Feb 03 2024

NETMANAGEIT

Intelligence Report

Trigona Ransomware Threat Actor Uses Mimic Ransomware

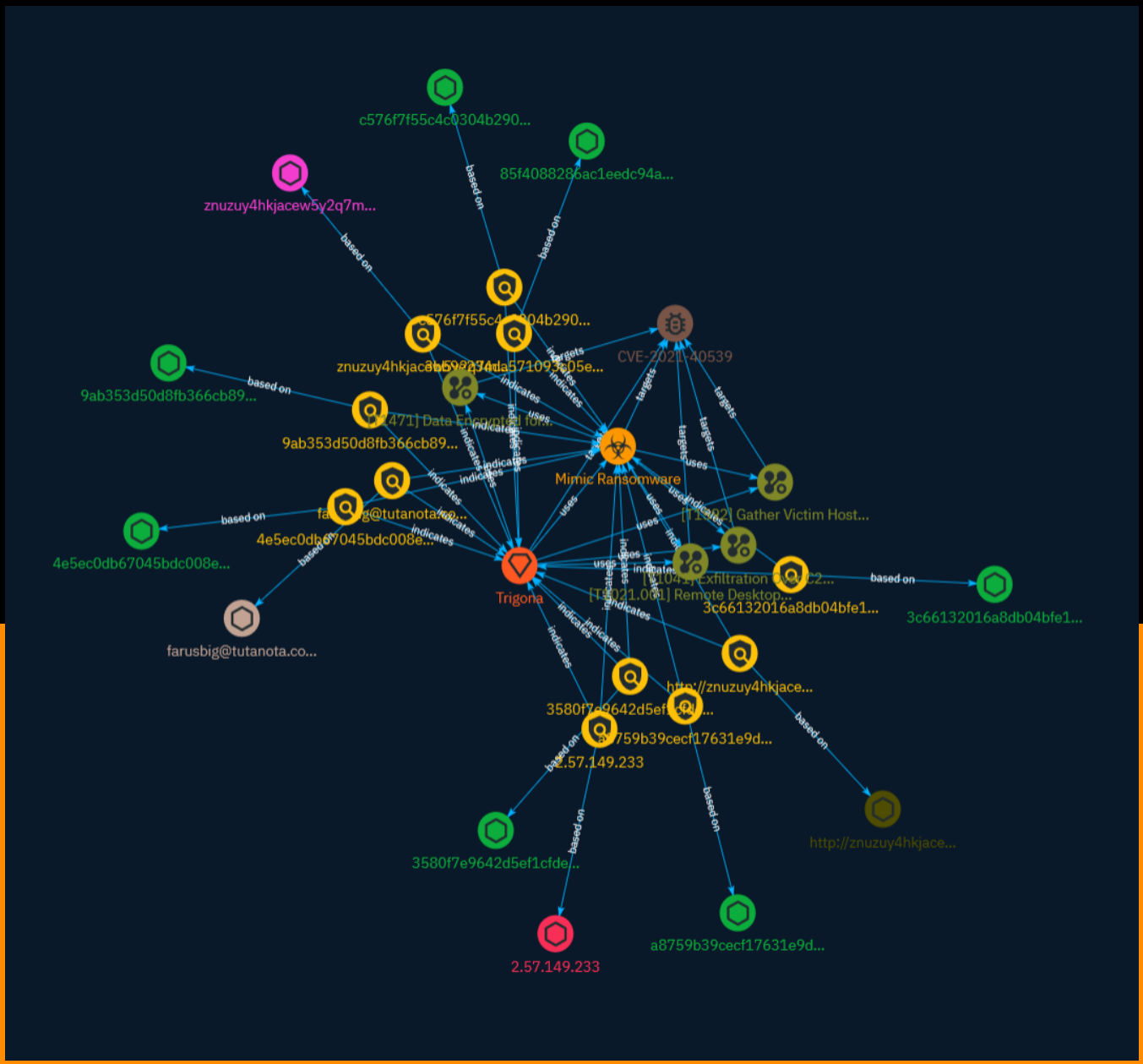

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new case of Trigona ransomware installing Mimic ransomware has been detected by AhnLab SEcurity intelligence Center, and it is believed to be the same attacker responsible for previous attacks.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

farusbig@tutanota.com

Description

- **Valid:** True - **Disposable:** False - **SMTP Score:** 3 - **Overall Score:** 4 - **First Name:** Unknown - **Generic:** False - **Common:** True - **DNS Valid:** True - **Honeypot:** False - **Deliverability:** medium - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** farusbig@tutanota.com - **Domain Age:** {'human': '12 years ago', 'timestamp': 1322671966, 'iso': '2011-11-30T11:52:46-05:00'} - **First Seen:** {'human': '11 months ago', 'timestamp': 1678248292, 'iso': '2023-03-07T23:04:52-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'farusbig@tutanota.com']

