INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-16 06:38 UTC

DPRK Crypto Theft, China Espionage, and BGH Ransomware Converge Against Financial Sector in 2025-2026

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0322
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Financial services organizations broadly; cryptocurrency and fintech platforms; Microsoft 365 environments; organizations using CrowdStrike Falcon (vendor context only)
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Financial Services Threat Landscape Report documents a three-front escalation against financial institutions: DPRK-linked actors stole $2.02 billion in digital assets through IT worker infiltration and supply chain compromise; China-nexus actor MURKY PANDA conducted espionage operations targeting Microsoft 365 environments; and Big Game Hunting ransomware groups named 27% more financial sector victims year-over-year. Hands-on-keyboard, operator-driven adaptive attacks rose 43% globally, meaning automated defenses alone are insufficient. The convergence of nation-state theft, espionage, and AI-accelerated fraud across shared identity and cloud infrastructure represents the defining threat profile for financial services in this period.

Technical Analysis

Source: CrowdStrike 2026 Financial Services Threat Landscape Report. Confidence: HIGH for trend data; MEDIUM for specific attribution pending independent corroboration.

Three distinct but overlapping threat clusters are active against financial sector infrastructure:

1. DPRK-nexus actors: Operators placed fraudulent IT workers inside target organizations (T1656, impersonation; T1195.002, supply chain compromise via software). Once inside, actors exfiltrated credentials (T1110, T1087), moved laterally via valid accounts (T1078, T1550), and exfiltrated assets (T1567). CWE-494 (download without integrity check) and CWE-506 (embedded malicious code) reflect the supply chain insertion vector. Total confirmed digital asset theft: $2.02B.

2. MURKY PANDA (China-nexus): Targeted Microsoft 365 environments within financial institutions consistent with long-term collection objectives. Techniques align with T1566/T1566.001 (phishing), T1021 (remote services), T1055 (process injection), T1657 (cloud infrastructure discovery), and T1588/T1588.005 (capability acquisition). CWE-287 (improper authentication) is the relevant weakness category for M365 identity exploitation.

3. BGH ransomware groups: Data extortion and encryption operations (T1486, data encrypted for impact; T1489, service stop) against financial sector organizations increased 27% by victim count on leak sites year-over-year. Ransomware access paths overlap with phishing (T1566), valid account abuse (T1078), and lateral movement (T1021).

Cross-cutting enabler: AI-accelerated social engineering, voice cloning, deepfake identity fraud, LLM-assisted phishing, is lowering the cost and raising the scale of credential theft across all three clusters.

CWEs: CWE-494 (supply chain integrity), CWE-287 (authentication weakness), CWE-506 (embedded malicious code).

No CVE IDs associated with this campaign report. No patch exists for threat actor TTPs, mitigation is control-based.

Action Checklist

1. Step 1: Containment, Audit all third-party IT contractors and vendor accounts with privileged access to financial systems. Suspend accounts that cannot be verified through out-of-band identity confirmation. Apply conditional access policies to Microsoft 365 tenants blocking authentication from non-managed or unregistered devices. Priority: all organizations with contractor or vendor access to cloud tenants.
2. Step 2: Detection, Hunt for anomalous Microsoft 365 sign-in patterns: logins from unexpected geographies, token reuse without re-authentication (T1550), and service principal permission escalations. Review audit logs for T1087 (account discovery) and T1567 (exfiltration to cloud storage). For DPRK IT worker vector, correlate HR onboarding records against device registrations and VPN endpoints, mismatches are a primary indicator. Query identity provider logs for T1078 (valid account abuse) events outside business hours.
3. Step 3: Eradication, Enforce phishing-resistant MFA (FIDO2/hardware token) across all Microsoft 365 accounts; remove SMS-based MFA for privileged roles. Implement software supply chain controls: verify integrity of all third-party packages and contractor-supplied code against known-good hashes (mitigates CWE-494, CWE-506). Revoke and reissue credentials for any account flagged in Step 2 review. Segment cryptocurrency custody and fintech API access behind dedicated identity providers separate from corporate M365 tenants.
4. Step 4: Recovery, Validate MFA enforcement via Azure AD/Entra ID sign-in logs; confirm zero successful authentications using legacy auth protocols. Confirm supply chain review completion with documented sign-off for all active contractor accounts. Run a tabletop exercise simulating a BGH ransomware event to validate backup isolation and recovery time objectives. Monitor M365 audit logs for 30 days post-remediation for residual T1021 and T1055 activity.
5. Step 5: Post-Incident, Conduct insider threat program gap assessment against NIST SP 800-53 PS (Personnel Security) and AT (Awareness and Training) control families. Evaluate AI-generated voice/deepfake verification procedures for wire transfer authorization and executive communication channels. Brief board and senior leadership on BGH victim naming risk, reputational exposure from leak

