INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:43 UTC

Akira Ransomware Group Remains Highly Active, Targeting Legal and Professional Services

THREAT ACTOR | HIGH

SCC Item ID	SCC-TAC-2026-0003
Type	Threat Actor
Severity	HIGH
Affected Products	Organizations in Legal and Professional Services sectors, primarily United States-based
Published	2026-03-26
Discovery Source	Gemini

Executive Summary

The Akira ransomware group is actively targeting legal and professional services organizations in the United States. According to secondary-tier reporting, Akira has reportedly targeted multiple victims in recent weeks; this claim awaits corroboration from authoritative sources (CISA, FBI). Akira operates as a ransomware-as-a-service (RaaS) group using double extortion: data is exfiltrated before encryption, and victims face public exposure on Akira's leak site if ransom is unpaid. Law firms and professional services firms carry high-value client data and privileged communications, making them attractive targets with significant reputational, legal, and operational exposure if compromised. Immediate action is recommended for organizations in this sector, pending confirmation of the current campaign details.

Technical Analysis

Akira is a RaaS operation with a well-documented TTP profile corroborated by a joint CISA/FBI advisory (AA23-284A, October 2023). Initial access is predominantly achieved via exploitation of vulnerabilities in Cisco ASA/FTD VPN appliances and through compromised valid credentials (T1078) targeting external remote services including VPNs (T1133). No specific CVE is attributed to this current campaign report; however, Akira has historically exploited CVE-2023-20269 (Cisco ASA/FTD unauthorized access) and CVE-2024-3400 (Palo Alto PAN-OS) in documented campaigns. Post-access activity includes data exfiltration over C2 channels (T1041), service disruption via stopping recovery mechanisms (T1490, T1489), and file encryption (T1486). Financial extortion is conducted under T1657. No CVSS or EPSS scores are associated with this campaign-level report. This report is based on secondary intelligence sources (Tier 3) pending authoritative corroboration from CISA/FBI advisories. The TTP mappings and early access vectors cited above derive from

the CISA/FBI AA23-284A advisory (T1 source).

Action Checklist

1. Step 1, Immediate: Audit VPN appliance patch levels, prioritizing Cisco ASA/FTD and any perimeter VPN devices; verify patches for CVE-2023-20269 and related CVEs listed in CISA/FBI AA23-284A (October 2023) are applied.
2. Step 2, Immediate: Review and rotate VPN and remote access credentials, especially service accounts and shared credentials; enforce MFA on all external-facing authentication points.
3. Step 3, Detection: Search SIEM and EDR for behavioral indicators of Akira activity, unexpected volume shadow copy deletion (vssadmin, wmic), lateral movement from VPN-assigned IPs, and large outbound data transfers to unknown destinations.
4. Step 4, Assessment: Inventory all external remote access entry points (VPN, RDP, remote management portals); confirm each requires MFA and logs authentication events to a centralized SIEM.
5. Step 5, Communication: If legal or professional services workflows are in scope, notify relevant department heads and legal counsel of elevated sector targeting; review cyber incident response retainer status.
6. Step 6, Long-term: Review and test data exfiltration detection rules aligned to T1041; validate backup integrity and offline/immutable backup posture to reduce leverage from double extortion.
7. Step 7, Long-term: Monitor CISA and FBI channels for an updated joint advisory corroborating this campaign; adjust controls and threat intelligence reporting once authoritative sources confirm TTPs.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external DFIR firm immediately if: (1) any evidence of successful VPN compromise is found (confirmed authentication from unknown actor or lateral movement post-VPN login), (2) volume shadow copies have been deleted on production systems, (3) large outbound data transfers (>100 GB per hour) to unknown destinations are detected, or (4) any ransomware executable is discovered on a networked system.
Recovery Notes	Post-containment recovery is two-phase: (1) System recovery — restore from validated offline backups (never from cloud snapshots that may contain malware), re-baseline systems using a gold-image deployment procedure (NIST SP 800-53 CM-3), and re-apply all security patches. (2) Confidence recovery — conduct a 72-hour post-recovery monitoring period with enhanced logging (verbose process auditing, firewall logging at max verbosity) to confirm no re-infection occurs. Only after 72 hours of clean monitoring can systems return to normal operational status. For legal/professional services organizations, schedule a formal 'Cyber Resilience Review' with counsel and executive leadership 30 days post-recovery to document lessons learned and update incident response procedures.

