INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-16 13:49 UTC

Financial Services Under Siege: DPRK Crypto Heists, China Espionage, and eCrime Surge Define 2025-2026 Threat Year

SECURITY ANALYSIS | HIGH | CVSS 9.5

SCC Item ID	SCC-STY-2026-0137
Type	Security Analysis
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Financial institutions, cryptocurrency exchanges, fintech platforms, insurance entities, Microsoft 365 environments
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Financial Services Threat Landscape Report documents a coordinated, multi-actor assault on global financial institutions, with DPRK-affiliated groups stealing $2.02 billion in digital assets, a 51% year-over-year increase, while eCrime groups named 423 financial entities on ransomware leak sites and China-nexus actors conducted parallel intelligence collection operations. Hands-on-keyboard intrusions across the sector rose 43% year-over-year, driven by accelerating adversary breakout speeds and identity-focused attack paths that bypass traditional perimeter defenses. This report signals a structural shift: financial institutions now face simultaneous pressure from state-sponsored theft, espionage, and organized cybercrime, outpacing reactive defense models built for single-vector threats.

Technical Analysis

CrowdStrike's 2026 Financial Services Threat Landscape Report presents a sector under sustained, multi-vector siege from three distinct adversary categories operating with increasing speed and sophistication.

DPRK-nexus actors, including Lazarus Group affiliates and FAMOUS CHOLLIMA, drove the most financially damaging campaigns. Their $2.02 billion in digital asset theft, up 51% year-over-year, reflects a deliberate strategic mission: cryptocurrency and fintech platforms serve as sanctions-evasion infrastructure for the North Korean state. These actors combined supply chain compromise (T1195, T1195.002) with credential theft and MFA bypass (T1621, T1550.001, CWE-287) to gain initial access, then used living-off-the-land tradecraft and legitimate remote access tooling (T1021.001, T1133) to persist and exfiltrate. The 43% increase in hands-on-keyboard intrusions reflects adversaries moving past automated tooling toward interactive sessions

that evade behavior-based detections tuned for scripted attack patterns.

FAMOUS CHOLLIMA's insider threat tradecraft, placing operatives inside financial firms as remote employees, represents a particularly difficult detection problem. This vector exploits hiring processes, not technical controls, and maps directly to T1586 (Compromise Accounts) and T1657 (Financial Theft), with CWE-287 (Improper Authentication) as the underlying weakness when identity verification fails at onboarding.

ECrime actors, notably Scattered Spider, targeted Microsoft 365 environments and financial sector identity infrastructure with social engineering-led intrusion chains. Scattered Spider's hallmark is voice phishing and SMS-based MFA fatigue attacks (T1621) that bypass hardware token controls by targeting help desk operators directly. Session hijacking (T1539) and cookie theft follow successful social engineering, enabling lateral movement without password compromise. The group's targeting of 423 named financial entities on ransomware leak sites, not all confirmed as successful breaches, indicates a broad targeting posture and willingness to pressure victims publicly before ransom payment.

China-nexus adversaries pursued a different objective: intelligence collection against developing market financial infrastructure. CrowdStrike did not attribute these operations to a specific named actor in the summary data provided. The observed targeting pattern - financial entities in emerging economies rather than direct theft - is consistent with publicly disclosed Chinese government interests in Belt and Road financial infrastructure, though attribution is inferred from targeting, not from technical or operational indicators. Techniques observed include phishing (T1566), exploitation of public-facing applications (T1190), and data archival before exfiltration (T1560).

Across all three adversary categories, the report identifies identity as the primary attack surface. Credential theft, MFA bypass, session hijacking, and valid account abuse (T1078) collectively represent the dominant intrusion pathway. CWE-494 (Download of Code Without Integrity Check) and CWE-426 (Untrusted Search Path) appear in supply chain-linked intrusions, consistent with DPRK tradecraft observed in prior cryptocurrency platform compromises. AI-assisted social engineering, generating convincing synthetic personas, scripted vishing calls, and tailored spearphishing content, is cited as a compounding factor accelerating the effectiveness of identity-focused attacks.