site publication is a board-level concern independent of operational impact. Map current detection coverage against MITRE ATT&CK techniques listed in this report; prioritize gaps in T1656, T1550, and T1574.001 detection.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO, Legal, and external IR retainer if any of the following are confirmed: a contractor account is identified as a DPRK IT worker placement, MURKY PANDA OAuth persistence survives credential rotation in the M365 tenant, BGH ransomware deployment is detected on any system with access to customer financial data or cryptocurrency custody infrastructure triggering potential FinCEN SAR obligations and state breach notification timelines.
Recovery Notes	Post-containment recovery must validate that legacy authentication is fully blocked in Entra ID before restoring normal contractor access — a single SMS-MFA or basic-auth enabled account reintroduces the primary DPRK and MURKY PANDA access vectors. Monitor M365 UAL for MailItemsAccessed, FileDownloaded, and service principal permission changes for a minimum of 30 days post-remediation, as MURKY PANDA OAuth persistence and DPRK IT worker re-infiltration attempts have been observed within weeks of initial detection. Financial regulators (OCC, FFIEC, SEC) may require notification of this campaign's scope even absent confirmed data exfiltration — engage Legal within 72 hours of incident declaration to assess reporting obligations.
Forensic Artifacts	Microsoft 365 Unified Audit Log (UAL) — Operation types 'MailItemsAccessed', 'Add app role assignment to service principal', 'FileUploaded to external SharePoint', and 'UserLoggedIn' from non-managed devices: primary artifact for MURKY PANDA M365 espionage and DPRK T1078 valid account abuse. Retain full 90-day export before any account remediation. | Entra ID Risky Sign-in and Risk Detection logs — fields RiskDetail, RiskEventType, and IPAddress: captures impossible travel detections and anonymous IP flags generated by DPRK IT workers routing through VPN endpoints inconsistent with their claimed contractor geolocation. | Azure AD OAuth2PermissionGrants and AppRoleAssignments export — application DisplayName, PermissionType (Delegated vs Application), and ConsentType: primary persistence artifact for MURKY PANDA operations, which survive password resets and MFA changes when OAuth app grants are not explicitly revoked. | Contractor device registration records from Entra ID/Intune — DeviceId, OperatingSystem, RegisteredDateTime, and ComplianceState correlated against HR onboarding dates and contractor-provided work location: the primary indicator for DPRK IT worker infiltration where a non-corporate, non-compliant device registers within days of hire from an unexpected jurisdiction. | Git repository commit history and dependency manifest snapshots (package-lock.json, requirements.txt, Pipfile.lock, go.sum) from all contractor-contributed codebases — SHA-256 hashes of delivered binaries compared against PyPI, npm, and GitHub release hashes: forensic artifact for CWE-494/CWE-506 supply chain implant detection consistent with DPRK code-poisoning TTPs documented in this campaign.

