INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-03-29 18:38 UTC

Akira Ransomware Group Escalates Attacks Against Critical Infrastructure Sectors

THREAT CAMPAIGN | CRITICAL | CVSS 9.0

SCC Item ID	SCC-CAM-2026-0006
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.0
Affected Products	Edge devices (VPNs, firewalls), ESXi hypervisors, Linux systems, Windows endpoints across critical infrastructure sectors including healthcare, education, finance, and manufacturing
Published	Nov 13, 2025

Executive Summary

The Akira ransomware group is actively targeting critical infrastructure sectors, including healthcare, education, finance, and manufacturing, using unpatched VPN appliances and firewalls as entry points. The group steals data before encrypting systems and threatens public release, compounding reputational and regulatory exposure alongside operational disruption. A joint FBI/CISA advisory (IC3 CSA 251113, November 2025) confirms cumulative losses in the hundreds of millions of dollars, making this a high-priority threat requiring immediate defensive action.

Technical Analysis

Akira operates a double-extortion ransomware campaign with confirmed targeting of edge devices (VPN appliances, firewall products), VMware ESXi hypervisors, and Linux systems in addition to Windows endpoints. Primary intrusion vectors are exploitation of known vulnerabilities in internet-facing edge products (T1190) and abuse of valid credentials on remote access services lacking MFA (T1078). Relevant weaknesses include CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Function), and CWE-522 (Insufficiently Protected Credentials). Post-access TTPs mapped to MITRE ATT&CK include: command execution (T1059), file and directory discovery (T1083), exfiltration over web services (T1567), defense evasion via indicator removal (T1070) and disabling security tools (T1562), service stop for pre-encryption preparation (T1489), and data encryption for impact (T1486). No single CVE is specified in the advisory; the attack surface spans multiple unpatched edge product vulnerabilities across vendors. ESXi targeting expands blast radius to virtualized workloads. Source: IC3 CSA 251113 (CISA/FBI, November 2025).

Action Checklist

1. Step 1, Immediate: Audit all internet-facing edge devices (VPN concentrators, firewalls) for pending vendor patches; apply critical patches within 24-48 hours or isolate unpatched devices from external access.
2. Step 2, Immediate: Enforce MFA on all remote access services (VPN, RDP, remote management consoles), accounts without MFA are a confirmed Akira entry vector per IC3 CSA 251113.
3. Step 3, Detection: Review VPN and firewall authentication logs for unusual login times, geographic anomalies, credential stuffing patterns, or accounts authenticating from unexpected IPs; cross-reference with Akira IOCs from the joint advisory.
4. Step 4, Assessment: Inventory VMware ESXi hosts and Linux systems for exposure; confirm hypervisor management interfaces are not internet-accessible and are protected by MFA and network segmentation.
5. Step 5, Assessment: Verify backup integrity, confirm backups are offline or immutable, have not been accessed by unauthorized accounts, and can support recovery without paying ransom.
6. Step 6, Communication: If your organization operates in healthcare, education, finance, or manufacturing, brief leadership and legal counsel on Akira risk posture and potential regulatory notification obligations if a breach is suspected.
7. Step 7, Long-term: Review and harden credential management practices addressing CWE-522; implement privileged access workstations and least-privilege policies for accounts with remote access; update incident response playbooks to include Akira-specific TTPs and the IC3 CSA 251113 IOC set.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm immediately if any confirmed unauthorized access to edge devices, remote access accounts, or hypervisor management interfaces is detected, or if data exfiltration indicators (anomalous outbound traffic, known Akira C2 IPs) are observed.
Recovery Notes	Post-containment: force password resets for all accounts with remote access privileges and all privileged accounts; perform full disk forensics on any compromised systems before returning to production; validate backup restoration capability on a non-critical test system; reimage any systems suspected of lateral movement or data staging; implement network segmentation to isolate critical infrastructure from general corporate networks; maintain heightened monitoring of edge devices and hypervisor access for 90 days post-recovery.
Forensic Artifacts	Windows Event Logs: Security (4624, 4625, 4648, 4672 - authentication events), System (1000-1200 - boot/shutdown, service start/stop), Application (logon service events) | Linux: /var/log/auth.log (authentication events), /var/log/syslog or /var/log/messages (system events), /var/log/audit/audit.log (auditd records if enabled) | VPN/Firewall: authentication logs (syslog), session logs, failed login attempts, geographic IP metadata, connection timestamps and durations | VMware ESXi: /var/log/auth.log, /var/log/hostd.log, vpxa.log (vCenter connection logs), stored event database (/var/log/vmkernel.log for kernel-level events) | Network: packet captures (tcpdump/Wireshark) from edge device and hypervisor management VLAN, DNS queries, outbound C2 traffic patterns, data exfiltration flows