The report's core defensive implication: controls optimized for known-malware detection and network-perimeter blocking are structurally mismatched against adversaries who authenticate legitimately, move interactively, and adapt in real time. Identity governance, behavioral detection in authentication pipelines, and insider threat programs are no longer optional capabilities for financial institutions.

Action Checklist

1. Step 1: Assess exposure, inventory all cryptocurrency custody, trading, and fintech platform integrations; identify any Microsoft 365 tenant exposure to external identity federation or third-party app grants that could be abused for session hijacking
2. Step 2: Review controls, audit MFA implementation across all privileged and customer-facing access paths; verify help desk identity verification procedures cannot be bypassed via voice phishing or SMS; confirm EDR coverage on all endpoints with access to financial transaction systems; validate software supply chain integrity checks (code signing, dependency verification) to address CWE-494 and CWE-426
3. Step 3: Update threat model, add Lazarus Group, FAMOUS CHOLLIMA, and Scattered Spider TTPs to your threat register; map T1621 (MFA Request Generation), T1550.001 (Pass the Cookie), T1539 (Steal Web Session Cookie), and T1195.002 (Compromise Software Supply Chain) against your current

detection coverage gaps

4. Step 4: Audit insider threat and hiring controls, validate remote employee identity verification processes against FAMOUS CHOLLIMA's documented tactic of placing operatives inside financial firms; review contractor and vendor onboarding identity assurance procedures

5. Step 5: Communicate findings, brief leadership on the 43% increase in hands-on intrusions and $2.02 billion in sector-wide DPRK crypto theft as evidence that adversary tempo now exceeds reactive defense cycles; present specific gaps in identity and supply chain controls as the prioritized investment case

6. Step 6: Monitor developments, track CrowdStrike's published IOC releases for this report (https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-financial-services-threat-landscape-report/), CISA advisories referencing DPRK financial sector operations, FinCEN enforcement actions (https://www.fincen.gov/enforcement-history), and OFAC sanctions (https://ofac.treasury.gov/specially-designated-nationals-list) related to DPRK cryptocurrency theft; watch for Scattered Spider indictment follow-on disclosures affecting named financial targets

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if any of the following are confirmed: (1) M365 OAuth token issued to unrecognized service principal with Microsoft Graph Mail.Read or Files.ReadWrite scope — indicator of Lazarus-style T1550.001 session hijacking; (2) remote employee VPN source IP resolves to DPRK, Chinese, or known FAMOUS CHOLLIMA proxy infrastructure; (3) outbound transfer of cryptocurrency assets to addresses on OFAC SDN list — triggers mandatory SAR filing with FinCEN within 30 days under 31 CFR 1020.320; (4) EDR alert on any endpoint touching crypto custody systems matching Lazarus Group process injection or BlindingCan/BLINDINGCAN implant signatures.
Recovery Notes	Post-containment, rotate all M365 service principal credentials and OAuth refresh tokens (not just access tokens) before restoring normal operations, as Lazarus Group is documented maintaining persistent access via refresh token abuse even after initial credential rotation. For any crypto custody or trading platform accounts, assume session cookies are compromised and force full re-authentication with phishing-resistant MFA for all users — do not rely on existing session state. Monitor M365 Sign-in Logs and crypto platform transaction logs continuously for 30 days post-recovery, specifically watching for ServicePrincipalSignIns from previously unseen ASNs and any transaction authorization requests initiated outside normal business hours, which is a documented Lazarus Group operational pattern.

