TIR-20250128 Akira Ransomware

1/28/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Akira is a Ransomware-as-a-Service (RaaS) group that has carried out attacks on finance, manufacturing, and higher education organizations across the U.S., Canada, the United Kingdom of Great Britain and Northern Ireland, and Germany. Lately, the group made headlines as it has now expanded its reach to Linux and VMware ESXi environments.

Originally surfacing in March 2023 as a ransomware group focused on Windows systems, Akira quickly pivoted to attack virtualized infrastructure, especially VMware ESXi servers. This sudden change aligns with the growing trend among threat actors to target hypervisors for maximum disruption - encrypting multiple virtual machines (VMs) at once.

Since its emergence, Akira has compromised hundreds of organizations worldwide, demanding ransoms ranging from $50,000 to $500,000 and accumulating an estimated $42 million in payments by early 2024. Let's discuss Akira's evolution, as well as the group's tactics and techniques.

TIR Summary

- Threat Group
  - Akira ransomware
  - Emerged in March 2023, initially focusing on Windows systems but quickly pivoted to Linux/ESXi environments for broader impact.
  - Demands ransoms ranging from $50,000 to $500,000 and reportedly gained $42 million by early 2024.
- Tactics and Techniques
  - Relies heavily on phishing, unpatched software vulnerabilities (e.g., CVE-2024-37085), and RDP brute-force attacks to gain initial access.
  - Uses a hybrid encryption scheme (ChaCha20 + RSA) and uses a double-extortion model, threatening to leak stolen data if demands are not met.
- Attacks
  - Initially targeted smaller businesses such as 4LEAF, Park-Rite, and Family Day Care Services, before expanding its reach to architecture firms, IT service providers, and colleges.
  - Compromised over 350 global victims across multiple sectors, showcasing a high level of adaptability and operational scale.
- Lessons Learned
  - Implement robust patch management and MFA, ensuring all systems (including ESXi) remain updated and access points remain secure.

AKIRA RANSOMWARE

Akira first gained attention in early 2023 by claiming responsibility for multiple attacks on small and medium-sized businesses, including:

- 4LEAF - An American engineering consultancy
- Park-Rite - A U.S.-based packaging materials manufacturer
- Family Day Care Services - A Canadian childcare service

Shortly after, Akira targeted a UK-based architecture firm (stealing over 11 GB of data), a U.S.-based IT services company (facing a $100,000 ransom), and a European pharmaceutical company ($50,000 ransom). The group also compromised BridgeValley Community and Technical College in West Virginia, causing a significant network outage in April 2023.

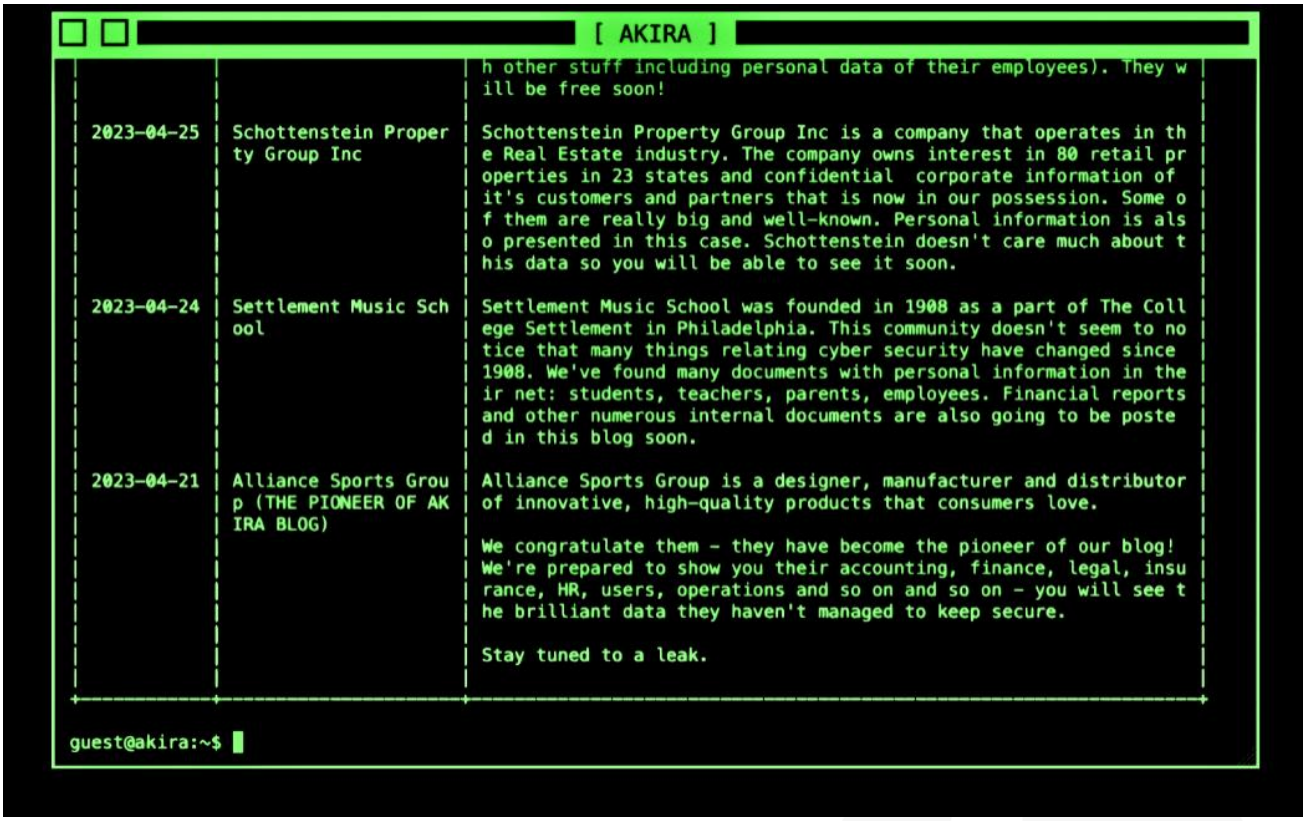
While Akira only captured widespread attention in early 2023, some security researchers suggest the group may have begun testing prototypes as far back as late 2022. Their initial focus on Windows systems appears to have involved close collaboration with a small circle of affiliates, implying Akira might operate on a Ransomware-as-a-Service (RaaS) model. In this framework, core developers provide encryptors and infrastructure, while affiliate partners perform intrusions, data theft, and negotiations with victims.

