Akira Ransomware: The Evolution of a Major Threat

Akira Ransomware: The Evolution of a Major Threat

September 11, 2024

Jason Franscisco

Introduction

Akira is a rapidly emerging ransomware group, first identified in early 2023, and is operated by the threat actors known as GOLD SAHARA, PUNK SPIDER, and Storm-1567. Utilizing a ransomware-as-a-service (RaaS) model, Akira employs a double extortion strategy by exfiltrating data before encrypting victims' devices. However, unlike some other ransomware groups, Akira offers victims a degree of flexibility by allowing them to choose whether to pay for decryption assistance, data deletion, or both.

This ransomware has demonstrated a global reach, with the attacks impacting North America, Europe, Asia, Australia, and Africa. A wide range of industries have been targeted, such as financial services, insurance, construction, education, healthcare, manufacturing, agriculture, legal, government, logistics, retail, information technology, and telecommunications.

Recent threat activity has revealed that Akira ransomware affiliates are exploiting a vulnerability in SonicWall devices, CVE-2024-40766, to gain initial access. They specifically target SSLVPN user accounts that are local to the devices, not integrated with centralized

authentication like Active Directory. These compromised accounts also lack multi-factor authentication (MFA) and are running vulnerable SonicOS firmware versions, making them prime targets for exploitation.

Key characteristics of Akira ransomware:

- It is designed to encrypt files and appends a unique "**.akira**" extension to the encrypted filenames.
- It is a cross-platform threat that targets both Windows and Linux devices.
- It can delete Windows Shadow Volume Copies and shut down Windows services during encryption.
- It is often spread through malicious files, such as phishing attachments or compromised software.
- It can also exploit VPN services to mask its network activity and evade detection.

Image representing Akira Tor leak site

Technical Analysis

Initial access

Akira threat actors often exploit vulnerabilities in Virtual Private Network (VPN) services, particularly those lacking multifactor authentication (MFA), to gain initial access to target organizations. They have been known to exploit vulnerabilities in SonicWall SonicOS

firmware, VMware ESXi hypervisor, Fortinet FortiOS, and Cisco software to compromise VPN infrastructure and gain unauthorized access to target networks.

Persistence and Discovery

Once initial access is obtained, Akira threat actors attempt to abuse the functions of domain controllers by creating new domain accounts to establish persistence. In some instances, the Akira threat actors were observed creating an administrative account named “**itadm**”.

Tools like SoftPerfect and Advanced IP Scanner are often used for network device discovery (reconnaissance) purposes and net Windows commands are used to identify domain controllers and gather information on domain trust relationships.

Defense Evasion

As these threat actors prepare for lateral movement, they often disable security software to evade detection. Researchers have noted that Akira actors use tools like PowerTool to exploit the **Zemana AntiMalware** driver and terminate antivirus related processes.

Credential Access

Reports indicate that Akira threat actors leverage post-exploitation attack techniques such as Kerberoasting to extract credentials from the process memory of the Local Security Authority Subsystem Service (LSASS). Akira threat actors also use credential scraping tools like Mimikatz and LaZagne to aid in privilege escalation.

Exfiltration

Akira threat actors leverage a range of tools, including FileZilla, WinRAR, WinSCP, and RClone, along with cloud storage services like Mega, to exfiltrate data. For establishing command and control channels, they employ widely available tools like AnyDesk, MobaXterm, RustDesk, Ngrok, and Cloudflare Tunnel. These tools facilitate data exfiltration through protocols such as File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP).

Encryption

Akira ransomware employs a sophisticated hybrid encryption scheme to compromise data. Combining ChaCha20 and RSA encryption, Akira tailors its encryption methods based on file type and size, allowing for both full and partial encryption. Encrypted files are typically identified by the "**.akira**" or "**.powerranges**" extension.

Akira threat actors enhance their encryption process by inserting additional threads, allowing more precise control over CPU core usage, which boosts both speed and efficiency. The latest version also incorporates a protective layer by using a Build ID as a runtime condition,

preventing successful execution without this unique identifier, which complicates dynamic analysis.

The updated Akira_v2 variant introduces functionalities such as deploying exclusively against virtual machines using the "**vmonly**" parameter and stopping running virtual machines with the "**stopvm**" command. After encryption, the Linux ESXi variant may use the file extension "**.akiranew**" and place a ransom note named "**akiranew.txt**" in directories where files have been encrypted under this new designation.

During the encryption process, the Akira encryptor avoids encrypting files located in the **Recycle Bin**, **System Volume Information**, **Boot**, **ProgramData**, and **Windows** folders. It also excludes Windows system files with extensions such as **.exe**, **.lnk**, **.dll**, **.msi**, and **.sys** from encryption. After encryption, a ransom note named "**fn.txt**" is placed in both the root directory (**C:**) and each user's home directory (**C:\Users**). This note provides instructions and demands a ransom payment for decryption.

