Jul 03 2023

NETMANAGEIT

Intelligence Report

An Overview of the Different Versions of the Trigona Ransomware

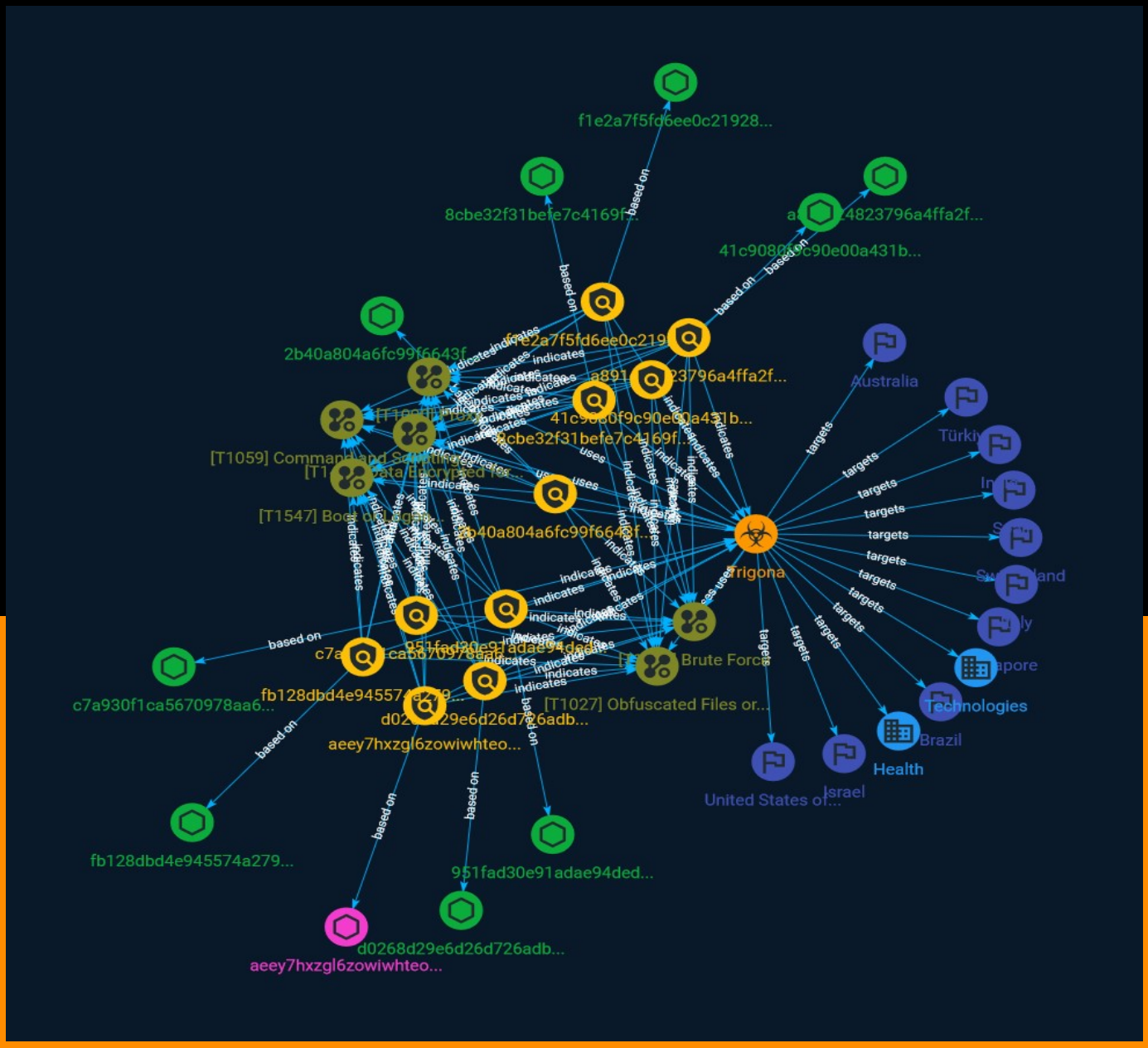

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Trigona ransomware is a relatively new ransomware family that began activities around late October 2022 — although samples of it existed as early as June 2022. Since then, Trigona's operators have remained highly active, and in fact have been continuously updating their ransomware binaries.