Forensic Artifacts	M365 Unified Audit Log — 'Add OAuth2PermissionGrant' and 'Consent to application' events correlating to Lazarus Group T1550.001 (Pass the Cookie) and T1539 (Steal Web Session Cookie) via malicious OAuth app registration; retain minimum 90 days per FinCEN BSA requirements | EntraID Non-Interactive Sign-in Logs — ServicePrincipalSignIns with resource='Microsoft Graph' and clientAppUsed='Other clients' from anomalous ASNs; these are left by automated Lazarus tooling using stolen OAuth tokens after initial session hijacking | Sysmon Event ID 10 (Process Access) logs on endpoints running crypto wallet software or trading platform clients — Lazarus Group implants inject into browser processes (chrome.exe, firefox.exe) specifically to steal session cookies via ReadProcessMemory; filter on GrantedAccess=0x1010 targeting browser PIDs | Git repository audit logs (GitHub Enterprise, GitLab, Bitbucket) showing 'git archive', 'git clone --mirror', or large blob downloads outside business hours by accounts matching FAMOUS CHOLLIMA insider placement profile — specifically accounts with mismatched timezone activity vs. declared work location | Cryptocurrency gateway transaction logs and blockchain mempool monitoring exports for outbound transfers to addresses matching OFAC SDN list entries or CrowdStrike/Chainalysis published Lazarus Group wallet clusters — these constitute mandatory SAR evidence if DPRK nexus is confirmed

Per-Action IR Details

Step 1: Assess exposure — inventory all cryptocurrency custody, trading, and fintech platform integrations; identify any Microsoft 365 tenant exposure to external identity federation or third-party app grants that could be abused for session hijacking

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish IR capability, asset visibility, and pre-incident resource mapping aligned to CSF [GV, ID, PR] functions

Controls: NIST IR-4 (Incident Handling) — implement handling capability with preparation as foundational phase, NIST SI-4 (System Monitoring) — establish visibility into M365 OAuth app grants and federation trust relationships, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — enumerate all crypto custody endpoints, trading platform API integrations, and fintech connectors, CIS 2.1 (Establish and Maintain a Software Inventory) — catalog third-party M365 app registrations and delegated permission scopes

Compensating: Run the free Microsoft 365 'EntraID App Audit' via PowerShell: Connect-MgGraph; Get-MgServicePrincipal -All | Where-Object {$_.KeyCredentials -or $_.PasswordCredentials} | Select DisplayName, AppId, SignInAudience | Export-Csv m365_app_audit.csv. For on-premises crypto platform integrations, use osquery with query 'SELECT * FROM listening_ports WHERE port IN (8332,8333,30303,9000)' to fingerprint blockchain node listeners. Cross-reference against CIS 1.1 asset inventory.

Evidence: Before remediating M365 app grants, preserve: Azure AD Audit Logs (AuditLogs table in Log Analytics) filtering on 'Add OAuth2PermissionGrant' and 'Consent to application' operations; M365 Unified Audit Log entries for 'Add service principal credentials' events; EntraID Sign-in Logs filtered on ServicePrincipalSignIns for non-interactive auth with resource = 'Microsoft Graph' (indicator of token abuse by Lazarus-style implants); exported JSON of all OAuth2PermissionGrants via MS Graph API GET /oauth2PermissionGrants before any revocation action.

Step 2: Review controls — audit MFA implementation across all privileged and customer-facing access paths; verify help desk identity verification procedures cannot be bypassed via voice phishing or SMS; confirm EDR coverage on all endpoints with access to financial transaction systems; validate software supply chain integrity checks (code signing, dependency verification) to address CWE-494 and CWE-426

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Pre-incident control validation and gap remediation to reduce dwell time when Scattered Spider or FAMOUS CHOLLIMA TTPs are employed against identity and supply chain entry points

