Jul 03 2023

NETMANAGEIT

Intelligence Report

Decrypted: Akira Ransomware

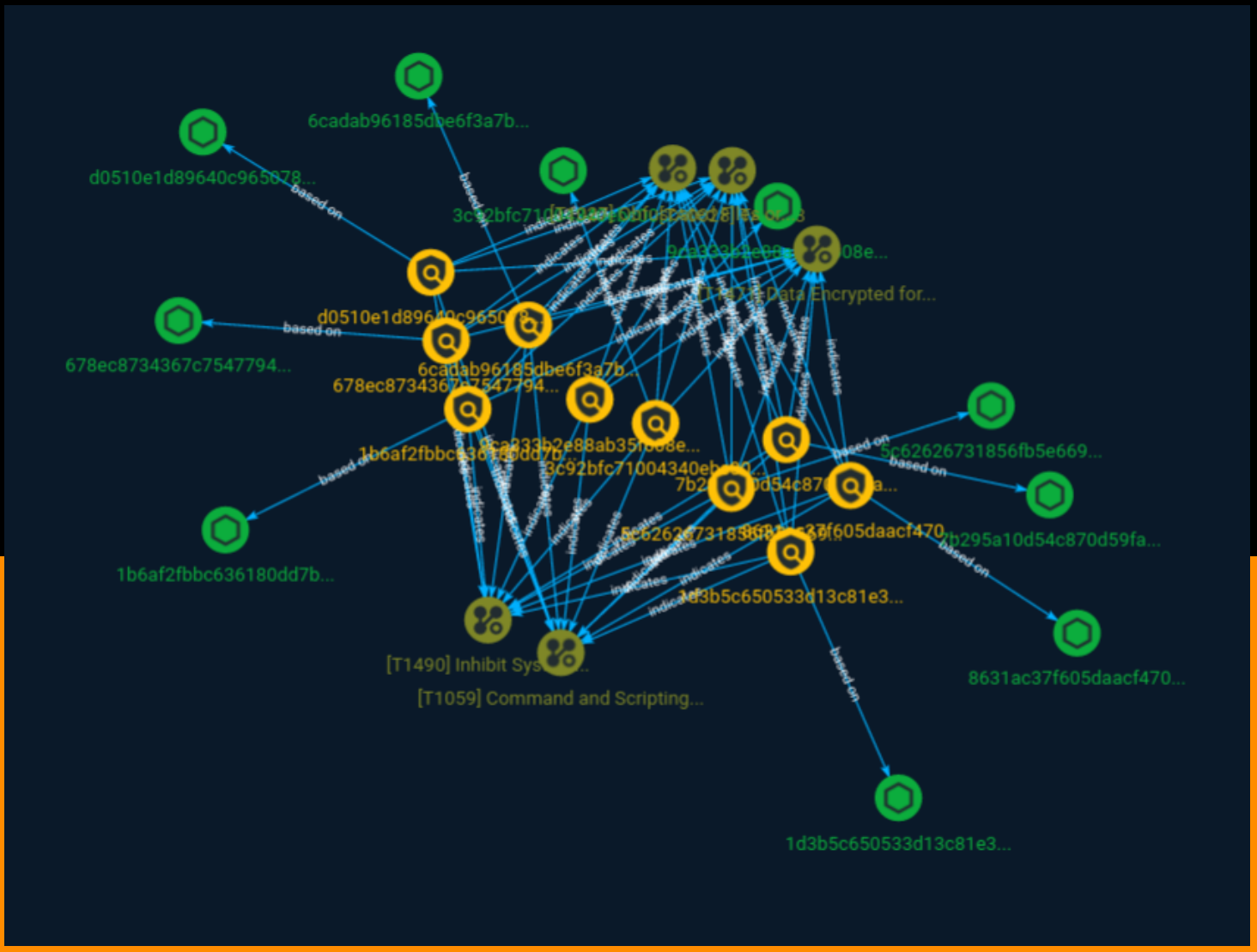

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers for Avast have developed a decryptor for the Akira ransomware and released it for public download. The Akira ransomware appeared in March 2023 and since then, the gang claims successful attacks on various organizations in the education, finance and real estate industries, amongst others.

Confidence

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

15 / 100

Indicator

Name
6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360']
Name
678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33']
Name

7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488']

Name

5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5']

Name

1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc']

Name

8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50']

Name

3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c']

Name

d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959']

Name

1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296']

Name

9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163']

Attack-Pattern

Name
TA0028
ID
TA0028
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
Inhibit System Recovery

ID

T1490

Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact] (https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot] (https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

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)

StixFile

Value
8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50
d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959
9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163
1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc
3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c
7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488
678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
5c626267318 56fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5
1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296
6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360

External References

- https://otx.alienvault.com/pulse/64a322848154907ed36d8aa6
- https://decoded.avast.io/threatresearch/decrypted-akira-ransomware/