacj2vz22nvwewlxcyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'uu2iggf5wq57dt6xanfdmwq3rvxqorkb43bh2eacj2vz22nvwewlxcyd.onion']

Name

89.31.120.126

Description

- **Zip Code:** N/A - **ISP:** M247 Europe SRL - **ASN:** 9009 - **Organization:** M247 Europe SRL - **Is Crawler:** False - **Timezone:** Asia/Dubai - **Mobile:** False - **Host:** 126.120.31.89.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** AE - **Region:** Dubai - **City:** Dubai - **Latitude:** 25.07309914 - **Longitude:** 55.29800034

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.31.120.126']

Name

wf4uxi6izbqppzb4fvg4sq7sm5t5w5xl5v5pkxpguwpr4aci7hvzboid.onion

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** wf4uxi6izbqppzb4fvg4sq7sm5t5w5xl5v5pkxpguwpr4aci7hvzboid.onion - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[domain-name:value = 'wf4uxi6izbqppzb4fvg4sq7sm5t5w5xl5v5pkxpguwpr4aci7hvzboid.onion']

Name

194.68.27.176

Description

- **Zip Code:** N/A - **ISP:** EDIS GmbH - **ASN:** 9009 - **Organization:** EDIS GmbH - **Is Crawler:** False - **Timezone:** Asia/Tokyo - **Mobile:** False - **Host:** 176.27.68.194.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** JP - **Region:** Tokyo - **City:** Tokyo - **Latitude:** 35.68930054 - **Longitude:** 139.68989563

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.68.27.176']

Name

151.236.23.232

Description

- **Zip Code:** N/A - **ISP:** Comvive Servidores S.L. - **ASN:** 39020 - **Organization:** Comvive Servidores S.L. - **Is Crawler:** False - **Timezone:** Europe/Madrid - **Mobile:** False - **Host:** 232.23.236.151.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** ES - **Region:** Andalusia - **City:** Seville - **Latitude:** 37.38410187 - **Longitude:** -5.97049999

Pattern Type

stix

Pattern

[ipv4-addr:value = '151.236.23.232']

Name

198.244.207.203

Description

- **Zip Code:** N/A - **ISP:** OVH SAS - **ASN:** 16276 - **Organization:** OVH SAS - **Is Crawler:** False - **Timezone:** Europe/London - **Mobile:** False - **Host:** ip203.ip-198-244-207.eu - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection

Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** GB - **Region:** England - **City:** London - **Latitude:** 51.50880051 - **Longitude:** -0.093

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.244.207.203']

Name

sourt33xcdoyg4jcrh33qvx6cjoneowihsfrbuqldkrrili54gdvryyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'sourt33xcdoyg4jcrh33qvx6cjoneowihsfrbuqldkrrili54gdvryyd.onion']

Name

44yd2dxmm5xuo7dsivwkf2fqyqmfsqkt5nkxdlgwpnbr57sca56j74yd.onion

Pattern Type

stix

Pattern

[domain-name:value = '44yd2dxmm5xuo7dsivwkf2fqyqmfsqkt5nkxdlgwpnbr57sca56j74yd.onion']

Name

yjh2bktujnqkj7u7g7hxotck6sfhjuf7crhc4vcf6ewpa7swoqalfkid.onion

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** yjh2bktujnqkj7u7g7hxotck6sfhjuf7crhc4vcf6ewpa7swoqalfkid.onion - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[domain-name:value = 'yjh2bktujnqkj7u7g7hxotck6sfhjuf7crhc4vcf6ewpa7swoqalfkid.onion']

Name

m5idjwoj4q5yrmo5xbnvhoqqrdld6pruxx5qjvr6gfnnmao4xiniwzid.onion

Pattern Type

stix

Pattern

[domain-name:value = 'm5idjwoj4q5yrmo5xbnvhoqqrdld6pruxx5qjvr6gfnnmao4xiniwzid.onion']

Name

91.132.95.204

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Europe/London - **Mobile:** False - **Host:** 204.95.132.91.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** GB - **Region:** England - **City:** Poplar - **Latitude:** 51.50640106 - **Longitude:** -0.02

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.132.95.204']

Name

c3uybau64lj32ty3z3sxgchnrmg72bvbpua66mcvydcjpgrbv2r6huyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'c3uybau64lj32ty3z3sxgchnrmg72bvbpua66mcvydcjpgrbv2r6huyd.onion']

Name

wjd2t2lzbgb7g7bcenpl2r2bsobkbwwpooqrmiwqjkpktm5p5seifcid.onion

Pattern Type

stix

Pattern

[domain-name:value = 'wjd2t2lzbgb7g7bcenpl2r2bsobkbwwpooqrmiwqjkpktm5p5seifcid.onion']