Forensic Artifacts	Windows Event Logs: 4688 (Process Creation), 4689 (Process Termination), 4720 (User Account Created), 5140 (Network Share Object Accessed), 4624 (Successful Logon), 4625 (Failed Logon) | VPN appliance logs: Cisco ASA syslog (authentication events, tunnel creation/destruction, denied connections), firewall rule hit counters | Firewall logs: NAT translations, ACL denials, egress traffic volume and destination IP/port tuples, DNS query logs from recursive resolvers | Process memory dumps and disk images: from systems with evidence of vssadmin/wmic execution, Shadow Copy deletion, or lateral movement | Network packet captures (PCAP): from VPN gateway and DMZ network segments, covering 72-hour window around suspected compromise, analyzed for C2 beacons and data exfiltration patterns

Per-Action IR Details

Step 1 — Immediate: Audit VPN appliance patch levels, prioritizing Cisco ASA/FTD and any perimeter VPN devices; verify patches for CVE-2023-20269 and related advisories are applied.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase — vulnerability management and patch posture)

Controls: NIST 800-53 SI-2 (Flaw Remediation), CIS Controls 3.11 (Address Unauthorized Software)

Compensating: If patch management tools unavailable: SSH into each VPN appliance (Cisco ASA: 'show version'), document current firmware build, compare against Cisco Security Advisories page (requires manual web lookup of CVE-2023-20269), and export configs via 'write net' or SFTP for offline version tracking. Maintain a spreadsheet correlating appliance serial numbers, firmware versions, and patch dates.

Evidence: Capture VPN appliance running configs via SSH or console ('show running-config' for Cisco ASA; redirect to file for chain of custody). Export SNMP MIB data if available. Document pre-patch state with screenshot of 'show version' output, syslog export covering the past 90 days (search for authentication failures, tunnel drops, or exploit signatures), and any IDS/IPS alerts triggered by CVE-2023-20269 proof-of-concept traffic.

Step 2 — Immediate: Review and rotate VPN and remote access credentials, especially service accounts and shared credentials; enforce MFA on all external-facing authentication points.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.2 (Containment strategies — access control reset) and §3.2.4 (credential revocation)

Controls: NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-4 (Identifier Management), CIS Controls 5.2 (Use Unique Passwords)

Compensating: Without credential vault tools: (1) Export all VPN user accounts from appliance config ('show running-config | include username' on Cisco ASA), document in encrypted local spreadsheet. (2) Revoke via CLI ('no username ' per appliance). (3) Force MFA via appliance policy: for Cisco ASA, enable RADIUS + TACACS+ pointing to on-premises Windows Server NIST SP 800-63b-compliant OTP (e.g., Windows Server Network Policy Server + free TOTP generator like FreeOTP). (4) For shared service accounts, generate new random 32-character passwords, store one copy in sealed envelope locked in secure location, second copy in separate secure location; audit access logs weekly.

Evidence: Before rotation: Export complete VPN user database (Cisco: 'show running-config'), capture RADIUS/TACACS+ server logs for past 90 days (search for failed authentication attempts and account lockouts). Document all currently-active VPN sessions ('show vpn-sessiondb detail'). After rotation: capture new user entries in running config, export authentication logs from MFA provider showing successful MFA enrollments, and document rotation completion timestamp and authorized personnel involved.