Early code analysis shows that Akira experimented with partial file encryption to reduce forensic detection and accelerate the encryption process. This approach allowed them to disrupt victim networks quickly without consuming extensive computational resources or triggering conventional security alarms. The group also used multiple reconnaissance tools for enumerating potential victims, scanning for misconfigurations in remote desktop ports, and purchasing initial access from broker services on cybercrime forums.

In 2023, Akira’s operators had perfected their double-extortion tactics, relying on a hidden Tor-based “shame site” to coerce ransom payments. Their willingness to publish stolen data, even partial dumps, demonstrated a level of aggressiveness comparable to more established ransomware groups. This pressure often forced victims to make quick decisions to avoid reputational harm or possible legal repercussions.

By mid-2023, federal agencies such as the FBI, CISA, EC3, and NCSC-NL released joint advisories warning of Akira’s expanding threat footprint. Investigations revealed that Akira had shifted from relying solely on Windows-based ransomware (written in C++) to using a Linux variant aimed at virtual machines running on VMware ESXi servers.

Image 1: Akira Ransomware Victim Shaming



Source: SentinelOne

TACTICS & TECHNIQUES

Initial Access and Propagation

Akira is known to rely on multiple entry vectors, especially phishing emails, unpatched vulnerabilities, and brute-forcing Remote Desktop Protocol (RDP). In the VMware ESXi space, security researchers have linked Akira's rise to the exploitation of CVE-2024-37085, an authentication bypass flaw affecting domain-joined ESXi hypervisors. When this vulnerability is left unpatched, attackers can manipulate Active Directory settings to gain administrative privileges on the hypervisor.

Persistence and Privilege Escalation

Once inside a network, Akira operators focus on creating or co-opting privileged accounts—often establishing a domain account named “itadm”—and exfiltrating authentication data via credential scraping tools such as Mimikatz or LaZagne. They sometimes use Kerberoasting to crack hashed credentials offline, further escalating their privileges. The attackers often disable or uninstall security software along the way, allowing them to move laterally with reduced risk of detection.

Data Exfiltration and Double Extortion

Akira commonly uses a double-extortion strategy. After they infiltrate a network, the attackers copy or exfiltrate sensitive data to remote servers before launching the file encryption stage. If the victim refuses to pay the ransom, Akira threatens to publish the stolen files on a Tor-based leak site, using this additional pressure to coerce payment. Tools like WinRAR, WinSCP, RClone, or FileZilla facilitate bulk data exfiltration, while remote connectivity and tunneling services such as AnyDesk, MobaXterm, RustDesk, Ngrok, and Cloudflare Tunnel support stealthy command-and-control.

Impact on ESXi

ESXi servers are a core target of this new wave of Akira attacks. By compromising a single hypervisor, attackers can encrypt multiple virtual machines simultaneously. Akira’s Linux variant can deploy commands to disable logging (for instance, by rerouting system logs to /tmp) and halt or corrupt running VMs, preventing administrators from identifying the source of the breach until it’s too late.

Recent Attacks

In 2024, the group’s activities reached a wider scope than ever before. A report from Bitdefender and advisories from Microsoft identified more than 350 global victims, with organizations in the manufacturing, finance, education, and critical infrastructure sectors among the hardest hit. Because Akira commonly exploits ESXi weaknesses to obtain administrative access and encrypt virtual machines, organizations suffer significant operational and financial losses.

Administrators who fail to patch ESXi servers or properly segment networks remain particularly vulnerable. Also, any reliance on incomplete or outdated backups can leave entire operations at the mercy of Akira's sophisticated double-extortion methods.