Name

213.183.57.72

Description

- **Zip Code:** N/A - **ISP:** Melbikomas UAB - **ASN:** 56630 - **Organization:** Speedify VPN - **Is Crawler:** False - **Timezone:** Europe/Moscow - **Mobile:** False - **Host:** 72.57.183.213.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** RU - **Region:** Moscow - **City:** Moscow - **Latitude:** 55.74829865 - **Longitude:** 37.61709976

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.183.57.72']

Name

92.243.64.184

Description

- **Zip Code:** N/A - **ISP:** M247 Europe SRL - **ASN:** 9009 - **Organization:** M247 Europe SRL - **Is Crawler:** False - **Timezone:** America/Toronto - **Mobile:** False - **Host:** 184.64.243.92.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** CA - **Region:** Quebec - **City:** Montreal - **Latitude:** 45.49940109 - **Longitude:** -73.57029724

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.243.64.184']

Name

185.26.239.98

Description

- **Zip Code:** N/A - **ISP:** M247 Europe SRL - **ASN:** 9009 - **Organization:** Slick VPN - **Is Crawler:** False - **Timezone:** Europe/Paris - **Mobile:** False - **Host:** 98.239.26.185.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** FR - **Region:** le-de-France - **City:** Paris - **Latitude:** 48.83229828 - **Longitude:** 2.40750003

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.26.239.98']

Name

tybocptxypx42ngrcqldrgas536syipwotmfnbjpwc5fpxth4xf4faqd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'tybocptxypx42ngrcqldrgas536syipwotmfnbjpwc5fpxth4xf4faqd.onion']

Name

208.115.230.243

Description

- **Zip Code:** N/A - **ISP:** Limestone Networks - **ASN:** 46475 - **Organization:** Limestone Networks - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 243-230-115-208.static.reverse.lstn.net - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.78087997 - **Longitude:** -96.80347443

Pattern Type

stix

Pattern

[ipv4-addr:value = '208.115.230.243']

Name

162.252.175.122

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 122.175.252.162.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Florida - **City:** Miami - **Latitude:** 25.76889992 - **Longitude:** -80.19460297

Pattern Type

stix

Pattern

[ipv4-addr:value = '162.252.175.122']

Name

wauby5e7m6zf2eb7rfn7nqm3diuaehdu6tfay4janiktgx33wjfifkyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'wauby5e7m6zf2eb7rfn7nqm3diuaehdu6tfay4janiktgx33wjfifkyd.onion']

Name

91.132.93.33

Description

- **Zip Code:** N/A - **ISP:** EDIS GmbH - **ASN:** 9009 - **Organization:** EDIS GmbH - **Is Crawler:** False - **Timezone:** Asia/Dubai - **Mobile:** False - **Host:** 33.93.132.91.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** AE - **Region:** Dubai - **City:** Dubai - **Latitude:** 25.07309914 - **Longitude:** 55.29800034

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.132.93.33']

Name

xjdhr5is3qsw2cyekdxo57gchpxusvkko3265x2lmmn4g6fnlimdngqd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'xjdhr5is3qsw2cyekdxo57gchpxusvkko3265x2lmmn4g6fnlimdngqd.onion']

Name

185.126.239.207

Description

- **Zip Code:** N/A - **ISP:** BrainStorm Network - **ASN:** 136258 - **Organization:** iProVPN - **Is Crawler:** False - **Timezone:** Europe/Moscow - **Mobile:** False - **Host:** 185.126.239.207 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** RU - **Region:** Moscow - **City:** Moscow - **Latitude:** 55.74829865 - **Longitude:** 37.61709976

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.126.239.207']

Name

npnsktlnofwisqvd3e6tpslinkypajmh5jctyjivuf6jza3syw2v6cid.onion

Pattern Type

stix

Pattern

[domain-name:value = 'npnsktlnofwisqvd3e6tpslinkypajmh5jctyjivuf6jza3syw2v6cid.onion']

Name

bvxx2p6hfttpiyntpuf72axcvaakjbz5zgiea7iklkrb2s6wrdrv4lid.onion

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp':

None, 'iso': None} - **IPQS: Domain:** bvxx2p6hfttpiyntpuf72axcvaakjbz5zgiea7iklkrb2s6wrdrv4lid.onion - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[domain-name:value = 'bvxx2p6hfttpiyntpuf72axcvaakjbz5zgiea7iklkrb2s6wrdrv4lid.onion']

Name

24rq2pvihkrct6pxl6zy3p36gt2wd6sn6izoz7ntlivxvbuu5ei3xwad.onion

Pattern Type

stix

Pattern

[domain-name:value = '24rq2pvihkrct6pxl6zy3p36gt2wd6sn6izoz7ntlivxvbuu5ei3xwad.onion']

Name

drv4lids5q2zsdf5n7dezz2hcah23iodsrn6gpyv6f2dxv62ikp7idntmlecvqd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'drv4lids5q2zsdf5n7dezz2hcah23iodsrn6gpyv6f2dxv62ikp7idntmlecvqd.onion']