Per-Action IR Details

Step 1, Immediate: Audit all internet-facing edge devices (VPN concentrators, firewalls) for pending vendor patches; apply critical patches within 24-48 hours or isolate unpatched devices from external access.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase), §2.2 (vulnerability management)

Controls: NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 CA-7 (Continuous Monitoring), CIS 3.12 (Patch Management)

Compensating: Use vendor CLI or web UI to check current firmware version against published security advisories; document findings in a spreadsheet with device hostname, current version, required patch, and remediation date. For isolation: create an air-gapped VLAN with no external routes; validate via traceroute and netstat -an. Free tool: nessus-cli or nmap version detection against known CVE databases.

Evidence: Capture device configuration backups (running-config, system.conf) before patching. Export authentication logs covering 90 days prior (VPN sessions, firewall logs) to preserve login patterns. Document baseline firewall rule counts and NAT/PAT configurations. Screenshot current firmware versions from each device management interface.

Step 2, Immediate: Enforce MFA on all remote access services (VPN, RDP, remote management consoles), accounts without MFA are a confirmed Akira entry vector per IC3 CSA 251113.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation), NIST 800-53 IA-2(1) (Multi-Factor Authentication)

Controls: NIST 800-53 IA-2(1) (MFA for remote access), NIST 800-53 IA-4 (Identifier Management), CIS 5.4 (MFA for Remote Access)

Compensating: If no MFA appliance: implement RADIUS-based authentication via free FreeRADIUS server + TOTP (Google Authenticator/Authy) on VPN concentrator. Bind RDP to port 3389 behind a bastion host with enforced TOTP. For remote mgmt consoles: restrict access to a jump box requiring SSH key + TOTP. Document MFA bypass procedures for emergency access and require approval logs.

Evidence: Export current remote access account lists (Active Directory users, RADIUS users, local device accounts) with last-login timestamps. Capture authentication policy configurations before MFA deployment. Preserve baseline firewall/VPN logs showing all remote sessions 90 days prior to identify accounts that may resist MFA enforcement.

Step 3, Detection: Review VPN and firewall authentication logs for unusual login times, geographic anomalies, credential stuffing patterns, or accounts authenticating from unexpected IPs; cross-reference with Akira IOCs from the joint advisory.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Detection and Analysis), §3.2.1 (log analysis)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 SI-4 (Information System Monitoring), CIS 8.2 (Logging and Log Retention)

Compensating: Use grep + awk to parse VPN/firewall syslog for failed auth attempts: `grep 'authentication failed' /var/log/auth.log | awk '{print $1, $2, $11}' | sort | uniq -c | sort -rn`. Extract unique source IPs and cross-reference against public IP geolocation databases (MaxMind, GeoIP2 free tier). For Windows RDP: parse Security Event Log 4625 (failed logons) and 4624 (successful logons) using wevtutil or Event Viewer, filter by logon type 3 (network). Create a baseline of normal login hours per account; flag logins outside baseline or from new geographies.

Evidence: Export 90-day VPN authentication logs (syslog or vendor format), firewall authentication logs, RDP Security Event Logs (4624, 4625, 4648, 4672), and any MFA challenge logs. Preserve source IP, timestamp, username, success/failure status, and session duration. Document known user IP ranges and expected login times per account for baseline comparison.