Step 3 — Detection: Search SIEM and EDR for behavioral indicators of Akira activity — unexpected volume shadow copy deletion (vssadmin, wmic), lateral movement from VPN-assigned IPs, and large outbound data transfers to unknown destinations.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Detection and Analysis — indicator identification and correlation)

Controls: NIST 800-53 AU-12 (Audit Generation), NIST 800-53 SI-4 (Information System Monitoring), CIS Controls 8.8 (Implement User Activity Logging)

Compensating: Without EDR/SIEM: (1) Search Windows Event Log 4688 (Process Creation) on all endpoints for 'vssadmin', 'wmic', or 'powershell' combined with 'copy', 'delete', or 'shadow' keywords (use wevtutil or Event Viewer export-to-CSV). (2) Search Process Monitor (procmon.exe) capture files saved from VPN-assigned client IPs for deletion operations on 'System Volume Information'. (3) Query firewall logs (Cisco ASA 'show log' or Windows Defender Firewall logs in Event ID 5156) for outbound connections to unknown IPs on port 443, 80, or uncommon ports; cross-reference destination IPs against threat intel feeds (Shodan, VirusTotal, Abuse.ch). (4) Use netstat or PowerShell 'Get-NetTCPConnection' to list active outbound connections, document suspicious ones.

Evidence: Collect Windows Event Logs 4688 (Process Creation), 4689 (Process Termination), 4720 (User Account Created), and 5140 (Network Share Object Accessed) for all systems within 72 hours of detection. Export firewall logs covering same window. Capture process memory dumps (ProcDump, Task Manager > Create Dump File) of any suspicious processes. Preserve VSS metadata if still present (dir /a /s C:\System\ Volume\ Information\). Document outbound DNS queries from internal recursive resolvers (if available). Preserve full packet captures (tcpdump, Wireshark) from network TAP or SPAN port capturing VPN-assigned client traffic.

Step 4 — Assessment: Inventory all external remote access entry points (VPN, RDP, remote management portals); confirm each requires MFA and logs authentication events to a centralized SIEM.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (Tools and resources — asset inventory and baseline documentation)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), NIST 800-53 IA-2 (Authentication), CIS Controls 1.1 (Establish and Maintain Detailed Asset Inventory)

Compensating: Without automated discovery tools: (1) Query DNS records and firewall NAT rules to identify all external IPs and hostnames (document 'nslookup ' and firewall rule exports). (2) For each entry point, manually verify MFA requirement: VPN appliance ('show running-config' search for 'group-policy' and 'tunnel-group'), RDP ('gpresult /h report.html' for Remote Desktop policies), web portals (review application source code or configuration files for 'require MFA' flags). (3) Verify logging: VPN appliance logs to syslog or onboard storage (configure 'logging enable', 'logging timestamp'), RDP via Windows Event Log 4624 (Logon), web portal via application logs (tail -f /var/log/app_auth.log). (4) Create manual spreadsheet: Column headers = Entry Point | Hostname | Port | MFA Enabled Y/N | Log Destination | Last Audit Date.

Evidence: Preserve network diagrams (Visio, draw.io export) showing all external IP space and DMZ architecture. Export complete firewall rule base for NAT and ACLs. Export DNS zone files or internal DNS query logs showing external hostname resolutions. Capture VPN appliance 'show running-config' output. Preserve application configuration files for any web-based remote access portals. Document the current state before remediation by taking screenshots of authentication prompts and MFA enrollment flows.

Step 5 — Communication: If legal or professional services workflows are in scope, notify relevant department heads and legal counsel of elevated sector targeting; review cyber incident response retainer status.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.3 (Tools and resources — roles and responsibilities); NIST 800-61r3 §3.4.7 (Post-incident analysis communication plan)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 CP-2 (Contingency Plan), CIS Controls 17.1 (Assign Incident Response Roles)