Controls: NIST IA-3 (Device Identification and Authentication) — enforce phishing-resistant MFA (FIDO2/passkeys) not bypassable via SS7 or voice social engineering used by Scattered Spider, NIST SI-7 (Software, Firmware, and Information Integrity) — enforce code signing verification and dependency hash checking to counter CWE-494 (Download of Code Without Integrity Check) and CWE-426 (Untrusted Search Path) exploited in supply chain intrusions, NIST SI-2 (Flaw Remediation) — validate patch state of all endpoints in financial transaction processing paths, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA on all customer-facing and privileged access paths; SMS OTP is insufficient against Scattered Spider SIM-swap capability, CIS 6.5 (Require MFA for Administrative Access) — require phishing-resistant MFA for all admin accounts, specifically M365 Global Admin and privileged identity management roles, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — include supply chain dependency scanning in vuln management scope

Compensating: For help desk bypass validation: conduct tabletop simulation where red team calls help desk posing as executive requesting MFA reset — document whether out-of-band identity verification (manager callback, government ID, hardware token possession) is enforced. For supply chain integrity without enterprise tooling: implement 'pip-audit' for Python dependencies and 'npm audit' for Node.js; use OSSEC or Wazuh (free) file integrity monitoring on directories containing trading platform binaries with SHA-256 baseline hashing via 'sha256sum -c checksums.txt' in cron. For EDR gap identification: run Sysmon with SwiftOnSecurity config and validate coverage by checking 'Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational' returns events from all endpoints touching payment rails.

Evidence: Preserve before audit: Windows Security Event Log Event ID 4625 (Failed Logon) and 4648 (Explicit Credential Logon) from help desk workstations and IT admin systems — Scattered Spider pivots through compromised help desk accounts; M365 MFA registration events from EntraID Audit Log ('User registered security info' operations) to identify accounts with only SMS MFA enrolled; Sysmon Event ID 11 (File Create) logs from software build directories and deployment pipelines to establish baseline for supply chain tampering detection; npm/pip dependency lock files (package-lock.json, requirements.txt) current state before any remediation for forensic comparison if a supply chain compromise is later discovered.

Step 3: Update threat model — add Lazarus Group, FAMOUS CHOLLIMA, and Scattered Spider TTPs to your threat register; map T1621 (MFA Request Generation), T1550.001 (Pass the Cookie), T1539 (Steal Web Session Cookie), and T1195.002 (Compromise Software Supply Chain) against your current detection coverage gaps

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Threat modeling and detection engineering prerequisite to DE.AE-07 (integrate CTI into adverse event analysis) and DE.AE-02 (analyze potentially adverse events with threat context)

Controls: NIST RA-3 (Risk Assessment) — formally assess likelihood and impact of Lazarus Group and Scattered Spider TTPs against your specific crypto custody and M365 environment, NIST SI-5 (Security Alerts, Advisories, and Directives) — ingest CISA advisories on DPRK financial sector operations (AA24-038A and related) as authoritative TTP source, NIST IR-8 (Incident Response Plan) — update IR plan to include DPRK crypto theft and Scattered Spider identity attack playbook branches, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — integrate ATT&CK TTP mapping into vuln management prioritization to surface T1195.002 supply chain exposure

Compensating: Deploy Sigma rules (free, community-maintained) for each mapped technique: use 'sigma/rules/cloud/azure/azure_ad_mfa_fatigue.yml' for T1621 MFA push fatigue detection against Entra ID logs; use 'sigma/rules/windows/process_creation/proc_creation_win_browsers_credential_dump.yml' variants for T1539 cookie theft via browser process injection. Convert Sigma to native query format with 'sigma convert -t splunk' or 'sigma convert -t elasticsearch'. For T1550.001 Pass-the-Cookie, implement conditional access policy in M365 requiring compliant device claim on all session tokens — this is free within M365 E3/E5 licensing. Map coverage gaps manually in a spreadsheet using MITRE ATT&CK Navigator (free web tool at attack.mitre.org/resources/attack-navigator/) exported as JSON layer.