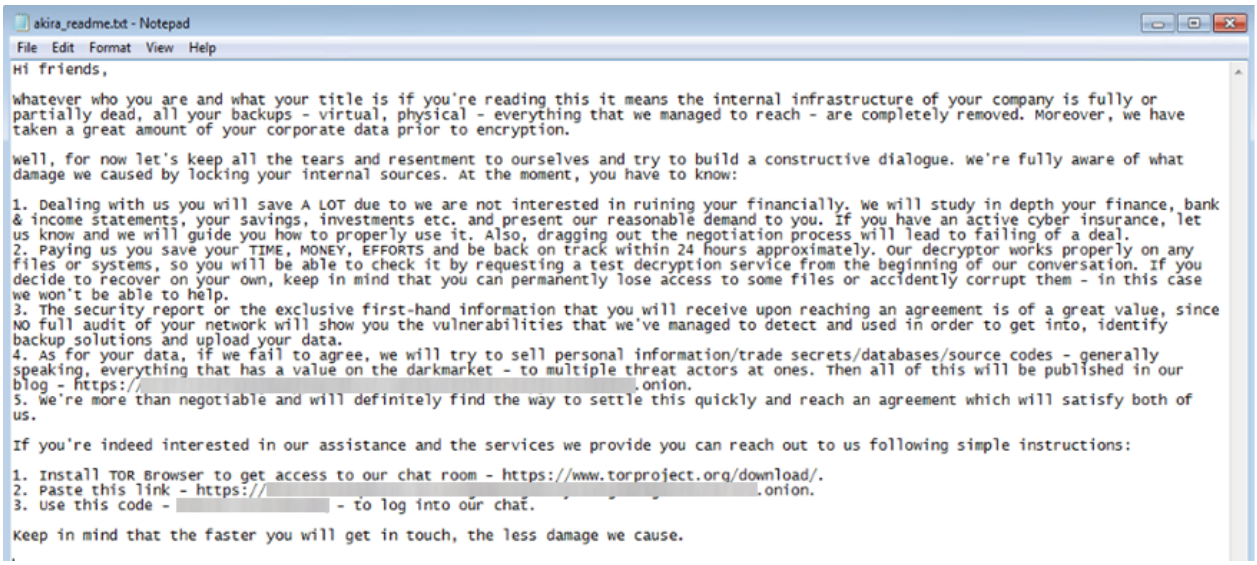

Image representing Akira Ransom note

Impact

In addition to data encryption, Akira exfiltrates sensitive information prior to encryption, exacerbating the risk of data breaches. To prevent system recovery, Akira's encryptor (**w.exe**) leverages PowerShell commands to delete volume shadow copies (VSS) on Windows systems. This strategy significantly impairs the ability to restore data from previous snapshots, complicating recovery efforts and prolonging downtime.

Akira ransomware employs a double-extortion model, encrypting systems after exfiltrating data. Ransom demands are provided upon victim contact, and payments are demanded in Bitcoin. Akira threatens data leaks and direct calls to increase pressure on victims.

Leveraged tools, exploits and malware

Procedure	Tool/Malware/Exploit leveraged
Initial access	VPN via compromised accounts and CVE-2024-40766, CVE-2024-37085, CVE-2024-3259 and CVE-2023-20269
Defense Evasion	PowerTool and KillAV (Terminator from GitHub)
Discovery	AdFind, PCHunter, Advanced IP Scanner, SharpHound and MASSCAN.
Credential Access	Mimikatz, LaZagne and LSASS dump
Command and Control	AnyDesk, Radmin, Cloudflare Tunnel, MobaXterm, RustDesk and ngrok
Lateral Movement	RDP
Exfiltration	WinSCP, Rclone and FileZilla

Recent activities

Recent investigations revealed that Akira ransomware was exploiting **CVE-2024-40766**, a critical access control vulnerability in SonicWall devices. The attacks focused on local accounts without multi-factor authentication (MFA) and exploited vulnerabilities in outdated SonicOS firmware versions.