Compensating: Without formal IR retainer: (1) Document internal escalation contacts in a sealed envelope stored offsite: General Counsel, Chief Security Officer, CFO, CEO, Board Risk Committee chair. Include external contacts: preferred outside counsel, preferred DFIR firm, local FBI field office (check ic3.gov for your region). (2) Prepare a templated 'Sector Alert Notification' document: 'On [DATE] Akira ransomware group announced 5 new victims in legal/professional services sector. Our organization [is/is not] currently in scope. We have [X] active controls. Next scheduled security review: [DATE].' (3) Schedule a 30-minute executive briefing with legal and operations leads; record attendance and decisions in a memo (BCC to your own email for evidence). (4) If no retainer exists, contact 3 vetted

DFIR firms and request incident response SLA quotes; document quotes with date, firm contact, and response time commitment.

Evidence: Preserve all communications: send notifications via recorded email or documented phone calls (take contemporaneous notes with date, time, attendees, key points). Document who received the notification and when. If a retainer review occurs, save the executed retainer agreement (or quote, if not yet signed) with dates and scope clearly marked. Archive meeting notes and attendance records. If this is a real incident (not a drill), preserve this communication log as part of the incident record.

Step 6 — Long-term: Review and test data exfiltration detection rules aligned to T1041; validate backup integrity and offline/immutable backup posture to reduce leverage from double extortion.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.3 (Recovery) and §4.4 (Post-incident analysis — detection and prevention improvements); NIST SP 800-34 (Contingency Planning Guidance)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CP-9 (Information System Backup), NIST 800-53 CP-10 (Information System Recovery and Reconstitution), CIS Controls 10.1 (Enable and Enforce Automated Data Backups)

Compensating: Without SIEM/DLP: (1) For T1041 detection (Exfiltration Over C2 Channel): Query firewall egress logs weekly for anomalous outbound volume (compare current week to 13-week historical baseline using awk/PowerShell; flag if >2 standard deviations above mean). Monitor DNS queries for domains not in whitelist (export recursive resolver logs, compare to approved domain list). (2) For backup validation: Each quarter, restore a test backup to an isolated environment (air-gapped from production) and verify: file count, integrity (md5sum or hash comparison), and recoverability (can you actually start a restored application?). Document with date, backup source, restore time, and signed-off-by authorized person. (3) For offline/immutable backup: if resources exist, maintain one full backup on external hard drives stored in a locked physical location (not in data center). If budget allows, implement Write-Once-Read-Many (WORM) storage using free tools like Bacula with disk-based WORM device or ZFS snapshots with 'zfs set snapdir=hidden' and restricted mount permissions.

Evidence: Preserve backup validation test results: screenshot of restored file listings, application startup logs from restored environment, and signed test log with date/time/personnel. Document backup inventory with: source system, backup timestamp, backup size, backup media (disk/tape/cloud), retention policy, and last successful restore date. Maintain a backup integrity log (checksum comparison results). If immutable backups implemented, capture OS-level WORM configuration (ZFS snapshots, disk device WORM status output). Store all documentation in a physically separate location from primary backups.

Step 7 — Long-term: Monitor CISA and FBI channels for an updated joint advisory corroborating this campaign; adjust controls and threat intelligence reporting once authoritative sources confirm TTPs.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 (Post-incident analysis) and §4.4 (Evidence retention and lessons learned); NIST SP 800-153 (Guidelines for Securing Wireless Local Area Networks)

Controls: NIST 800-53 SI-5 (Security Alerts, Advisories, and Directives), CIS Controls 4.1 (Establish and Maintain a Process for Receiving, Reviewing, and Responding to Security Advisories)

Compensating: Without threat intelligence platform: (1) Subscribe to free threat feeds: CISA Alerts (alerts.cisa.gov), FBI IC3 (ic3.gov), MITRE ATT&CK Updates (attack.mitre.org/resources/updates), Shodan (shodan.io free tier for IP reputation). Set up email alerts or RSS readers (Feedly, Inoreader) to monitor these daily. (2) Establish a monthly 'TI Review' meeting (30 min) with SOC lead or security lead: review new Akira indicators (IP, hashes, domains), update your organization's YARA rules or firewall rules if needed (search for 'Akira' in known indicators), and document what changed from previous month. (3) Maintain a 'TI Log' spreadsheet: Date | Source | Indicator Type | Indicator Value | Action Taken | Responsible Person. (4) When CISA publishes a joint advisory, immediately cross-reference the TTP list against your controls: map each TTP to a CIS Control or NIST 800-53 control you own, and update your annual security roadmap if gaps exist.