Evidence: Preserve before threat model update: current SIEM/log query outputs showing which of T1621, T1550.001, T1539, T1195.002 generate zero alerts in the last 90 days — these gaps are forensic evidence of pre-existing blind spots; M365 Conditional Access policy export (Get-MgIdentityConditionalAccessPolicy | ConvertTo-Json) as baseline snapshot; current EDR exclusion lists from all endpoints touching crypto wallets or trading APIs — Lazarus tooling frequently exploits AV/EDR exclusion paths to maintain persistence.

Step 4: Audit insider threat and hiring controls — validate remote employee identity verification processes against FAMOUS CHOLLIMA's documented tactic of placing operatives inside financial firms; review contractor and vendor onboarding identity assurance procedures

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: Identify indicators of insider placement via behavioral anomaly analysis aligned to DE.CM-03 (monitor personnel activity and technology usage for anomalous patterns)

Controls: NIST IR-4 (Incident Handling) — extend incident handling scope to include insider threat as a distinct incident category with FAMOUS CHOLLIMA operative placement as a named scenario, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — conduct structured review of remote employee activity logs for FAMOUS CHOLLIMA behavioral indicators: anomalous git commit patterns, code exfiltration to personal repos, VPN geolocation inconsistencies, NIST PS-3 (Personnel Screening) — validate that background checks for remote hires include live video identity verification against government-issued ID, not just document submission, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — enumerate all remote contractor and vendor accounts; identify accounts with access to source code repositories, financial transaction systems, or crypto key management

Compensating: For behavioral detection without a UEBA platform: query M365 Audit Logs for remote employees exhibiting FAMOUS CHOLLIMA indicators — 'Search-UnifiedAuditLog -Operations FileDownloaded,FileCopied -ResultSize 1000' filtered on users with >500 file downloads in 24 hours; for git-based exfiltration, enable GitHub/GitLab audit log streaming and alert on 'git clone' or 'git archive' operations outside business hours from new IP ranges. For identity verification of existing remote employees, implement a surprise live video check policy requiring government ID alongside face match — free to operationalize with existing video conferencing tools. Cross-reference employee-provided addresses against OFAC SDN list using free OFAC sanctions search API for contractor onboarding.

Evidence: Preserve before any HR or access actions: M365 Unified Audit Log entries for the target employee accounts covering 90 days of FileAccessed, FileDownloaded, and SensitiveFileAccessed operations; git repository audit logs showing commit authorship email addresses (FAMOUS CHOLLIMA operatives have been documented using multiple persona emails on single accounts); VPN connection logs showing geolocation of remote employee connections — IP addresses resolving to China, Russia, or DPRK proxy infrastructure are documented FAMOUS CHOLLIMA indicators; employee-submitted identity documents and video interview recordings if available — preserve as potential evidence chain for law enforcement referral.

Step 5: Communicate findings — brief leadership on the 43% increase in hands-on intrusions and $2.02 billion in sector-wide DPRK crypto theft as evidence that adversary tempo now exceeds reactive defense cycles; present specific gaps in identity and supply chain controls as the prioritized investment case

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned communication and investment prioritization to update policies and improve detection capability, mapped to CSF [GV, ID] governance functions

Controls: NIST IR-6 (Incident Reporting) — establish reporting cadence to leadership that includes sector-level threat intelligence alongside organization-specific gap findings, NIST IR-8 (Incident Response Plan) — use gap findings to formally update IR plan investment priorities and resource allocation, specifically for identity and supply chain controls, NIST RA-3 (Risk Assessment) — present quantified risk: $2.02B sector theft and 43% intrusion increase translates to specific residual risk exposure for leadership to approve or accept, CIS 7.2 (Establish and Maintain a Remediation Process) — formalize risk-based remediation prioritization with identity gaps (MFA bypass, session hijacking) and supply chain gaps (CWE-494, CWE-426) ranked by FAMOUS CHOLLIMA and Lazarus Group exploitation likelihood

Compensating: For teams without a formal GRC platform: produce a one-page executive risk brief using the NIST CSF 2.0 Organizational Profile format (free template at nist.gov/cyberframework) — map each identity and supply chain gap to a CSF Function/Category with current vs. target maturity. Quantify investment case using FS-ISAC's published average cost of a financial sector breach rather than proprietary data. Share brief via encrypted email with audit trail — do not distribute sector intelligence data (CrowdStrike report findings) via unencrypted channels.