Name

162.252.175.136

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 136.175.252.162.in-addr.arpa - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Florida - **City:** Miami - **Latitude:** 25.76889992 - **Longitude:** -80.19460297

Pattern Type

stix

Pattern

[ipv4-addr:value = '162.252.175.136']

Malware

Name
Mirai

Name
Rimasuta

Domain-Name

Value
yjh2bktujnqkj7u7g7hxotck6sfhjuf7crhc4vcf6ewpa7swoqalfkid.onion
wjd2t2lzbgb7g7bcenpl2r2bsobkbwwpooqrmiwqjkpktm5p5seifcid.onion
m7wajjzas7eotqw4b6k4aei5q4zijdal3spsec7wsfmf2xqjhmydjiyd.onion
bvxx2p6hfttpiyntpuf72axcvaakjbz5zgiea7iklkrb2s6wrdrv4lid.onion
3crj2ylhdffpf2yik4bb2hn32xey2bdhcpykxfezb4sq53eelglp3sqd.onion
24rq2pvihkrct6pxl6zy3p36gt2wd6sn6izoz7ntlivxvbuu5ei3xwad.onion
44yd2dxmm5xuo7dsivwkf2fqyqmfsqkt5nkxdlgwpnbr57sca56j74yd.onion
wauby5e7m6zf2eb7rfn7nqm3diuaehdu6tfay4janiktgx33wjfifkyd.onion
uu2iggf5wq57dt6xanfdmwq3rvxqorkb43bh2eacj2vz22nvwewlxcyd.onion
npnsktlnofwisqvd3e6tpslinkypajmh5jctyjivuf6jza3syw2v6cid.onion
yqs4gu4c2kb5ybgcigkl5gcsqbjuk5n2su2pozpsw4ojav2op5gddkid.onion
pcjvbrttcy2s3gqpgwklgsco4u4bskr5xhvdzs4pzqqcrfllkwe437id.onion
m5idjwoj4q5yrmo5xbnvhoqqrdld6pruxx5qjvr6gfnnmao4xiniwzid.onion

syd5mtjvcqxvnnkeqjjkdm2oz2jzl6swrfhnvliiemxtgiqvcbm26nyd.onion

wf4uxi6izbqppzb4fvg4sq7sm5t5w5xl5v5pkxpguwpr4aci7hvzboid.onion

sourt33xcdoyg4jcrh33qvx6cjoneowihsfrbuqldkrrili54gdvryyd.onion

acuy77ahadd6g5rw2pxsuejskirjmxaoj37ck7fvj4h4kc36a3uwirqd.onion

tybocptxypx42ngrcqldrgas536syipwotmfnbjpwc5fpxth4xf4faqd.onion

c3uybau64lj32ty3z3sxgchnrmg72bvbpua66mcvydcjpgrbv2r6huyd.onion

u7kteztwfg3p6wdeiq6y7zidxx3xtto4gmm2vwz42mzd6s4ixgvpgxyd.onion

s5q2zsdf5n7dezz2hcah23iodsrn6gpyv6f2dxv62ikp7idntmlecvqd.onion

xjdhr5is3qsw2cyekdxo57gchpxusvkko3265x2lmmn4g6fnlimdngqd.onion

fend7yhjoeam7b4fp4rj5oobphuvmhjbovhtvporusjex4nyoiamgdyd.onion

s4ofksblif7bmo7sp64f56gij6xzh7sznvrn46m6daup2hwdmwbiabqd.onion

bbknilviexavjvnwdtdqmhsexqcokfwgdqthxexvuwzlwgaggddaahxn.onion

drv4lids5q2zsdf5n7dezz2hcah23iodsrn6gpyv6f2dxv62ikp7idntmlecvqd.onion

StixFile

Value
43dc4acbf65be07f00d53e6b2c65b572e4b43f30227aa42438e34d21ecc50acd

IPv4-Addr

Value
194.233.174.22
176.120.74.3
198.244.207.203
91.132.93.33
92.243.64.36
92.243.64.184
162.252.175.109
95.164.45.27
151.236.23.232
151.236.20.39
194.68.27.149
208.115.230.243
162.252.175.122

37.235.53.217
89.31.120.126
91.132.95.204
185.126.239.207
194.68.27.176
162.252.175.90
91.132.95.135
213.183.57.174
162.252.175.163
158.255.212.173
162.252.175.136
37.235.56.204
185.26.239.98
45.120.178.161
158.255.208.140
91.132.95.28
37.143.128.223
31.40.212.130

213.183.57.72

External References

- https://otx.alienvault.com/pulse/65a50abee199d553d8817cb0
- https://blog.xlab.qianxin.com/rimasuta-new-variant-switches-to-chacha20-encryption-en/