ADVISORY FOR ICM SECTORS

Akira Ransomware Pivoting Back to Double Extortion

Original report published on: Oct 21, 2024

Executive Summary

Cisco Talos published the evolution of Akira ransomware operator and its impact on various systems. The operator constantly evolves the ransomware operation and adapts to new vulnerabilities. The ransomware targets Windows and Linux systems and has been observed to use a variety of techniques to gain initial access to networks. Cisco Talos assessed throughout 2024 that Akira targeted a significant number of victims, with a clear preference for organisations in the manufacturing and professional, scientific, and technical services sectors, based on Cisco Talos' analysis of Akira's data leak site.

Background

Akira ransomware witnessed a surge in 2024, leveraging a range of vulnerabilities to compromise networks and deploy the ransomware. Initial access was often gained through exploited network appliances like SonicWall SonicOS (CVE-2024-40766), Cisco ASA and FTD (CVE-2020-3259 and CVE-2023-20263), and FortiClientEMS (CVE-2023-48788).

Once initial access is established, the attackers will leverage PowerShell scripts for credential harvesting and privilege escalation, targeting systems like Veeam backup servers (CVE-2023-27532) disclosed in September 2024 and VMware ESXi (CVE-2024-37085) in June 2024. Techniques to delete shadow copies and disable security tools to hinder recovery efforts will be used.

In early September 2024, Cisco Talos identified new C++-based ransomware samples that encrypt files with the ".akira" extension and drop a ransom note titled "akira_readme.txt". This aligns with pre-August 2023 Akira ransomware tactics, suggesting a strategic shift toward proven techniques. This observation matches with public reports on the group's initial Linux variant, indicating a calculated return to effective methods.

Akira's shift to pure data-theft extortion in late 2023 and early 2024 could been a temporary measure during code refactoring period. This allowed them to sustain pressure on victims and revenue generation while focusing on enhancing the encryptor's capabilities.

Based on Cisco Talos' analysis, Akira will likely continue to target VMWare ESXi and Linux systems throughout 2024, reflecting a broader industry trend. Adversaries are drawn to these platforms due to widespread usage in enterprise infrastructure, hosting critical systems and valuable data. Ransomware attacks targeting ESXi hypervisors are highly disruptive due to virtualisation's critical role in large-scale cloud deployments. Encrypting the ESXi environment, attackers can rapidly encrypt vast amounts of data without extensive lateral movement or credential theft. The lack of comprehensive security protection on many ESXi hypervisors becomes attractive targets for ransomware operators.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Ensure multi-factor authentication (MFA) is enabled, especially on critical accounts.
- Deploy privileged access management (PAM) to manage and monitor privilege accounts & password with authorised usage within a limited approved period.
- Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to identify malicious activity.
- Perform network segmentation with bastion (jump) host as an intermediary gateway for access into servers.
- Implement proper network access control to only allow authorised users to connect your CII/enterprise networks.
- Deploy Endpoint Detection and Response (EDR) solutions to monitor endpoint behaviour for signs of malicious activity, such as file encryption, unusual process execution, and network anomalies.
- Corelate security events and create alerts for suspicious activity, such as mass file encryption, unusual login attempts and failed authentication attempts.
- Regularly scan system for vulnerabilities and apply security patches promptly when available, especially for critical systems.
- Maintain regular backups of critical data. The 3-2-1 backup rule is a data protection strategy that involves making three copies of data, storing them on two different media types, and keeping one copy offsite/offline.

Notable MITRE ATT&CK Tactics and Techniques

Tactic	Technique
Initial Access	T1133 – External Remote Services
	T1190 – Exploit Public-Facing Application
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell
Persistence	T1136.001 – Create Account: Local Account
Privilege Escalation	T1068 – Exploitation for Privilege Escalation
	T1078 – Valid Accounts
Defence Evasion	T1027.001 – Obfuscated Files or Information: Binary Padding
	T1036.005 – Masquerading: Match Legitimate Name or Location
	T1562.001 – Impair Defences: Disable or Modify Tools
Credential Access	T1003 – OS Credential Dumping
Lateral Movement	T1021.001 – Remote Services: Remote Desktop Protocol
	T1570 – Lateral Tool Transfer
Impact	T1485 – Data Destruction
	T1486 – Data Encrypted for Impact

References

1. “Cisco Talos Intelligence - Akira Ransomware Continues to Evolve”
2. “MITRE ATT&CK - Akira [S1129]”
3. “Joint Advisory on Akira Ransomware - Cyber Security Agency of Singapore (CSA), Singapore Police Force (SPF), and Personal Data Protection Commission (PDPC)”
4. “Arctic Wolf Labs - Increased Fog and Akira Ransomware Activity Linked to SonicWall SSL VPN”