Evidence: Compile before leadership brief: output of M365 app audit from Step 1, MFA enrollment gap report from Step 2, and ATT&CK coverage gap layer from Step 3 as appendices — these are your organization-specific evidence that sector-level threat is locally relevant; document any open audit findings from prior assessments that overlap with

Lazarus/Scattered Spider TTPs as evidence of known-unmitigated risk; retain all evidence artifacts in tamper-evident storage (write-once log archive or hashed ZIP with documented chain of custody) per NIST AU-9 (Protection of Audit Information) in case findings later support regulatory disclosure.

Step 6: Monitor developments — track CrowdStrike's published IOC releases for this report, CISA advisories referencing DPRK financial sector operations, and FinCEN or OFAC enforcement actions related to DPRK cryptocurrency theft; watch for Scattered Spider indictment follow-on disclosures affecting named financial targets

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Continuous intelligence integration to update detection and share findings, aligned to DE.AE-07 (integrate CTI into adverse event analysis) and RS.MA-01 (coordinate IR with relevant third parties)

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — establish formal process to receive and act on CISA DPRK advisories (AA24-038A series) and FinCEN/OFAC DPRK cryptocurrency enforcement notices within defined SLA, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — integrate newly published Lazarus Group and Scattered Spider IOCs into log review queries within 24 hours of CISA advisory publication, NIST IR-5 (Incident Monitoring) — track and document sector-wide incident disclosures from Scattered Spider indictment proceedings as external incident intelligence informing your own monitoring posture, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate IOC feeds from CrowdStrike, CISA, and FS-ISAC into vulnerability and threat management process as standing input sources

Compensating: Subscribe to CISA's free email alerts at cisa.gov/news-events/cybersecurity-advisories filtered for 'North Korea' and 'financial sector' keywords. Ingest CrowdStrike published IOCs (when released) into MISP (free open-source threat intelligence platform) and auto-export to Sigma rules or Suricata rules for network-layer detection. Monitor OFAC SDN list updates via free RSS feed or OFAC API for newly sanctioned DPRK-linked cryptocurrency addresses — block these at firewall/crypto gateway within 24 hours of addition per OFAC compliance obligation. Set Google Alerts for 'Scattered Spider indictment' and 'DPRK cryptocurrency financial' for passive intelligence collection at zero cost.

Evidence: Establish and preserve ongoing evidence collection: retain all CISA advisories and IOC feeds as dated, archived PDFs with hash verification (sha256sum) to establish compliance audit trail for regulatory examiners; maintain a rolling 90-day Suricata/Zeek PCAP index on perimeter traffic filtered for known Lazarus C2 IP ranges published in CISA advisories — this constitutes forensic evidence if a compromise is later confirmed; document all OFAC-sanctioned DPRK cryptocurrency addresses blocked at your gateway with timestamps — FinCEN examination may require evidence of sanctions compliance monitoring as a regulatory obligation for covered financial institutions.

Detection Guidance

Detection priorities for this threat landscape fall into four categories, ordered by observed adversary prevalence.

Identity and Authentication Anomalies: Hunt for MFA push fatigue patterns, repeated authentication requests to the same user within short windows (T1621). Flag out-of-hours logins from new geographic locations or ASNs not associated with the user's baseline. Monitor for session token reuse from IP addresses inconsistent with the authentication origin (T1550.001, T1539). In Microsoft 365 environments, audit OAuth application consent grants, service principal activity, and mailbox delegation changes - Scattered Spider frequently abuses these post-access.