Evidence: Preserve all threat intelligence subscriptions (screenshots of signup confirmations, RSS feed URLs). Maintain the TI Log as a permanent record with dates and actions. Archive copies of all CISA/FBI advisories

mentioning Akira (PDF, date-stamped). When TTPs are confirmed, save your response: updated firewall rules (before/after comparison), updated detection rules (YARA/Sigma/Splunk queries with version control), and signed-off change log showing who approved the updates and when. If a lessons-learned meeting is held post-incident, preserve meeting notes and any resulting roadmap adjustments.

Detection Guidance

Focus detection efforts on Akira's known pre-encryption behaviors documented in CISA/FBI AA23-284A. This guidance is based on known Akira behavioral patterns; campaign-specific IOCs for the current incident are not yet available from public sources. Validate detection rules against your environment baseline before deployment. Key behavioral indicators: (1) Volume shadow copy deletion, query Windows event logs for EventID 4688 with process names vssadmin.exe or wmic.exe and arguments containing 'delete shadows'; (2) Credential-based VPN access anomalies, alert on VPN authentications from new geographies, unusual hours, or high-velocity login attempts against the same account; (3) Large outbound transfers, baseline normal egress volumes by host and alert on sustained transfers exceeding normal thresholds to external IPs, particularly over ports 443 or 80 to uncategorized destinations (T1041); (4) Service termination, monitor for bulk service stop commands targeting backup agents, AV, or database services (T1489); (5) Encryption activity, file rename events at high velocity with extension changes across network shares are a late-stage indicator (T1486). MITRE ATT&CK techniques to map detection rules against: T1041, T1078, T1133, T1486, T1489, T1490, T1657. Monitor Akira-specific threat feeds and the CISA Known Exploited Vulnerabilities catalog for updates.

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No confirmed IOCs available`	No specific indicators of compromise were present in the source data for this campaign report. All listed sources are Tier 3 with a source quality score of 0.64. IOCs should be sourced from authoritative feeds such as CISA advisories, FBI flash alerts, or established threat intelligence platforms once corroborating reporting is published.	LOW

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1490** — Inhibit System Recovery
- **T1657** — Financial Theft
- **T1078** — Valid Accounts
- **T1133** — External Remote Services
- **T1486** — Data Encrypted for Impact

- **T1489** — Service Stop

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **CM-6** — Configuration Settings
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

NIST-CSF-2

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

HIPAA-SECURITY

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.24** — Use of cryptography

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1490	Inhibit System Recovery	Impact

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1078	Valid Accounts	Defense-Evasion
T1133	External Remote Services	Persistence
T1486	Data Encrypted for Impact	Impact
T1489	Service Stop	Impact

Sources

Source	URL	Tier
Initiatives - Center for Cybersecurity Policy and Law	https://www.centerforcybersecuritypolicy.org/initiatives	T3
Cybersecurity Services - Venable LLP	https://www.venable.com/services/industries/cybersecurity-services	T3
Best Law Firms for Cyber Security & Privacy Law - Vault	https://vault.com/best-companies-to-work-for/law/best-law-firms-in-...	T3
The Top Cybersecurity Threats Law Firms Face - ArmorPoint	https://armorpoint.com/2025/12/10/the-top-cybersecurity-threats-law...	T3
Securing Legal Fortresses: The 10 Best Cybersecurity Services for ...	https://www.edendata.com/post/cybersecurity-service-providers-for-l...	T3

Generated 2026-03-29 18:43 UTC by TJS Security Command Center