Per-Action IR Details

Step 1: Containment — Audit all third-party IT contractors and vendor accounts with privileged access to financial systems. Suspend accounts that cannot be verified through out-of-band identity confirmation. Apply conditional access policies to Microsoft 365 tenants blocking authentication from non-managed or unregistered devices. Priority: all organizations with contractor or vendor access to cloud tenants.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), NIST IA-8 (Identification and Authentication — Non-Organizational Users), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Export Azure AD/Entra ID sign-in logs via Microsoft Graph API using the free PowerShell module (Install-Module Microsoft.Graph) and run: Get-MgAuditLogSignIn -Filter "userType eq 'Guest' or clientAppUsed eq 'Exchange ActiveSync'" to enumerate contractor and vendor authentications. Cross-reference output against your HR/vendor roster in a spreadsheet to identify unverifiable accounts. For conditional access enforcement without Entra ID P1/P2 licensing, use Security Defaults in Azure AD (free tier) to block legacy authentication protocols immediately — this single toggle eliminates a primary DPRK IT worker persistence vector.

Evidence: Before suspending accounts, preserve: (1) Entra ID/Azure AD sign-in logs (portal.azure.com > Azure Active Directory > Sign-in logs) filtered for all contractor UPNs — export as CSV capturing IP addresses, device IDs, and authentication methods used; (2) Microsoft 365 Unified Audit Log (UAL) entries for OfficeActivity type 'UserLoggedIn' and 'Add member to role' correlated to contractor accounts within the prior 90 days; (3) Conditional Access policy export (current state snapshot) before modification, preserving the pre-remediation configuration as forensic baseline; (4) Device compliance records from Intune/Endpoint Manager for all registered devices associated with contractor UPNs, capturing last check-in timestamps and compliance state.

Step 2: Detection — Hunt for anomalous Microsoft 365 sign-in patterns: logins from unexpected geographies, token reuse without re-authentication (T1550), and service principal permission escalations. Review audit logs for T1087 (account discovery) and T1567 (exfiltration to cloud storage). For DPRK IT worker vector, correlate HR onboarding records against device registrations and VPN endpoints — mismatches are a primary indicator. Query identity provider logs for T1078 (valid account abuse) events outside business hours.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1550 (Use Alternate Authentication Material — Pass-the-Token), MITRE ATT&CK T1078 (Valid Accounts), MITRE ATT&CK T1087 (Account Discovery), MITRE ATT&CK T1567 (Exfiltration to Cloud Storage)

Compensating: Use the free Microsoft 365 Audit Log Search (requires E3 minimum, 90-day retention) with these specific queries: (1) In the M365 Compliance Center, filter UAL for Operation='FileUpload' AND SiteUrl containing 'sharepoint.com' OR 'onedrive.com' cross-referenced against external recipient domains to surface T1567 exfiltration. (2) Query for Operation='Add app role assignment to service principal' to catch MURKY PANDA-style service principal escalation. (3) For token reuse (T1550), use the free Hawk PowerShell tool (github.com/T0pCyber/hawk) which parses UAL for impossible travel, token anomalies, and OAuth app grants without requiring Entra ID P2. For DPRK IT worker correlation, build a two-column spreadsheet mapping HR start dates to first device registration timestamps in Entra ID — a delta greater than 7 days with a non-corporate device fingerprint is your primary hunt pivot.

Evidence: Capture before analysis is complete: (1) Microsoft 365 UAL raw export for the prior 90 days via PowerShell (Search-UnifiedAuditLog -StartDate -EndDate -ResultSize 5000) — specifically preserving ClientIP, UserAgent, and Operation fields for all service principal and OAuth application activity tied to MURKY PANDA's known M365 targeting; (2) Entra ID risky sign-in report (Identity Protection blade) capturing all medium/high-risk events, preserving the risk detection reason field which will log impossible travel and anonymous IP detections relevant to DPRK VPN endpoint mismatches; (3) Azure AD OAuth2PermissionGrants export showing all delegated permissions granted to third-party applications in the past 90 days — MURKY PANDA espionage operations commonly abuse OAuth app consent to maintain persistent mail access; (4) Identity provider authentication logs from the corporate VPN or ZTNA solution showing source IP, device fingerprint, and geolocation for all contractor logins, to be correlated against HR-provided contractor physical work locations.