Help Desk and Identity Verification: Review call logs and ticket records for password reset and MFA re-enrollment requests that were approved without secondary identity verification. Scattered Spider's initial access frequently routes through help desk social engineering; detection requires process audit, not just log review.

Supply Chain and Execution Integrity: Alert on unsigned or newly appearing executables in financial application directories (CWE-494, T1574.001). Monitor for DLL search order hijacking indicators, unexpected DLLs loaded from user-writable paths by privileged processes (T1574.001, CWE-426). Flag software update processes that retrieve payloads over unencrypted channels or from domains registered within the last 90 days.

Insider Threat Indicators: For remote employees, establish behavioral baselines, working hours, systems accessed, data volumes transferred. Alert on access to systems outside job function, large internal data transfers, or attempts to enumerate financial transaction databases without a support ticket. FAMOUS CHOLLIMA operatives tend to access high-value data quickly after onboarding.

Log Sources to Prioritize: Azure AD / Entra ID sign-in logs and audit logs; endpoint telemetry for process creation chains involving scripting engines (PowerShell, cmd.exe) launched by financial application parent processes; network logs for C2 beaconing patterns (T1071), particularly HTTPS to low-reputation domains with high beacon regularity; email gateway logs for spearphishing delivery (T1566) targeting finance and treasury staff.

Specific IOCs: CrowdStrike's published report contains C2 infrastructure indicators, payload hashes, and tool signatures associated with these campaigns. Security teams should retrieve these directly from the CrowdStrike 2026 Financial Services Threat Landscape Report blog post (https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-financial-services-threat-landscape-report/). Note: Additional IOC feeds may be available through the CrowdStrike Adversary Intelligence portal, which may require subscription. Validate IOC recency before operational use.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to CrowdStrike 2026 Financial Services Threat Landscape Report for published indicators`	C2 infrastructure indicators, payload hashes, and tool signatures associated with Lazarus Group, FAMOUS CHOLLIMA, and Scattered Spider campaigns are documented in the CrowdStrike report and Adversary Intelligence portal; specific values were not included in the summary data provided for this analysis	LOW

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1195** — Supply Chain Compromise
- **T1071** — Application Layer Protocol
- **T1021.001** — Remote Desktop Protocol
- **T1190** — Exploit Public-Facing Application
- **T1133** — External Remote Services
- **T1574.001** — DLL

- **T1550.001** — Application Access Token
- **T1195.002** — Compromise Software Supply Chain
- **T1560** — Archive Collected Data
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1539** — Steal Web Session Cookie
- **T1562** — Impair Defenses
- **T1621** — Multi-Factor Authentication Request Generation
- **T1586** — Compromise Accounts
- **T1657** — Financial Theft

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **CM-3** — Configuration Change Control
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity 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
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

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

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1195	Supply Chain Compromise	Initial-Access
T1071	Application Layer Protocol	Command-And-Control
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1190	Exploit Public-Facing Application	Initial-Access
T1133	External Remote Services	Persistence

Technique ID	Technique Name	Tactic
T1574.001	DLL	Persistence
T1550.001	Application Access Token	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access
T1560	Archive Collected Data	Collection
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1539	Steal Web Session Cookie	Credential-Access
T1562	Impair Defenses	Defense-Evasion
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1586	Compromise Accounts	Resource-Development
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-financial-s...	T3
	https://www.crowdstrike.com/en-us/blog/crowdstrike-named-leader-gar...	T3
	https://www.crowdstrike.com/en-us/blog/announcing-threat-ai-industr...	T3
	https://www.crowdstrike.com/en-us/blog/crowdstrike-2024-global-thre...	T3
CrowdStrike 2026 Financial Services Threat Landscape ...	https://www.crowdstrike.com/content/crowdstrike-www/locale-sites/us...	T3

Generated 2026-05-16 13:49 UTC by TJS Security Command Center