Name

znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion']

Name

http://znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion/

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion/']

Name

2.57.149.233

Description

- **Zip Code:** N/A - **ISP:** Red Byte - **ASN:** 208312 - **Organization:** Red Byte - **Is Crawler:** False - **Timezone:** Europe/Warsaw - **Mobile:** False - **Host:** 2.57.149.233 - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium

required. - **Abuse Velocity:** Premium required. - **Country Code:** PL - **Region:** Lesser Poland - **City:** Krakow - **Latitude:** 50.05849838 - **Longitude:** 19.93420029

Pattern Type

stix

Pattern

[ipv4-addr:value = '2.57.149.233']

Name

c576f7f55c4c0304b290b15e70a638b037df15c69577cd6263329c73416e490e

Description

autoit SHA256 of ac34ba84a5054cd701efad5dd14645c9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c576f7f55c4c0304b290b15e70a638b037df15c69577cd6263329c73416e490e']

Name

a8759b39cecf17631e9d4952aecd32ce233e01d08841178e7ef81f3afdd8e455

Description

GamaredonPteranodon_SFX SHA256 of 6d44f8f3c1608e5958b40f9c6d7b6718

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8759b39cecf17631e9d4952aecd32ce233e01d08841178e7ef81f3afdd8e455']

Name

9ab353d50d8fb366cb898ffaba2a71b1ae772475d1ad550232d6416b15fd3b54

Description

case_4485_ekix4 SHA256 of b3c8d81d6f8d19e5c07e1ca7932ed5bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ab353d50d8fb366cb898ffaba2a71b1ae772475d1ad550232d6416b15fd3b54']

Name

4e5ec0db67045bdc008e949214bea81a5d1e4c1e0de211159f0e9d7d33ecbf7a

Description

ConventionEngine_Term_Users SHA256 of a24bac9071fb6e07e13c52f65a093fce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4e5ec0db67045bdc008e949214bea81a5d1e4c1e0de211159f0e9d7d33ecbf7a']

Name

3c66132016a8db04bfe12363253ec78e8f8ad8b187c5aa1fea6e3bf551634f6e

Description

GamaredonPteranodon_SFX SHA256 of d6b4b1b6b0ec1799f57142798c5daf5b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c66132016a8db04bfe12363253ec78e8f8ad8b187c5aa1fea6e3bf551634f6e']

Name

3580f7e9642d5ef1cfde3d7c2379e5a7a00169ddf95d9ddbec0d2e681e9ae0fd

Description

ConventionEngine_Term_Users SHA256 of 3e26e778a4d28003686596f988942646

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3580f7e9642d5ef1cfde3d7c2379e5a7a00169ddf95d9ddbec0d2e681e9ae0fd']

Name

3bb9e234da571093c05e21b4ffdfa7ceb9d6f95a33a07e39260a974fdc19dfc7ba72e7f9a579ec45585857d5d543ff99a535b479cf77629858c3cfa1c824e46f

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '85f4088286ac1eedc94ad9dc6465e9e4b89d1cde3012f9949450fcc9f2b60431']

Name

farusbig@tutanota.com

Description

- **Valid:** True - **Disposable:** False - **SMTP Score:** 3 - **Overall Score:** 4 - **First Name:** Unknown - **Generic:** False - **Common:** True - **DNS Valid:** True - **Honeypot:** False - **Deliverability:** medium - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** farusbig@tutanota.com - **Domain Age:** {'human': '12 years ago', 'timestamp':

1322671966, 'iso': '2011-11-30T11:52:46-05:00'} - **First Seen:** {'human': '11 months ago', 'timestamp': 1678248292, 'iso': '2023-03-07T23:04:52-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'farusbig@tutanota.com']

Name

znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion']

Name

http://znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion/

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion/']

Name

2.57.149.233

Description

- **Zip Code:** N/A - **ISP:** Red Byte - **ASN:** 208312 - **Organization:** Red Byte - **Is Crawler:** False - **Timezone:** Europe/Warsaw - **Mobile:** False - **Host:** 2.57.149.233 - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** PL - **Region:** Lesser Poland - **City:** Krakow - **Latitude:** 50.05849838 - **Longitude:** 19.93420029

Pattern Type

stix

Pattern

[ipv4-addr:value = '2.57.149.233']

Name

c576f7f55c4c0304b290b15e70a638b037df15c69577cd6263329c73416e490e

Description

autoit SHA256 of ac34ba84a5054cd701efad5dd14645c9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c576f7f55c4c0304b290b15e70a638b037df15c69577cd6263329c73416e490e']

Name

a8759b39cecf17631e9d4952aecd32ce233e01d08841178e7ef81f3afdd8e455

Description

GamaredonPteranodon_SFX SHA256 of 6d44f8f3c1608e5958b40f9c6d7b6718

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8759b39cecf17631e9d4952aecd32ce233e01d08841178e7ef81f3afdd8e455']