Step 3: Eradication — Enforce phishing-resistant MFA (FIDO2/hardware token) across all Microsoft 365 accounts; remove SMS-based MFA for privileged roles. Implement software supply chain controls: verify integrity of all third-party packages and contractor-supplied code against known-good hashes (mitigates CWE-494, CWE-506). Revoke and reissue credentials for all accounts flagged in Step 2 review. Segment cryptocurrency custody and fintech API access behind dedicated identity providers separate from corporate M365 tenants.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IA-2 (Identification and Authentication — Organizational Users), NIST IA-5 (Authenticator Management), NIST SA-12 (Supply Chain Protection), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SC-8 (Transmission Confidentiality and Integrity), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: For FIDO2 enforcement without Entra ID P2: use Entra ID free Authentication Methods Policy to disable SMS/voice MFA for Global Administrator and Privileged Role Administrator roles — navigate to Entra ID > Security > Authentication Methods > Policies and set Microsoft Authenticator to 'Passwordless phone sign-in' while removing 'SMS' from allowed methods. For supply chain integrity verification of contractor-supplied code, use the free tool 'sha256sum' (Linux) or 'Get-FileHash -Algorithm SHA256' (PowerShell) against all contractor-delivered binaries or packages; maintain a running CSV log of filename, SHA-256 hash, delivery date, and contractor name to establish chain of custody for CWE-494/CWE-506 remediation documentation. For fintech API segmentation on a shoestring, implement separate Azure AD B2C tenants (free tier up to 50,000 MAU) for cryptocurrency custody system identities, physically isolating those credentials from the corporate M365 directory.

Evidence: Preserve before credential revocation and MFA changes: (1) Full export of current MFA registration state for all accounts via Microsoft Graph (Get-MgUserAuthenticationMethod) — this creates the pre-eradication baseline proving which accounts used SMS MFA (the method exploited or bypassed by DPRK SIM-swapping and social engineering vectors); (2) Azure AD Conditional Access named locations configuration export, capturing the pre-remediation trusted IP ranges that contractor accounts authenticated from — needed to identify if any DPRK-controlled VPN exit nodes were whitelisted as trusted locations; (3) Git history and package manifest files (package-lock.json, requirements.txt, go.sum) for all contractor-contributed repositories, capturing dependency versions at the time of suspected compromise to enable retroactive hash comparison against PyPI/npm audit logs; (4) Screenshot and export of all OAuth applications with admin consent in the M365 tenant before revocation — MURKY PANDA persistence often survives credential rotation via OAuth app grants that outlast password resets.

Step 4: Recovery — Validate MFA enforcement via Azure AD/Entra ID sign-in logs; confirm zero successful authentications using legacy auth protocols. Confirm supply chain review completion with documented sign-off for all active contractor accounts. Run a tabletop exercise simulating a BGH ransomware event to validate backup isolation and recovery time objectives. Monitor M365 audit logs for 30 days post-remediation for residual T1021 and T1055 activity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CA-7 (Continuous Monitoring), NIST SI-4 (System Monitoring), CIS 7.2 (Establish and Maintain a Remediation Process), MITRE ATT&CK T1021 (Remote Services), MITRE ATT&CK T1055 (Process Injection)

Compensating: Validate legacy auth blockage for free using the Entra ID Sign-in Logs filtered by 'Client app' = 'Exchange ActiveSync', 'IMAP4', 'POP3', 'SMTP Auth', and 'Other clients' — any successful authentication in these categories post-remediation is a recovery failure requiring immediate re-containment. For the BGH ransomware tabletop without a commercial simulation platform, use CISA's free Tabletop Exercise Packages (CTEPs) for the financial sector (available at cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages) with the ransomware scenario deck; specifically test backup isolation by requiring participants to demonstrate — not just assert — that

backup systems cannot be reached from a compromised domain admin account. For post-remediation T1021/T1055 monitoring without SIEM, deploy Sysmon with SwiftOnSecurity's configuration (github.com/SwiftOnSecurity/sysmon-config) on M365-connected endpoints and pipe logs to Windows Event Forwarding to a central collector, querying for Event ID 1 (Process Create) with parent-child relationships indicative of lateral movement from cloud-synced credential stores.