Step 4, Assessment: Inventory VMware ESXi hosts and Linux systems for exposure; confirm hypervisor management interfaces are not internet-accessible and are protected by MFA and network segmentation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation, asset inventory), NIST 800-53 CM-8 (Information System Component Inventory)

Controls: NIST 800-53 CM-8 (Asset Inventory), NIST 800-53 AC-3 (Access Control), NIST 800-53 SC-7 (Boundary Protection), CIS 1.1 (Asset Inventory), CIS 4.1 (Network Segmentation)

Compensating: Use nmap from an internal scanner: `nmap -p 443,22,5900 --script ssl-cert ` to identify hypervisor mgmt ports. Cross-reference against firewall ACLs and routing tables (netstat -rn, ip route show) to confirm no external routes. Document ESXi hosts via `esxcli system version get` and Linux via `cat /etc/os-release`. For exposure: use shodan.io, censys.io free tier to search public IPs for open ESXi/Linux SSH ports and flag findings. Enforce vSphere port group isolation using VLAN tagging; isolate hypervisor mgmt traffic to a separate network segment accessible only from jump boxes.

Evidence: Capture network topology diagrams showing ESXi and Linux system placement. Export firewall ACL configs, routing tables, VLAN definitions, and port group configurations. Document current hypervisor access control settings (root accounts, SSH key policies, vCenter RBAC assignments). Baseline current firewall logs filtering for traffic to ESXi management IPs.

Step 5, Assessment: Verify backup integrity, confirm backups are offline or immutable, have not been accessed by unauthorized accounts, and can support recovery without paying ransom.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation, recovery capability), NIST 800-53 CP-9 (Information System Backup)

Controls: NIST 800-53 CP-9 (System Backup), NIST 800-53 CP-10 (Information System Recovery), NIST 800-53 SI-12 (Information Handling and Retention), CIS 3.14 (Backup and Disaster Recovery)

Compensating: For offline backups: document storage location, encryption method, and physical access controls. Test restoration of a non-critical backup (full cycle) quarterly to a quarantined test environment and document RTO/RPO metrics. For immutable backups (if using cloud): verify retention lock settings via provider API. Audit backup access logs: `grep -i 'backup' /var/log/audit/audit.log | grep 'access'`. Cross-reference backup access against authorized admin accounts and flag unauthorized access. If backup immutability unavailable, store offline copies on write-once media (WORM) and maintain a separate air-gapped recovery server.

Evidence: Export backup job logs (success/failure history, backup sizes, encryption details, destination paths). Capture access control lists on backup storage (NTFS ACLs, Linux file permissions via ls -l, cloud IAM policies). Document backup encryption keys and their storage location/access controls. Record last successful restore test date and RTO/RPO metrics. Preserve authentication logs for all accounts with backup storage access.

Step 6, Communication: If your organization operates in healthcare, education, finance, or manufacturing, brief leadership and legal counsel on Akira risk posture and potential regulatory notification obligations if a breach is suspected.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation, communication planning), NIST 800-53 IR-4 (Incident Handling)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 IR-2 (Incident Response Training), CIS 17.1 (Incident Response Program)

Compensating: Document sector-specific breach notification requirements (HIPAA 60-day notification, GLBA, FERPA, state-level laws). Create a pre-incident communication template addressing leadership, legal, PR, and incident response roles. Identify key stakeholders and escalation paths. Maintain a contact list for regulatory bodies (state AG, FBI field office, CISA, sector ISACs). Brief once per quarter; update template after each regulatory change. For manufacturing/critical infra: coordinate with relevant sector ISACs (e-ISAC, FS-ISAC, NH-ISAC) and have their contact information readily accessible.

Evidence: Preserve copies of applicable breach notification laws and regulatory guidance (HIPAA Security Rule, state breach notification statutes, IC3 CSA 251113). Document organization's previous incident response performance metrics and any prior breaches to establish credibility. Record attendees, date, and topics covered in leadership briefings for audit trail.

