Quorum Cyber

Threat Intelligence
Akira Ransomware

TLP Status: CLEAR

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
0.1	07/06/2023	Initial Report Drafted.
1.1		PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
	dd/mm/yyyy	

Akira Ransomware

Overview

Akira ransomware is a strain of ransomware that emerged in March 2023 and has since targeted various industry sectors, including education, finance, real estate, manufacturing, and consulting.

The ransomware deletes shadow volume copies on victim devices via a PowerShell command prior to encrypting victim files and adding the '.akira' file extension. Akira uses the Windows Restart Manager application programming interface (API) to terminate processes or shut down Windows services that keep files open so as not to interfere with encryption. Prior to encryption, Akira steals corporate data from its victims to use as leverage in negotiations for unlocking encrypted files later. The malware gains initial access to systems through various means, including search engine optimisation (SEO) poisoning or malvertising.

Akira's ransom notes contain 'akira_readme.txt' files that contain links to Akira's ransomware extortion blog and instructions on how victims can negotiate the release of their files.

The ransomware exploited at least 16 victims within the first two months of its existence. Akira ransomware operators use a unique negotiation system and host a TOR-based (.onion) website where victims are listed along with any stolen data, should a victim fail to comply with the ransom demands.

Impact

Successful exploitation by Akira ransomware will almost certainly result in the encryption and exfiltration of significant quantities of data held on the compromised system, prior to a ransom of a predetermined value being issued. The ransom amount demanded will almost certainly depend on the estimated value of the compromised organisation. Furthermore, such a compromise of data will also result in the organisation incurring a negative reputational impact. Encrypted data may include private customer data, corporate finance data and system credentials that if released can assist threat actors with future attacks.

Incident Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against ransomware threats like that implemented by the Akira ransomware. EDR solutions can alert system users of potential breaches and stop further progress before the malware can do significant damage.

If an EDR solution is not being used, the first instance of detection is likely to be the ransom note. The note will be labelled with the following file extension: akira_readme.txt.

Targeted Products

Windows OS.

Containment, Mitigations & Remediations

As mentioned previously, a primary method of reducing the threat of Akira ransomware is to detect it in the early stages through the use of an effective and monitored EDR solution. An effective EDR tool such as the Microsoft Defender suite will block ransomware attempts once detected.

Organisations can also perform routine back-ups of sensitive data that is required for business operations and to keep a copy offline in case back-ups are impacted by the attack. Therefore, if a breach occurs and the business can no longer function, a back-up is ready to use, and the business can continue to operate with minimal disruption.

Indicators of Compromise

Akira Ransomware Associated File Hash (SHA256):

9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163

Threat Group

The Akira ransomware group is a threat actor that has been active since at least April 2023. The group uses the double-extortion technique of stealing data and threatening to leak it if the ransom is not paid. The most common tactics, techniques and procedures (TTPs) used by the group include the use of PowerShell to delete Windows Shadow Volume Copies and the encryption of files found in certain folders. The group operates a dark web extortion blog, which displays the names of victim organisations. The most notorious events involving the group include attacks against New World Travel and the Perry Law Firm LLC.

Threat Landscape

Ransomware continues to be one of the prominent threats facing the private sector. Recent attacks and the developing nature of the ransomware threat landscape suggests that the threat is growing as criminal groups are becoming more comfortable demanding ever-increasing ransom fees.

Due to the significant number of targets within the first two months of its existence, it is likely that Akira ransomware will continue to exploit victims at a high frequency and as such will emerge into an increasingly notorious ransomware strain.