Evidence: Document as recovery validation evidence: (1) Entra ID Sign-in Log export filtered for 'legacy authentication client apps' showing zero successful authentications post-MFA enforcement — this is the primary recovery validation artifact for the DPRK IT worker and MURKY PANDA vectors that abused legacy auth; (2) Signed contractor account review spreadsheet with reviewer identity, review date, and disposition (verified/suspended/terminated) for every account in scope — regulatory-grade documentation for financial sector supervisory examinations; (3) Backup isolation test results from the BGH ransomware tabletop documenting whether backup administrator credentials are stored in Active Directory (a primary BGH target) or in a physically separate credential store; (4) 30-day M365 UAL query results for Operations matching 'MailItemsAccessed' (MURKY PANDA mail collection TTP) and 'FileDownloaded' from SharePoint, establishing a post-remediation behavioral baseline.

Step 5: Post-Incident — Conduct insider threat program gap assessment against NIST SP 800-53 PS (Personnel Security) and AT (Awareness and Training) control families. Evaluate AI-generated voice/deepfake verification procedures for wire transfer authorization and executive communication channels. Brief board and senior leadership on BGH victim naming risk — reputational exposure from leak site publication is a board-level concern independent of operational impact. Map current detection coverage against MITRE ATT&CK techniques listed in this report; prioritize gaps in T1656, T1550, and T1574.001 detection.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST PS-3 (Personnel Screening), NIST PS-7 (External Personnel Security), NIST AT-2 (Literacy Training and Awareness), NIST AT-3 (Role-Based Training), NIST RA-3 (Risk Assessment), NIST SI-4 (System Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), MITRE ATT&CK T1656 (Impersonation), MITRE ATT&CK T1550 (Use Alternate Authentication Material), MITRE ATT&CK T1574.001 (Hijack Execution Flow — DLL Search Order Hijacking)

Compensating: For ATT&CK coverage gap assessment without a commercial platform, use the free MITRE ATT&CK Navigator (mitre-attack.github.io/attack-navigator) to layer your existing detection rules against T1656, T1550, and T1574.001 — export the gap heatmap as board-ready documentation. For deepfake/AI voice verification procedures with no budget, implement a shared secret callback protocol for wire transfers exceeding defined thresholds: the receiving party calls back the requestor on a pre-registered number (not caller-ID-spoofable) and confirms a daily rotating code word distributed via encrypted messaging — a zero-cost control directly mitigating the DPRK social engineering vector documented in this campaign. To detect T1574.001 (DLL hijacking used in DPRK supply chain implants), deploy Sysmon Event ID 7 (Image Loaded) with rules flagging unsigned DLLs loaded from user-writable paths (AppData, Temp, Downloads) by financial applications or M365 desktop clients.

Evidence: Capture for post-incident lessons learned and regulatory documentation: (1) MITRE ATT&CK Navigator layer file export showing detection coverage gaps across T1656, T1550, T1574.001, T1078, T1087, and T1567 — this is the gap assessment artifact for board reporting and regulatory examination; (2) Board communication records and crisis communication plan version history, documenting whether BGH leak site publication was addressed in the IR plan prior to this campaign — absence of this coverage is a program gap finding; (3) Personnel screening records for all IT contractors engaged over the prior 12 months (NIST PS-3/PS-7 gap assessment), specifically whether background checks verified physical work location matching contractor-claimed jurisdiction — the primary DPRK IT worker detection failure point; (4) Wire transfer authorization procedure documentation showing whether voice callback verification or out-of-band confirmation was required before this campaign, establishing the pre-incident baseline for AI-voice/deepfake control gap assessment.

Detection Guidance

Priority detection targets by threat cluster:

MURKY PANDA / M365 espionage:

- Microsoft Entra ID / Azure AD sign-in logs: flag authentications from Tor exit nodes, datacenter IP ranges, or countries outside operating footprint.