Name

9ab353d50d8fb366cb898ffaba2a71b1ae772475d1ad550232d6416b15fd3b54

Description

case_4485_ekix4 SHA256 of b3c8d81d6f8d19e5c07e1ca7932ed5bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ab353d50d8fb366cb898ffaba2a71b1ae772475d1ad550232d6416b15fd3b54']

Name

4e5ec0db67045bdc008e949214bea81a5d1e4c1e0de211159f0e9d7d33ecbf7a

Description

ConventionEngine_Term_Users SHA256 of a24bac9071fb6e07e13c52f65a093fce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4e5ec0db67045bdc008e949214bea81a5d1e4c1e0de211159f0e9d7d33ecbf7a']

Name

3c66132016a8db04bfe12363253ec78e8f8ad8b187c5aa1fea6e3bf551634f6e

Description

GamaredonPteranodon_SFX SHA256 of d6b4b1b6b0ec1799f57142798c5daf5b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c66132016a8db04bfe12363253ec78e8f8ad8b187c5aa1fea6e3bf551634f6e']

Name

3580f7e9642d5ef1cfde3d7c2379e5a7a00169ddf95d9ddbec0d2e681e9ae0fd

Description

ConventionEngine_Term_Users SHA256 of 3e26e778a4d28003686596f988942646

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3580f7e9642d5ef1cfde3d7c2379e5a7a00169ddf95d9ddbec0d2e681e9ae0fd']

Name

3bb9e234da571093c05e21b4ffdfa7ceb9d6f95a33a07e39260a974fdc19dfc7ba72e7f9a579ec45585857d5d543ff99a535b479cf77629858c3cfa1c824e46f

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '85f4088286ac1eedc94ad9dc6465e9e4b89d1cde3012f9949450fcc9f2b60431']

Malware

Name
Mimic Ransomware

Name
Mimic Ransomware

Intrusion-Set

Name
Trigona

Name
Trigona

Vulnerability

Name
CVE-2021-40539
Description
Zoho ManageEngine ADSelfService Plus contains an authentication bypass vulnerability affecting the REST API URLs which allow for remote code execution.
Name
CVE-2021-40539
Description
Zoho ManageEngine ADSelfService Plus contains an authentication bypass vulnerability affecting the REST API URLs which allow for remote code execution.

Attack-Pattern

Name
Remote Desktop Protocol
ID
T1021.001
Description
Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services) Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)
Name
Exfiltration Over C2 Channel
ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Name

Data Encrypted for Impact

ID

T1471

Description

An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. 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.

Name

Gather Victim Host Information

ID

T1592

Description

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). Adversaries may gather this

information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Name

Remote Desktop Protocol

ID

T1021.001

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services) Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Name

Data Encrypted for Impact

ID

T1471

Description

An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. 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.

Name

Gather Victim Host Information

ID

T1592

Description

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Email-Addr

Value
farusbig@tutanota.com
farusbig@tutanota.com

Domain-Name

Value
znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion
znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion

Url

Value
http://znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion/
http://znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd.onion/

IPv4-Addr

Value
2.57.149.233

2.57.149.233

StixFile

Value
c576f7f55c4c0304b290b15e70a638b037df15c69577cd6263329c73416e490e
a8759b39cecf17631e9d4952aecd32ce233e01d08841178e7ef81f3afdd8e455
9ab353d50d8fb366cb898ffaba2a71b1ae772475d1ad550232d6416b15fd3b54
85f4088286ac1eedc94ad9dc6465e9e4b89d1cde3012f9949450fcc9f2b60431
4e5ec0db67045bdc008e949214bea81a5d1e4c1e0de211159f0e9d7d33ecbf7a
3c66132016a8db04bfe12363253ec78e8f8ad8b187c5aa1fea6e3bf551634f6e
3580f7e9642d5ef1cfde3d7c2379e5a7a00169ddf95d9ddbec0d2e681e9ae0fd
c576f7f55c4c0304b290b15e70a638b037df15c69577cd6263329c73416e490e
a8759b39cecf17631e9d4952aecd32ce233e01d08841178e7ef81f3afdd8e455
9ab353d50d8fb366cb898ffaba2a71b1ae772475d1ad550232d6416b15fd3b54
85f4088286ac1eedc94ad9dc6465e9e4b89d1cde3012f9949450fcc9f2b60431
4e5ec0db67045bdc008e949214bea81a5d1e4c1e0de211159f0e9d7d33ecbf7a
3c66132016a8db04bfe12363253ec78e8f8ad8b187c5aa1fea6e3bf551634f6e

3580f7e9642d5ef1cfde3d7c2379e5a7a00169ddf95d9ddbec0d2e681e9ae0fd

External References

- https://asec.ahnlab.com/en/61000/
- https://otx.alienvault.com/pulse/65bcc56a0c2cff1bf11ba75a