Historically, this ransomware was observed exploiting

- **CVE-2024-37085** - An authentication bypass vulnerability in the VMware ESXi
- **CVE-2022-40684** - An authentication bypass vulnerability in the Fortinet FortiOS
- **CVE-2020-3259**- An information disclosure vulnerability in the Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software
- **CVE-2023-20269**- An unauthorized access vulnerability in the VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software

MITRE ATT&CK TACTICS AND TECHNIQUES

Table representing technique and tactics employed by Akira ransomware:

ID	Technique	Comments

T1078	Valid Accounts	Akira threat actors gain initial access by acquiring and abusing credentials from existing accounts.
T1190	Exploit Public-Facing Application	Akira threat actors leverage vulnerabilities in internet-facing systems to infiltrate target networks.
T1133	External Remote Services	Akira threat actors have utilized remote access services, such as RDP and VPN connections, to achieve initial access.
T1566	Phishing: Spear phishing Attachment	Akira threat actors use phishing emails with Word (.docx), Excel (.xlsx), or PDF (.pdf) extensions with malicious attachments.
T1566.002	Phishing: Spear phishing Link	Akira threat actors utilize phishing emails with malicious links.
T1003	OS Credential Dumping	Akira threat actors leverage tools such as Mimikatz and LaZagne to extract credentials.
T1003.001	OS Credential Dumping: LSASS Memory	Akira threat actors attempt to retrieve credential data from the process memory of LSASS.
T1558.003	Steal or Forge Kerberos Tickets	Akira threat actors leverage Kerberoasting techniques to extract credentials.
T1016	System Network Configuration Discovery	Akira threat actors utilize tools to scan systems and detect services running on remote hosts and local network infrastructure.
T1082	System Information Discovery	Akira threat actors employ tools such as PCHunter64 to gather detailed process and system information.
T1482	Domain Trust Discovery	Akira threat actors utilize the Windows "net" command to gather domain information.
T1057	Process Discovery	Akira threat actors use the Tasklist utility through PowerShell to retrieve information about running processes.
T1069.001	Permission Groups Discovery: Local Groups	Akira threat actors use the net localgroup /dom command to identify local system groups and their permission settings.
T1069.002	Permission Groups Discovery: Domain Groups	Akira threat actors use the net group /domain command to seek out domain-level groups and their associated permission settings.
T1018	Remote System Discovery	Akira threat actors use the nltest /dclist command to compile a list of other systems on a network based on IP address, hostname, or other logical identifiers.

T1136.002	Create Account: Domain Account	Akira threat actors try to exploit domain controllers by creating new domain accounts to maintain persistence.
T1562.001	Impair Defenses: Disable or Modify Tools	Akira threat actors employ BYOVD (Bring Your Own Vulnerable Driver) attacks to disable antivirus software.
T1219	Remote Access Software	Akira threat actors utilize legitimate desktop support software, such as AnyDesk, to gain remote access to victim systems.
T1090	Proxy	Akira threat actors used Ngrok to establish a secure tunnel to servers, facilitating the exfiltration of data.
T1560.001	Archive Collected Data: Archive via Utility	Akira threat actors use tools such as WinRAR to compress files.
T1048	Exfiltration Over Alternative Protocol	Akira threat actors utilize file transfer tools like WinSCP to transfer data.
T1537	Transfer Data to Cloud Account	Akira threat actors use tools such as CloudZilla and Mega to exfiltrate data to a cloud account and establish connections with exfiltration servers they control.
T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Akira threat actors utilized RClone to synchronize files with cloud storage services for data exfiltration.
T1486	Date Encrypted for Impact	Akira threat actors encrypt data on target systems to disrupt access to system and network resources.
T1490	Inhibit System Recovery	Akira threat actors remove volume shadow copies from Windows systems.
T1657	Financial Theft	Akira threat actors employ a double-extortion model to achieve financial gain.

Defending against Akira Ransomware

- **Training programs:** Akira employs phishing emails and stolen credentials to spread their malware. By providing cybersecurity awareness training, organizations can mitigate their risk by educating employees on security best practices and how to identify common attack methods.

- **Anti-Ransomware Solutions:** The data encryption and exfiltration activities associated with ransomware attacks are distinctive and serve as clear indicators of such threats. Anti-ransomware solutions can leverage these behavioral patterns, among other factors, to detect, block, and remediate infections caused by Akira and other ransomware variants.
- **Data Backups:** Ransomware like Akira aims to coerce companies into paying a ransom by encrypting critical data and holding it hostage. Maintaining regular data backups allows organizations to restore their encrypted files without needing to comply with ransom demands.
- **Patch Management:** Akira frequently takes advantage of vulnerabilities in VPN software to gain access to target systems. Regularly applying patches and updates helps organizations close these security gaps, preventing the ransomware group from exploiting them.
- **Implementing strong user authentication policies:** Akira ransomware often targets VPNs without multi-factor authentication (MFA), making it easier to exploit compromised credentials. Enforcing MFA on corporate systems significantly raises the barrier for attackers, reducing the likelihood of a successful malware infection.
- **Network Segmentation:** Ransomware typically spreads laterally within a corporate network from its initial entry point to systems containing valuable data. Implementing network segmentation helps detect and block this movement, limiting the ransomware's ability to encrypt or steal sensitive information.

Sources Cited: