INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-28 18:49 UTC

Talos 2025 Data Reframes the Defender Mandate: Identity, Patterns, and the Persistence of Old Vulnerabilities

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0091
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	IAM/PAM platforms, VPNs, Active Directory, application delivery controllers (ADCs), firewalls, PHP frameworks, Log4j (CVE-2021-44228), Adobe ColdFusion, network management platforms
Published	2026-04-28T13:23:20+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Cisco Talos' 2025 Year in Review, drawn from active incident response engagements, documents that adversaries are winning not through novel tradecraft but through disciplined reuse of proven techniques: stolen credentials, multifactor authentication bypass, and exploitation of vulnerabilities disclosed years ago. The report shifts focus away from perimeter hardening and raw CVSS-driven patching toward identity control, behavioral detection, and exposure-based vulnerability prioritization. For CISOs and boards, the signal is clear: investment in detection programs that cannot distinguish legitimate tool use from attacker activity, and patch programs that prioritize recency over exploitability, are empirically underperforming against the current threat landscape.

Technical Analysis

The Talos 2025 Year in Review synthesizes incident response data across ransomware operators and nation-state actors linked to China, Russia, North Korea, and Iran. The findings do not describe a single campaign; they describe a threat landscape shaped by structural advantages attackers have built over years of defender underinvestment in identity and detection.

Initial access is dominated by identity abuse. Valid credential compromise (T1078) and MFA bypass techniques including MFA fatigue (T1621) are the primary entry vectors into IAM and PAM platforms, VPNs, and Active Directory environments. External-facing services (T1133) remain a reliable fallback when credential attack paths

are blocked. The CWE profile for this pattern, CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Function), CWE-1390 (Weak Authentication), and CWE-770 (Allocation of Resources Without Limits or Throttling), maps precisely to the authentication control gaps Talos observed across engagements.

Post-compromise activity is dominated by living-off-the-land (LotL) techniques. Attackers use legitimate system binaries and administrative tools, mapped to T1059 (Command and Scripting Interpreter) and T1021.002 (SMB/Windows Admin Shares), to blend with normal operational traffic. Scheduled tasks (T1053), obfuscation (T1027), and authentication modification (T1556, T1556.006) extend dwell time. This pattern creates a fundamental detection problem: behavioral anomaly detection programs that baseline normal administrative activity are better positioned to catch LotL abuse than signature-based controls, but many organizations have not operationalized that capability.

Legacy vulnerability exploitation is not a tail risk, it is a present operational reality. Log4j (CVE-2021-44228, disclosed December 2021) and Adobe ColdFusion vulnerabilities are appearing in active IR cases in 2025. Exploit public-code availability (T1588.002) and exploitation of public-facing applications (T1190) remain viable because patch programs driven by CVSS scores and disclosure recency fail to account for actual exploitability in context. Exposure-based prioritization models that weight KEV status, EPSS scores, and reachability analysis are outperforming volume-driven patching approaches.

AI tooling is accelerating attacker tempo rather than introducing new attack categories. Talos documents AI use in phishing lure creation and reconnaissance (T1595, T1589.001), consistent with the broader industry observation that AI lowers the skill floor for social engineering and initial access operations without fundamentally changing the kill chain.

For detection engineering, the implication is structural: programs centered on behavioral anomaly detection and exposure-based prioritization are producing better outcomes than perimeter-centric or signature-dependent models. The MITRE ATT&CK techniques observed, spanning reconnaissance, credential access, lateral movement, persistence, and defense evasion, require detections across the full kill chain, not just at the perimeter.

Action Checklist

1. Step 1: Assess exposure, audit IAM and PAM platforms, VPNs, Active Directory configurations, and external-facing services (ADCs, firewalls, network management platforms) for credential hygiene weaknesses and MFA coverage gaps; separately verify whether Log4j (CVE-2021-44228) or Adobe ColdFusion instances remain in your environment
2. Step 2: Review controls, validate MFA implementation against bypass-resistant standards (phishing-resistant FIDO2/hardware token where feasible); audit MFA fatigue protections (number matching, push rate limiting); review behavioral detection coverage for LotL techniques including scheduled task creation (T1053), lateral SMB movement (T1021.002), and scripting interpreter abuse (T1059)
3. Step 3: Update threat model, incorporate the authentication abuse pattern (T1078, T1621) and LotL post-compromise pattern as primary threat scenarios in your threat register; if your organization is in a sector targeted by China-, Russia-, North Korea-, or Iran-linked actors, map those actor TTPs explicitly
4. Step 4: Communicate findings, brief leadership on the finding that perimeter investment and CVSS-volume patching programs are empirically underperforming; frame the identity control and behavioral detection gaps as investment priorities with concrete IR-case evidence from Talos

5. Step 5: Monitor developments, track Talos intelligence publications for follow-on IR-derived IOC releases and campaign-specific indicators; monitor CISA KEV additions for any newly listed legacy vulnerabilities (Log4j, ColdFusion variants) that signal active exploitation confirmation

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to immediate priority and activate the IR plan if any of the following are confirmed: (1) Log4j CVE-2021-44228 JNDI callback traffic detected in outbound connection logs indicating active exploitation attempt against an unpatched instance; (2) MFA push approval anomaly detected — multiple approvals within a short window from different geolocations indicating T1621 MFA fatigue attack in progress; (3) Unauthorized scheduled task creation (Event ID 4698) on a domain controller or PAM host correlated with an account authenticating via VPN without MFA; (4) CISA KEV addition of a ColdFusion or Log4j variant CVE confirming active in-the-wild exploitation against products confirmed present in your environment; or (5) Evidence of T1021.002 lateral SMB movement from a VPN-authenticated session to a domain controller, indicating post-authentication lateral movement consistent with the Talos-documented credential-reuse post-compromise pattern.
Recovery Notes	Post-containment recovery for credential-based intrusions documented in Talos IR cases must include full credential rotation for all accounts with any authentication activity during the compromise window — not just privileged accounts — because adversaries using T1078 frequently establish persistence via lower-privilege accounts as fallback access. Verify scheduled task inventory on all domain-joined systems post-eradication using `Get-ScheduledTask | Where-Object {$_.TaskPath -notlike '\Microsoft\*'} \| Select TaskName, TaskPath, @{N='Actions';E={$_.Actions.Execute}}` and cross-reference against a known-good baseline, as T1053 persistence is a primary post-exploitation artifact in Talos IR cases. Maintain elevated monitoring of VPN authentication logs, AD privileged account activity, and outbound SMB for a minimum of 30 days post-recovery, as Talos IR data consistently shows adversaries re-entering environments within weeks using secondary credentials harvested during the initial compromise dwell period.

Forensic Artifacts	Windows Security Event ID 4648 (Logon using explicit credentials) and 4624 (Type 3 network logon) on domain controllers — in Talos-documented T1078 credential reuse cases, these events show the stolen credential being used from VPN-assigned IP ranges, providing the authentication chain from initial VPN access through lateral movement | VPN authentication logs with MFA method field — Cisco ASA `show vpn-sessiondb detail` or Palo Alto GlobalProtect `pan_gp_gw.log` — specific to MFA bypass (T1621): look for sessions authenticated without a second factor or with anomalous MFA approval timing (approval within <5 seconds of push issuance indicating pre-staged attacker access to the victim's device or session hijack) | Web server access logs filtered for Log4j JNDI injection payloads: Apache `/var/log/apache2/access.log` or IIS W3C logs searched for `%24%7Bjndi`, `${jndi:ldap://`, `${jndi:rmi://`, or obfuscated variants using nested lookup bypass patterns (`${${::-j}${::-n}${::-d}${::-i}`) — these are the exact URI-encoded strings CVE-2021-44228 exploitation leaves in HTTP request logs | Scheduled task XML files in `C:\Windows\System32\Tasks\` and `C:\Windows\SysWOW64\Tasks\` with creation timestamps during the suspected compromise window — in LotL post-exploitation (T1053), adversaries create scheduled tasks with legitimate-appearing names (e.g., mimicking Windows Update or Defender tasks) that execute PowerShell or cmd.exe payloads; these XML files persist even after the task is deleted from the task scheduler UI | PowerShell Script Block Logging Event ID 4104 in the Microsoft-Windows-PowerShell/Operational log — T1059.001 LotL activity documented in Talos IR cases leaves encoded command strings, `Invoke-Expression` with Base64 payloads, or `Net.WebClient.DownloadString` calls in script block logs even when the execution was designed to be fileless, providing the command chain from initial credential use through post-exploitation

Per-Action IR Details

Step 1: Assess exposure — audit IAM and PAM platforms, VPNs, Active Directory configurations, and external-facing services (ADCs, firewalls, network management platforms) for credential hygiene weaknesses and MFA coverage gaps; separately verify whether Log4j (CVE-2021-44228) or Adobe ColdFusion instances remain in your environment

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and reducing the attack surface before an incident occurs, including asset inventory and control gap identification

Controls: NIST IR-4 (Incident Handling) — ensuring preparation activities feed the incident handling capability, NIST SI-2 (Flaw Remediation) — identify and correct system flaws including CVE-2021-44228 (Log4j) and unpatched ColdFusion instances, NIST IA-5 (Authenticator Management) — audit credential hygiene and MFA coverage across IAM/PAM, VPN, and AD, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — required to locate all Log4j-affected JVM-based services and ColdFusion instances before exploitation occurs, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — exposure-based prioritization, not raw CVSS volume, per the Talos finding, CIS 6.3 (Require MFA for Externally-Exposed Applications) — directly maps to VPN, ADC, and firewall management interfaces identified in this advisory

Compensating: For Log4j discovery without a commercial scanner: run `find / -name 'log4j*.jar' 2>/dev/null` and `find / -name '*.war' -o -name '*.ear' -o -name '*.jar' | xargs -I{} unzip -l {} 2>/dev/null | grep -i log4j` on Linux hosts; on Windows use `Get-ChildItem -Recurse -Filter 'log4j*.jar' -ErrorAction SilentlyContinue`. For ColdFusion: check IIS/Apache access logs for requests to `/CFIDE/administrator/` or `/cf_scripts/`. For AD credential hygiene with no SIEM: run `Get-ADUser -Filter * -Properties PasswordLastSet, PasswordNeverExpires, LastLogonDate | Where-Object {$_.PasswordNeverExpires -eq $true -or $_.PasswordLastSet -lt (Get-Date).AddDays(-180)}` and review results manually. For MFA gap identification on VPNs without EDR: pull authentication logs from the VPN concentrator and cross-reference accounts with no MFA enrollment in your IdP.

Evidence: Capture BEFORE auditing: (1) Active Directory last logon timestamps and password age for all privileged accounts via `Get-ADUser` export — establishes dormant credential baseline that Talos IR cases show adversaries

exploit; (2) VPN authentication logs (e.g., Cisco ASA `show vpn-sessiondb` or Palo Alto GlobalProtect auth logs) showing authentication method per session — identifies accounts authenticating without MFA; (3) Current Log4j JAR inventory with file paths and associated process/service names — documents pre-audit exposure state; (4) ColdFusion version strings from `cf_server_config.xml` or `/CFIDE/administrator/index.cfm` response headers — establishes patch level against known ColdFusion exploitation campaigns confirmed in Talos IR data.

Step 2: Review controls — validate MFA implementation against bypass-resistant standards (phishing-resistant FIDO2/hardware token where feasible); audit MFA fatigue protections (number matching, push rate limiting); review behavioral detection coverage for LotL techniques including scheduled task creation (T1053), lateral SMB movement (T1021.002), and scripting interpreter abuse (T1059)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Implementing detection instrumentation and validating controls prior to an incident, directly enabling the Detection & Analysis phase

Controls: NIST IA-3 (Device Identification and Authentication) — validate phishing-resistant authenticator standards (FIDO2) for VPN and administrative access, NIST SI-4 (System Monitoring) — implement behavioral detection coverage for T1053 (scheduled task creation), T1021.002 (lateral SMB), and T1059 (scripting interpreter abuse) as documented LotL patterns in Talos IR cases, NIST AU-2 (Event Logging) — ensure event types required to detect LotL activity are enabled: process creation, scheduled task events, SMB session events, and PowerShell/script block logging, NIST IR-3 (Incident Response Testing) — validate that existing detection controls actually fire on these LotL techniques through tabletop or purple team exercise, CIS 6.3 (Require MFA for Externally-Exposed Applications) — validate bypass-resistant MFA specifically on IAM/PAM portals, VPN gateways, and ADC management interfaces, CIS 6.5 (Require MFA for Administrative Access) — number matching and push rate limiting map directly to this safeguard for AD admin and PAM accounts, CIS 8.2 (Collect Audit Logs) — verify logging is enabled and capturing the specific event types needed for LotL detection before an incident forces retroactive discovery

Compensating: For FIDO2 gap assessment without enterprise IdP tooling: query Azure AD or on-prem AD FS authentication logs for MFA method per user — look for `OTP` or `Phone` entries where `FIDO2` or `Certificate` is absent. For MFA fatigue detection without SIEM: deploy free Sysmon (config v14+) with SwiftOnSecurity's base config, which logs process creation (Event ID 1) and network connections (Event ID 3); pipe to Windows Event Log and alert on `mshta.exe`, `wscript.exe`, or `cscript.exe` spawned by unexpected parent processes. For T1053 detection: enable Windows Security Event ID 4698 (Scheduled Task Created) via GPO (`Audit Other Object Access Events`) — no SIEM required, review locally or forward via Windows Event Forwarding (WEF) to a free Graylog or Elastic instance. For T1021.002 lateral movement: deploy the free Sigma rule `proc_creation_win_net_share_mount.yml` against WEF-collected logs. For T1059 PowerShell abuse: enable PowerShell Script Block Logging via GPO (`HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging`) and review Event ID 4104.

Evidence: Capture BEFORE control review: (1) Current Sysmon configuration file hash and version — documents instrumentation state at review time, critical if LotL activity is later discovered to have preceded the audit; (2) Windows Security Event Log export filtered for Event ID 4698 (Scheduled Task Created) and 4702 (Scheduled Task Updated) for the prior 90 days — Talos IR data shows adversaries pre-stage persistence via scheduled tasks during the dwell period before detection; (3) PowerShell Event ID 4104 (Script Block Logging) entries for the prior 30 days — LotL actors using T1059.001 will leave encoded or obfuscated blocks here if logging was already enabled; (4) SMB session logs (Windows Security Event ID 5140 — Network Share Object Accessed) filtering on `IPC$` and `ADMIN$` from lateral movement source IPs — T1021.002 artifact; (5) MFA push log export from your IdP (Okta system log, Azure AD Sign-In logs, Duo Admin API) showing push approval timestamps and geolocation — MFA fatigue attacks leave a pattern of rapid sequential push approvals across short windows.

Step 3: Update threat model — incorporate the authentication abuse pattern (T1078, T1621) and LotL post-compromise pattern as primary threat scenarios in your threat register; if your organization is in a sector targeted by China-, Russia-, North Korea-, or Iran-linked actors, map those actor TTPs explicitly

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Developing and maintaining threat intelligence inputs that inform IR plan scope, detection priorities, and escalation criteria before incidents occur

Controls: NIST IR-8 (Incident Response Plan) — threat model updates must feed directly into the IR plan's scenario coverage, specifically adding credential-based initial access (T1078) and MFA bypass (T1621) as named scenarios, NIST RA-3 (Risk Assessment) — formal threat modeling using Talos IR-derived evidence constitutes a risk assessment update; document nation-state actor mappings as named threat sources, NIST SI-5 (Security Alerts, Advisories, and Directives) — receiving and actioning Talos Year in Review as an authoritative advisory is the operational expression of this control, NIST IR-4 (Incident Handling) — threat register updates directly expand the scope of incidents the handling capability must address, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — threat model refinement based on Talos IR evidence is the exposure-prioritization mechanism this safeguard requires

Compensating: For teams without a formal threat intelligence platform: maintain threat register in a shared spreadsheet or Confluence page using the MITRE ATT&CK Navigator (free, browser-based at attack.mitre.org/resources/attack-navigator/) to visualize TTP coverage gaps. Export the ATT&CK Navigator layer as JSON and version-control it in Git — this creates a dated, auditable threat model without any tooling cost. For nation-state TTP mapping: use MITRE ATT&CK Groups page (e.g., G0096 for APT41, G0007 for APT28, G0032 for Lazarus Group, G0003 for UNC215/APT1 proxies) and cross-reference with CISA advisories for each actor group relevant to your sector. Document in your threat register with advisory citation dates.

Evidence: Capture BEFORE updating the threat model: (1) Current threat register snapshot (dated export) — establishes the pre-update baseline so delta changes driven by Talos findings are auditable for post-incident review under NIST 800-61r3 §4; (2) Existing ATT&CK Navigator layer export showing current TTP detection coverage — documents where T1078 and T1621 were absent or unmonitored before this review cycle; (3) Any prior IR tickets, SIEM alerts, or authentication anomaly reports from the past 12 months referencing failed MFA, unusual VPN authentication sources, or AD credential spraying — these are pre-existing signals that may retroactively confirm the Talos-documented pattern was already present in your environment.

Step 4: Communicate findings — brief leadership on the finding that perimeter investment and CVSS-volume patching programs are empirically underperforming; frame the identity control and behavioral detection gaps as investment priorities with concrete IR-case evidence from Talos

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned and reporting processes that translate IR evidence into organizational improvement and resource allocation decisions

Controls: NIST IR-6 (Incident Reporting) — while this is a proactive brief rather than an active incident report, the control's requirement to communicate findings to appropriate organizational roles applies directly, NIST IR-8 (Incident Response Plan) — leadership briefs that result in resource allocation changes must be captured as IR plan updates, not just verbal commitments, NIST IR-4 (Incident Handling) — the Talos finding that identity and behavioral gaps are the primary failure mode is an IR capability gap that requires documented escalation to leadership per this control, CIS 7.2 (Establish and Maintain a Remediation Process) — reframing from CVSS-volume patching to exposure-based prioritization is operationally the risk-based remediation strategy this safeguard requires; leadership must authorize the methodology shift

Compensating: For teams without a dedicated GRC or reporting platform: use the free CISA Cybersecurity Performance Goals (CPGs) self-assessment template as the structured evidence baseline — it maps directly to identity and MFA gaps Talos documented and provides a government-credentialed framework leadership will recognize. Supplement with the Talos 2025 Year in Review PDF (publicly available from Talos Intelligence blog) as primary source material. Build the brief as a one-page risk register delta showing: current state of MFA coverage, detection coverage for T1078/T1621/T1059, and cost-to-exploit for an adversary using the Talos-documented credential reuse pattern versus a novel zero-day — this quantifies the identity gap without requiring a commercial risk quantification tool.

Evidence: Capture BEFORE the leadership brief: (1) MFA enrollment coverage percentage by system tier (VPN, PAM, AD admin, external applications) from your IdP — this is the primary metric that maps directly to the Talos finding and must be documented as a pre-brief baseline; (2) Patch currency data for Log4j (CVE-2021-44228) and ColdFusion across your environment — if any unpatched instances exist, document them with system owner and business justification before the brief to preempt the question; (3) Current detection rule inventory for T1053, T1021.002, and T1059 from your SIEM or Sysmon/WEF deployment — absence of rules for these specific LotL techniques is the

concrete evidence gap the brief must convey; (4) Any open vulnerability scanner findings older than 90 days for the affected product categories (IAM/PAM, VPN, ADC) — aged unresolved findings directly evidence the CVSS-volume patching gap Talos identified.

Step 5: Monitor developments — track Talos intelligence publications for follow-on IR-derived IOC releases and campaign-specific indicators; monitor CISA KEV additions for any newly listed legacy vulnerabilities (Log4j, ColdFusion variants) that signal active exploitation confirmation

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Continuous monitoring and threat intelligence integration to identify adverse events, with CTI feeds informing detection tuning and triage decisions

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — formalizes the requirement to receive and action Talos and CISA KEV advisories as authoritative external intelligence sources, NIST SI-4 (System Monitoring) — IOC releases from Talos IR cases must be operationalized into active monitoring rules, not passively noted, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — CISA KEV additions for Log4j or ColdFusion variants constitute a trigger requiring immediate log review against those specific CVE exploitation signatures, NIST IR-5 (Incident Monitoring) — tracking Talos and CISA KEV updates is an organizational incident monitoring activity that must be documented and assigned ownership, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — CISA KEV additions are the authoritative active-exploitation confirmation signal that triggers re-prioritization of legacy CVEs like Log4j and ColdFusion variants in your remediation queue

Compensating: Subscribe to Talos Intelligence blog RSS feed and CISA KEV JSON feed (https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json) — the KEV feed is machine-readable and can be parsed with a simple Python script or `curl | jq` pipeline in a daily cron job to alert on new additions matching your asset inventory CVEs. For Log4j IOC operationalization without SIEM: deploy the free YARA rule `log4shell_exploit.yar` (available from Florian Roth's signature-base repository on GitHub) via ClamAV or a standalone YARA scan scheduled via cron against web server directories. For ColdFusion exploitation monitoring: configure web server access logging (Apache `mod_log_config` or IIS advanced logging) to capture full request URIs and alert on patterns matching known ColdFusion exploit paths (`/CFIDE/`, `/cf_scripts/`, `?url=`, `?source=`) using `grep` or a free Elastic/Graylog pipeline. For Talos IOC ingestion without a TIP: maintain a flat-file IOC list and run daily `grep` sweeps against web server, VPN, and firewall logs using a bash script.

Evidence: Capture BEFORE establishing ongoing monitoring: (1) Baseline snapshot of current IOC blocklist/watchlist state (dates of last update, source, format) — documents pre-monitoring gap so any IOC match discovered after feed integration can be retroactively dated; (2) Web server access logs (Apache `/var/log/apache2/access.log` or IIS `%SystemDrive%\inetpub\logs\LogFiles\`) for the prior 90 days filtered for known Log4j JNDI injection strings (`${jndi:`, `${${::-j}`, `${${lower:j}`) and ColdFusion exploit URI patterns — establishes whether active exploitation preceded this monitoring step; (3) DNS query logs or firewall outbound connection logs for the prior 30 days checking for callbacks to known Log4Shell LDAP/RMI exploit infrastructure domains — Log4j exploitation produces characteristic outbound JNDI callback traffic that may be present in existing logs before a detection rule was deployed; (4) CISA KEV current state export (dated JSON pull) — creates an auditable baseline for tracking future additions relevant to your environment.

Detection Guidance

Detection priorities drawn from the Talos findings fall into three categories.

Identity and authentication anomalies: Hunt for MFA push notification volumes inconsistent with user behavior baselines, multiple pushes in short windows signal MFA fatigue attempts (T1621). Review authentication logs for impossible travel, off-hours access to privileged accounts, and token reuse patterns (T1550.001). Alert on authentication failures followed by success without corresponding legitimate user activity. In Active Directory, monitor for account modification events (T1556), new scheduled task creation by non-admin accounts (T1053), and changes to authentication policy objects.