- Unified Audit Log (UAL): monitor MailItemsAccessed, FileAccessed, and SearchQueryInitiated operations by service principals or newly registered OAuth applications.

- Alert on T1550 (pass-the-token): OAuth token reuse from a different IP than the issuing session within the same token lifetime.

- Behavioral indicator: bulk mailbox access or SharePoint file enumeration (T1087) outside business hours by a single account.

DPRK IT worker / insider vector:

- HR and identity reconciliation: contractor accounts registered to residential VPN or cloud-hosted IP ranges (common DPRK IT worker evasion technique).

- EDR telemetry: process injection patterns (T1055) from developer tooling processes (node.exe, python.exe) against LSASS or financial application processes.

- DLP / proxy logs: T1567 exfiltration via cloud storage services (Google Drive, Dropbox, OneDrive) from contractor-owned endpoints.

- Alert on T1574.001 (DLL search order hijacking) in software build environments.

BGH ransomware pre-encryption:

- T1486 precursor: volume shadow copy deletion (vssadmin delete shadows), service stop commands (T1489), and rapid large-volume file renaming in SMB shares.

- T1021 lateral movement: PsExec or WMI remote execution across financial application servers.

- Network: unusual SMB traffic volumes between workstations (east-west) in environments where workstation-to-workstation SMB should be blocked.

AI-enabled social engineering:

- No automated detection available for deepfake voice. Control: enforce callback verification procedures using pre-established numeric codes for all wire transfer and credential reset requests. Log all out-of-band verification attempts.

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1489** — Service Stop
- **T1195.002** — Compromise Software Supply Chain
- **T1588** — Obtain Capabilities
- **T1586** — Compromise Accounts
- **T1590** — Gather Victim Network Information

- **T1021** — Remote Services
- **T1195** — Supply Chain Compromise
- **T1055** — Process Injection
- **T1657** — Financial Theft
- **T1566** — Phishing
- **T1656** — Impersonation
- **T1110** — Brute Force
- **T1567** — Exfiltration Over Web Service
- **T1087** — Account Discovery
- **T1566.001** — Spearphishing Attachment
- **T1588.005** — Exploits
- **T1574.001** — DLL
- **T1078** — Valid Accounts
- **T1550** — Use Alternate Authentication Material

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)
- **SR-2** — Supply Chain Risk Management Plan
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-8** — Spam Protection
- **AC-7** — Unsuccessful Logon Attempts
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **CM-3** — Configuration Change Control
- **IA-8** — Identification and Authentication (Non-Organizational Users)

- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **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
- **164.308(a)(5)(i)** — Security Awareness and Training

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.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1489	Service Stop	Impact
T1195.002	Compromise Software Supply Chain	Initial-Access

Technique ID	Technique Name	Tactic
T1588	Obtain Capabilities	Resource-Development
T1586	Compromise Accounts	Resource-Development
T1590	Gather Victim Network Information	Reconnaissance
T1021	Remote Services	Lateral-Movement
T1195	Supply Chain Compromise	Initial-Access
T1055	Process Injection	Defense-Evasion
T1657	Financial Theft	Impact
T1566	Phishing	Initial-Access
T1656	Impersonation	Defense-Evasion
T1110	Brute Force	Credential-Access
T1567	Exfiltration Over Web Service	Exfiltration
T1087	Account Discovery	Discovery
T1566.001	Spearphishing Attachment	Initial-Access
T1588.005	Exploits	Resource-Development
T1574.001	DLL	Persistence
T1078	Valid Accounts	Defense-Evasion
T1550	Use Alternate Authentication Material	Defense-Evasion

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/crowdstrike-launches-falcon-...	T3
	https://www.crowdstrike.com/en-us/blog/announcing-threat-ai-industr...	T3
CrowdStrike 2026 Financial Services Threat Landscape Report	https://www.crowdstrike.com/en-us/press-releases/crowdstrike-2026-f...	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 2026-05-16 06:38 UTC by TJS Security Command Center