Step 7, Long-term: Review and harden credential management practices addressing CWE-522; implement privileged access workstations and least-privilege policies for accounts with remote access; update incident response playbooks to include Akira-specific TTPs and the IC3 CSA 251113 IOC set.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities), NIST 800-53 IA-4, IA-5 (Credential Management)

Controls: NIST 800-53 IA-5 (Authentication and Credential Management), NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-6 (Least Privilege), CIS 5.3 (PAM), CIS 5.2 (Privilege Escalation Restrictions)

Compensating: Use Active Directory Group Policy to enforce password complexity (14+ char, uppercase, numbers, symbols) and 90-day rotation via `gpresult /h` reports. Implement PAM via free/open-source alternatives: HashiCorp Vault (credential rotation) or Keeper (password manager) with audit logging. For PAWs (Privileged Access Workstations): isolate via separate VLAN, disable USB/removable media, enforce drive encryption (BitLocker/LUKS), and restrict network access to mgmt servers only. Build playbook with Akira TTPs: initial access (VPN/firewall compromise), lateral movement (Windows/Linux), persistence (scheduled tasks, cron), data exfiltration (SMB/SSH), and encryption (ESXi/Windows targets). Include IOC indicators from IC3 CSA 251113 (file hashes, C2 domains, etc.).

Evidence: Document current credential management practices, password policies, and privileged account assignments. Export Active Directory account audits (privileged group memberships, last-changed dates). Capture baseline network segmentation configs. Preserve prior incident response playbooks and lessons-learned documents. Record attendance and content updates in playbook review meetings.

Detection Guidance

Focus detection efforts on edge device logs, authentication systems, and endpoint telemetry. Key behavioral indicators based on IC3 CSA 251113 TTPs: (1) Authentication anomalies, look for successful logins using valid credentials (T1078) from unusual source IPs, especially on VPN or remote access portals, particularly outside business hours; (2) Defense evasion, monitor for security tool process terminations (T1562) or log clearing events (T1070) on endpoints and servers; (3) Discovery activity, high-volume file system enumeration (T1083) from a single account or process within a short window; (4) Exfiltration, large outbound data transfers to cloud storage or file-sharing services (T1567), particularly from endpoints not typically performing such transfers; (5) Pre-encryption indicators, service stop commands (T1489) targeting backup agents, VSS (Volume Shadow Copy Service) deletion, or database services being disabled; (6) ESXi-specific, unexpected SSH sessions to ESXi hosts, unauthorized VM snapshot deletions, or configuration changes to host firewalls. Retrieve the IOC list (file hashes, IP addresses, domain indicators) from IC3 CSA 251113 PDF (https://www.ic3.gov/CSA/2025/251113.pdf) and load into SIEM as detection rules. Validate SIEM coverage against T1059, T1078, T1083, T1486, T1489, T1562, T1567, and T1070.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.ic3.gov/CSA/2025/251113.pdf`	IC3 CSA 251113, Joint FBI/CISA advisory containing confirmed Akira IOCs (file hashes, IPs, domains), TTPs, and mitigations. Pull the full IOC list from this document for SIEM ingestion.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter

- **T1078** — Valid Accounts
- **T1083** — File and Directory Discovery
- **T1567** — Exfiltration Over Web Service
- **T1562** — Impair Defenses
- **T1489** — Service Stop
- **T1190** — Exploit Public-Facing Application
- **T1486** — Data Encrypted for Impact
- **T1070** — Indicator Removal

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection
- **A04:2021** — Insecure Design

CIS-V8

- **6.3**
- **6.4**
- **6.5**

- **16.10**
- **5.2**
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.8.24** — Use of cryptography

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1078	Valid Accounts	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1567	Exfiltration Over Web Service	Exfiltration
T1562	Impair Defenses	Defense-Evasion
T1489	Service Stop	Impact
T1190	Exploit Public-Facing Application	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1070	Indicator Removal	Defense-Evasion

Sources

Source	URL	Tier
Cybersecuritydive	https://www.cybersecuritydive.com/news/akira-ransomware-critical-se...	T3
CISA, FBI and Partners Unveil Critical Guidance to Protect Against ...	https://www.cisa.gov/news-events/news/cisa-fbi-and-partners-unveil-...	T1
[PDF] #StopRansomware: Akira Ransomware - IC3.gov	https://www.ic3.gov/CSA/2025/251113.pdf	T1
CISA, FBI, and Partners Issue Critical Guidance on Akira ...	https://www.netbankaudit.com/resources/akira-ransomware-joint-state...	T3
Akira Ransomware's Shift to Target Critical Infrastructure and Linux	https://www.extrahop.com/blog/akira-ransomware-s-shift-to-target-cr...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 18:38 UTC by TJS Security Command Center