Living-off-the-land activity: Baseline legitimate administrative tool use (PowerShell, WMI, PsExec, net.exe, cmd.exe) per user and system role. Alert on deviations: scripting interpreter invocations from unexpected parent processes (T1059), SMB lateral movement from workstations rather than jump hosts (T1021.002), and obfuscated command-line arguments (T1027). Network scanning from internal hosts (T1046) is a strong post-compromise signal.

Legacy vulnerability exploitation: If Log4j-vulnerable components or Adobe ColdFusion instances remain in your environment, prioritize log review for JNDI lookup strings in HTTP headers and request parameters, and for ColdFusion-specific exploitation patterns (unusual CFM file creation, unexpected outbound connections from the ColdFusion process). Correlate web application firewall logs against these signatures.

Phishing and reconnaissance uplift: Given Talos' documentation of AI-assisted phishing lure creation, email gateway detections should be reviewed for increased bypass rates. Monitor for active scanning patterns (T1595) against external assets and credential harvesting site registrations mimicking your domain (T1586.002, T1589.001).

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to Cisco Talos 2025 Year in Review for published indicators`	Talos IR engagements produced campaign-specific IOCs including indicators associated with credential abuse, LotL tooling, and legacy vulnerability exploitation; specific hashes, C2 domains, and IPs are published in Talos intelligence reporting at https://blog.talosintelligence.com/five-defender-priorities-from-the-talos-year-in-review/	LOW

Framework Mappings

MITRE-ATTACK

- **T1595** — Active Scanning
- **T1059** — Command and Scripting Interpreter
- **T1046** — Network Service Discovery
- **T1133** — External Remote Services
- **T1021.002** — SMB/Windows Admin Shares
- **T1078** — Valid Accounts
- **T1621** — Multi-Factor Authentication Request Generation
- **T1053** — Scheduled Task/Job
- **T1027** — Obfuscated Files or Information
- **T1556** — Modify Authentication Process
- **T1588.002** — Tool

- **T1550.001** — Application Access Token
- **T1556.006** — Multi-Factor Authentication
- **T1586.002** — Email Accounts
- **T1190** — Exploit Public-Facing Application
- **T1589.001** — Credentials

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **AC-3** — Access Enforcement
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

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)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1595	Active Scanning	Reconnaissance
T1059	Command and Scripting Interpreter	Execution
T1046	Network Service Discovery	Discovery
T1133	External Remote Services	Persistence
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1078	Valid Accounts	Defense-Evasion
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1053	Scheduled Task/Job	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1556	Modify Authentication Process	Credential-Access
T1588.002	Tool	Resource-Development
T1550.001	Application Access Token	Defense-Evasion
T1556.006	Multi-Factor Authentication	Credential-Access
T1586.002	Email Accounts	Resource-Development
T1190	Exploit Public-Facing Application	Initial-Access
T1589.001	Credentials	Reconnaissance

Sources

Source	URL	Tier
Cisco Talos Blog	https://blog.talosintelligence.com/five-defender-priorities-from-th...	T3
CVE-2025-0111 PAN-OS: Authenticated File Read Vulnerability in ...	https://security.paloaltonetworks.com/CVE-2025-0111	T3
Adobe Patches 55 Vulnerabilities Across 11 Products - SecurityIT	https://www.show.it/en/adobe-patches-55-vulnerabilities-across-11-p...	T3
APSB26-12 - Adobe Security Bulletin	https://helpx.adobe.com/security/products/coldfusion/apsb26-12.html	T3
Mass Exploitation Campaign Targeting Adobe ColdFusion Servers ...	https://www.secpod.com/blog/mass-exploitation-campaign-targeting-ad...	T3

Generated 2026-04-28 18:49 UTC by TJS Security Command Center