Confidence

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

15 / 100

Indicator

Name
d0268d29e6d26d726adb848eff991754486880ebfd7afffb3bb2a9e91a1dbb7c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd0268d29e6d26d726adb848eff991754486880ebfd7afffb3bb2a9e91a1dbb7c']
Name
f1e2a7f5fd6ee0c21928b1cae6e66724c4537052f8676feeaa18e84cf3c0c663
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f1e2a7f5fd6ee0c21928b1cae6e66724c4537052f8676feeaa18e84cf3c0c663']
Name

c7a930f1ca5670978aa6d323d16c03a97d897c77f5cff68185c8393830a6083f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7a930f1ca5670978aa6d323d16c03a97d897c77f5cff68185c8393830a6083f']

Name

2b40a804a6fc99f6643f8320d2668ebd2544f34833701300e34960b048485357

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b40a804a6fc99f6643f8320d2668ebd2544f34833701300e34960b048485357']

Name

a891d24823796a4ffa2fac76d92fec2c7ffae1ac1c3665be0d4f85e13acd33f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a891d24823796a4ffa2fac76d92fec2c7ffae1ac1c3665be0d4f85e13acd33f9']

Name

aeey7hxzgl6zowiwhteo5xjbf6sb36tkbn5hptykgmbsjrbiygv4c4id.onion

Pattern Type

stix

Pattern

[domain-name:value = 'aeey7hxzgl6zowiwhteo5xjbf6sb36tkbn5hptykgmbsjrbiygv4c4id.onion']

Name

951fad30e91adae94ded90c60b80d29654918f90e76b05491b014b8810269f74

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '951fad30e91adae94ded90c60b80d29654918f90e76b05491b014b8810269f74']

Name

8cbe32f31befe7c4169f25614afd1778006e4bda6c6091531bc7b4ff4bf62376

Description

Delphi

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8cbe32f31befe7c4169f25614afd1778006e4bda6c6091531bc7b4ff4bf62376']

Name

fb128dbd4e945574a2795c2089340467fcf61bb3232cc0886df98d86ff328d1b

Description

Delphi

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fb128dbd4e945574a2795c2089340467fcf61bb3232cc0886df98d86ff328d1b']

Name

41c9080f9c90e00a431b2fb04b461584abe68576996379a97469a71be42fc6ff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41c9080f9c90e00a431b2fb04b461584abe68576996379a97469a71be42fc6ff']

Malware

Name
Trigona

Country

Name
Switzerland
Name
Türkiye
Name
Singapore
Name
Israel
Name
Spain
Name
Brazil
Name
Australia

Name
Italy
Name
India
Name
United States of America

Sector

Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Attack-Pattern

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
Brute Force
ID
T1110
Description
Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via

interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

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

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly

benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Domain-Name

Value
aeey7hxzgl6zowiwhteo5xjbf6sb36tkbn5hptykgmbsjrbiygv4c4id.onion

StixFile

Value
951fad30e91adae94ded90c60b80d29654918f90e76b05491b014b8810269f74
8cbe32f31befe7c4169f25614afd1778006e4bda6c6091531bc7b4ff4bf62376
a891d24823796a4ffa2fac76d92fec2c7ffae1ac1c3665be0d4f85e13acd33f9
fb128dbd4e945574a2795c2089340467fcf61bb3232cc0886df98d86ff328d1b
2b40a804a6fc99f6643f8320d2668ebd2544f34833701300e34960b048485357
41c9080f9c90e00a431b2fb04b461584abe68576996379a97469a71be42fc6ff
c7a930f1ca5670978aa6d323d16c03a97d897c77f5cff68185c8393830a6083f
f1e2a7f5fd6ee0c21928b1cae6e66724c4537052f8676feeaa18e84cf3c0c663
d0268d29e6d26d726adb848eff991754486880ebfd7afffb3bb2a9e91a1dbb7c

External References

- https://otx.alienvault.com/pulse/64a2e5d062000ad64ecc27fb
- https://www.trendmicro.com/en_us/research/23/f/an-overview-of-the-trigona-ransomware.html