Mitre Methodologies

Initial Access

T1078 - Valid Accounts[1]

T1133 - External Remote Services[2]

[1] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®

[2] External Remote Services, Technique T1133 - Enterprise | MITRE ATT&CK®

Execution

T1047 - Windows Management Instrumentation[3]

T1053.005 - Scheduled Task[4]

T1059.001 - Command and Scripting Interpreter: PowerShell[5]

Persistence

T1053.005 - Scheduled Task[6]

T1078 - Valid Accounts[7]

T1133 - External Remote Services[8]

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder[9]

Privilege Escalation

T1053.005 - Scheduled Task[10]

T1078 - Valid Accounts[11]

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder[12]

Defence Evasion

T1036.004 - Masquerading: Masquerade Task or Service[13]

T1078 - Valid Accounts[14]

T1497.001 - Virtualization/Sandbox Evasion: System Checks[15]

T1497.003 - Virtualization/Sandbox Evasion: Time Based Evasion[16]

T1562.001 - Impair Defenses: Disable or Modify Tools[17]

Credential Access

T1003.001 - OS Credential Dumping: LSASS Memory[18]

---

[3] Windows Management Instrumentation, Technique T1047 - Enterprise | MITRE ATT&CK®
[4] Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®
[5] Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®
[6] Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®
[7] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®
[8] External Remote Services, Technique T1133 - Enterprise | MITRE ATT&CK®
[9] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[10] Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®
[11] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®
[12] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[13] Masquerading: Masquerade Task or Service, Sub-technique T1036.004 - Enterprise | MITRE ATT&CK®
[14] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®
[15] Virtualization/Sandbox Evasion: System Checks, Sub-technique T1497.001 - Enterprise | MITRE ATT&CK®
[16] Virtualization/Sandbox Evasion: Time Based Evasion, Sub-technique T1497.003 - Enterprise | MITRE ATT&CK®
[17] Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®
[18] OS Credential Dumping: LSASS Memory, Sub-technique T1003.001 - Enterprise | MITRE ATT&CK®

Discovery

T1018 - Remote System Discovery[19]

T1057 - Process Discovery[20]

T1082 - System Information Discovery[21]

T1083 - File and Directory Discovery[22]

T1217 - Browser Information Discovery[23]

T1497.001 - Virtualization/Sandbox Evasion: System Checks[24]

T1497.003 - Virtualization/Sandbox Evasion: Time Based Evasion[25]

Collection

T1005 - Data from Local System[26]

Command and Control

T1219 - Remote Access Software[27]

Impact

T1486 - Data Encrypted for Impact[28]

T1490 - Inhibit System Recovery[29]

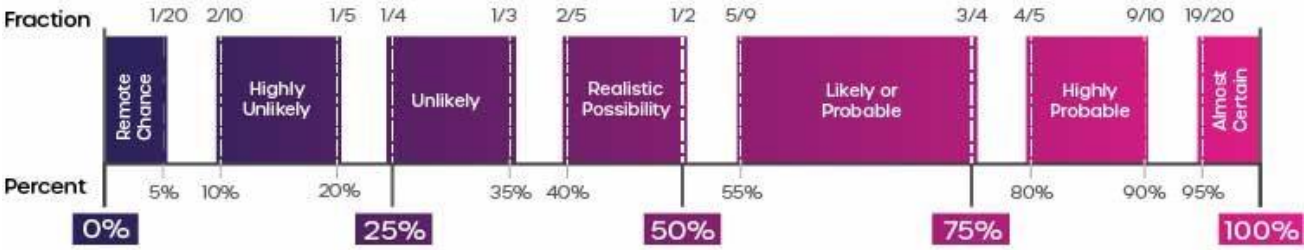
Further Information

- PCrisk Akira Ransomware Analysis

Intelligence Cut-off Date (ICoD): 07/06/2023 10:00 UTC

[19] Remote System Discovery, Technique T1018 - Enterprise | MITRE ATT&CK®
[20] Process Discovery, Technique T1057 - Enterprise | MITRE ATT&CK®
[21] System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
[22] File and Directory Discovery, Technique T1083 - Enterprise | MITRE ATT&CK®
[23] Browser Information Discovery, Technique T1217 - Enterprise | MITRE ATT&CK®
[24] Virtualization/Sandbox Evasion: System Checks, Sub-technique T1497.001 - Enterprise | MITRE ATT&CK®
[25] Virtualization/Sandbox Evasion: Time Based Evasion, Sub-technique T1497.003 - Enterprise | MITRE ATT&CK®
[26] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®
[27] Remote Access Software, Technique T1219 - Enterprise | MITRE ATT&CK®
[28] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®
[29] Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®

Intelligence Terminology Yardstick



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events