Conclusion

Akira has shown how fast ransomware groups can adapt. They started out attacking Windows systems in early 2023, then moved on to Linux and VMware ESXi servers for bigger payoffs. Their double-extortion tactics and use of known vulnerabilities have proven extremely disruptive to finance, manufacturing, and higher education organizations. They have already collected millions in ransom payments and are not likely to stop.

To fight back, teams need to patch systems quickly, segment networks, and train users to spot phishing attempts. Keeping secure, offline backups is also critical if you want to recover without paying. A strong incident response plan - tailored for both Windows and Linux environments - can make all the difference when Akira or any other ransomware strikes.

Aspire's Recommendations

Aspire Technology Partners recommends the following measures to enhance organizational resilience against threats like Akira ransomware:

- **Patching and Configuration**
  - Applying up-to-date patches for ESXi and associated VMware components is important. CVE-2024-37085, with a CVSS score of 6.8, is a commonly targeted vulnerability.
  - VMware provides security updates and specific mitigation steps, including disabling "ESX Admins" auto-add settings. Ensuring

correct Active Directory configurations and restricting administrative privileges can further curb attackers' movements.

- **Network Segmentation**
  - Maintaining strict network segmentation can limit the lateral movement of ransomware threats. Critical systems, such as domain controllers, hypervisors, and backup servers, should reside on isolated subnetworks, with additional controls to limit traffic flows.
- **Access Controls and MFA**
  - Credential hygiene is a core defense measure against Akira. Enforcing multifactor authentication (MFA) for administrative and remote access drastically reduces the success rate of phishing campaigns, brute force attempts, and stolen credential exploits.
  - Administrators should also adopt long, complex passwords following the latest NIST guidelines and avoid repetitively cycling user credentials.
- **Endpoint Detection and Response (EDR)**
  - An advanced EDR or XDR platform that monitors both endpoints and network traffic can detect and flag unusual behaviors, such as mass file encryption, data exfiltration attempts, or unauthorized administrative account creation.
  - Comprehensive logging and visibility across both Windows and Linux environments will help detect intrusions early, even if the threat actor targets ESXi.

MITRE MAP

Reconnaissance	T1598 – Phishing for Information T1593 – Search Open Websites/Domains
Initial Access	T1078 – Valid Accounts
Execution	T1204 – Use Execution
Lateral Movement	T1534 – Internal Spearphishing
Privilege Escalation	T1548.002 – Abuse Elevation Control Mechanism
Defense Evasion	T1055 – Process Injection T1497 – Virtualization/Sandbox Evasion
Impact	T1486 – Inhibit System Recovery

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers

around-the-clock protection across cloud, network, and endpoints in one integrated solution.
    - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

MD5

- 436c014614477e79696e838d6b605f4e
- 4aecef9ddc8d07b82a6902b27f051f34
- 56f673b1d3d65dce3ef3c8754098df04
- 9df999f142f137b0794b8afcaaedc588
- 9f801240af1124b66defcd4b4ae63f2a
- b163803130f466db74f68a19f9cee11e
- d68a565f1a5962ea081a212b2e7c36e2
- f46623da78371b828f66b602c6487338
- fd380db23531bb7bb610a7b32fc2a6d5

SHA1

- 1ff0c089c5a3b93e95c337e7644119c7bd7133c6
- 41323075a7dc590f20a154f503e089d2dac2fd12
- 8951e54fabdd4d8e424573e53a51e309203f6f41
- 8ad1b4ed98794e8f0a9a9d6fc161697974099d91
- a129c2cff13f7672e27f4c43608da2293e1b5bb7

- a420fbd6cb9d10db807251564c1c9e1718c6fbc5
- a9364eedcc79a19fe96b2e016c27b4fa95ddda52
- c0aafc8c63d0bf316722968d1fe8f1d7637271cd
- d8a6a358ddc57524d9b7db2241750f207f79917f

SHA256

- 3805f299d33ef43d17a5a1040149f0e5e2d5db57ec6f03c5687ac23db1f77a30
- 78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0
- 88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2
- 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a
- 988776358d0e45a4907dc1f4906a916f1b3595a31fa44d8e04e563a32557eb42
- a546ef13e8a71a8b5f0803075382eb0311d0d8dbae3f08bac0b2f4250af8add0
- c9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0
- ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5
- dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198

SUPPORTING DOCUMENTATION

Akira Ransomware: A Shifting Force in the RaaS Domain - LevelBlue - Open Threat Exchange
Akira's New Linux Ransomware Attacking VMware ESXi Servers
Akira Ransomware
20,275 VMware ESXi Vulnerable Instances Exposed
#StopRansomware: Akira Ransomware | CISA
Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption | Microsoft Security Blog
Ransomware gang Akira leaks unprecedented number of victims' data in one day | The Record from Recorded Future News
Akira and RansomHub Surge as Ransomware Claims Reach All-Time High - Infosecurity Magazine
Akira takes in $42 million in ransom payments, now targets Linux servers | SC Media
Akira, again: The ransomware that keeps on taking – Sophos News
Automatic disruption of human-operated attacks through containment of compromised user accounts | Microsoft Security Blog
From Conti to Akira | Decoding the Latest Linux & ESXi Ransomware Families
Akira Ransomware: A Shifting Force in the RaaS Domain

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.