INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-28 06:45 UTC

Financial Services Under Siege: Nation-State and eCrime Actors Converge on Banks, Crypto, and Fintech

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0374
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Financial institutions, cryptocurrency exchanges, fintech platforms, insurance entities, Microsoft 365 environments (MURKY PANDA targeting)
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Financial Services Threat Landscape Report documents a 43% global increase in hands-on-keyboard intrusions targeting banks, cryptocurrency exchanges, fintech platforms, and insurance entities over the past two years. DPRK-affiliated actors stole $2.02 billion in digital assets, a 51% year-over-year increase, while China-nexus group MURKY PANDA conducted sustained espionage against Microsoft 365 environments and ransomware operators compounded pressure across the sector. The convergence of nation-state intelligence collection, AI-amplified social engineering, and financially motivated eCrime represents a multi-vector threat to financial sector operations, customer trust, and regulatory standing.

Technical Analysis

CrowdStrike's report (April 2025-March 2026) identifies three converging threat clusters against financial services. DPRK-nexus actors, focused on cryptocurrency exchanges and fintech platforms, escalated digital asset theft to $2.02B, leveraging supply chain compromise (T1195, T1195.002), valid account abuse (T1078), and command-and-script execution (T1059). China-nexus MURKY PANDA targeted Microsoft 365 environments using spearphishing (T1598.003, T1566), data collection from information repositories (T1213), and encrypted C2 (T1071, T1090.003). Ransomware operators applied data encryption (T1486) and archive collection (T1560) alongside DLL hijacking (T1574.001) and web session cookie abuse (T1550.004). Relevant CWEs: CWE-494 (Download of Code Without Integrity Check), relevant to supply chain and update mechanisms; CWE-287 (Improper Authentication), relevant to MFA bypass and session hijacking (T1621);

CWE-506 (Embedded Malicious Code), relevant to trojanized packages and insider-delivered payloads. AI-amplified social engineering is flagged as an accelerating vector across all three clusters. No CVE IDs are cited; this is a campaign-level report rather than a discrete vulnerability advisory. The authoritative CrowdStrike primary report is listed as sources[0]; supporting vendor documentation is included as sources[1-4]. This report should be treated as authoritative pending human validation of link resolution.

Action Checklist

1. Step 1: Containment. Audit all Microsoft 365 OAuth application grants, conditional access policies, and third-party integrations immediately; revoke any unrecognized or over-privileged delegated permissions to limit MURKY PANDA's access to cloud data repositories (NIST AC-3, AC-6; CIS 5.4). For crypto and fintech environments, freeze any withdrawal or transfer processes initiated via non-standard API calls or newly registered endpoints pending review.
2. Step 2: Detection. Query Azure AD / Entra ID audit logs for anomalous application consent grants, mail rule creation, and bulk data access from unfamiliar IPs or user agents (addresses MURKY PANDA TTPs: T1213, T1071). Hunt for DLL side-loading artifacts (T1574.001) in financial application directories and review process creation logs for unexpected scripting interpreters (T1059). Monitor for MFA fatigue or push-bombing patterns in authentication logs (T1621), correlate with NIST AU-6, AU-12, CIS 8.2. Flag all software update or package installation events against an approved hash baseline to detect CWE-494 and CWE-506 exploitation attempts (D3-FMBV, D3-SFA).
3. Step 3: Eradication. Enforce phishing-resistant MFA (FIDO2/hardware tokens) on all externally exposed and administrative accounts, especially Microsoft 365 and crypto platform admin consoles, per CIS 6.3, 6.4, 6.5 and NIST IA controls; this directly counters T1621 and CWE-287. Implement software supply chain integrity verification for all third-party packages and update mechanisms (CWE-494, CWE-506; T1195.002): require signed packages and validate checksums against vendor manifests before deployment. Rotate all credentials and API keys for any accounts with anomalous access patterns (D3-CRO, D3-CH).
4. Step 4: Recovery. Validate that conditional access policies enforce compliant device requirements and named location restrictions across Microsoft 365 tenants. Confirm audit logging is fully enabled and retention meets policy minimums (NIST AU-11, AU-4; CIS 8.2). Re-validate asset and software inventories (CIS 1.1, 2.1) to confirm no unauthorized software or accounts persist. Monitor post-remediation for resumed lateral movement, new OAuth grants, or resumed C2 beacon patterns (T1071, T1090.003) using SIEM alerting tuned to the behavioral indicators above.
5. Step 5: Post-Incident. Conduct a tabletop exercise simulating simultaneous ransomware and nation-state intrusion, given the documented convergence of eCrime and espionage actors in this sector. Formally assess supply chain vendor security practices against CIS 2.2 and NIST CM controls. Review separation of duties across financial transaction approval workflows (NIST AC-5) to limit blast radius from valid account abuse (T1078). Evaluate AI-generated social engineering detection capabilities; current email gateway rules tuned to legacy phishing signatures may not detect AI-synthesized lures (T1598.003, T1566).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and your designated regulatory contact (OCC, FDIC, SEC, or FinCEN as applicable) if: any confirmed unauthorized M365 data access involving customer PII or non-public financial data is identified (triggering GLBA breach notification obligations and potentially SEC cybersecurity disclosure requirements under 17 CFR 229.106), any digital asset transfer or withdrawal is confirmed as unauthorized and attributable to DPRK-affiliated actors (triggering OFAC reporting obligations under 31 CFR 501.604 for transactions potentially involving sanctioned entities), or if forensic evidence indicates the intrusion originated from a compromised third-party software vendor (triggering supply chain incident escalation under your institution's TPRM program and potential FSOC reporting).
Recovery Notes	Post-containment, maintain enhanced monitoring of all M365 OAuth application grants, Entra ID sign-in events, and network egress for a minimum of 90 days — MURKY PANDA and similar China-nexus APT actors have documented patience in re-establishing footholds using previously registered but dormant OAuth app registrations or through re-compromising supply chain vendors. Verify that all re-enabled financial transaction workflows have separation-of-duties controls validated end-to-end, not just at the policy level — DPRK-affiliated actors specifically target the gap between policy and technical enforcement in crypto and fintech transaction approval systems. Confirm with your crypto/fintech platform vendors that any API keys or wallet signing keys active during the intrusion window have been rotated at the HSM or cold storage layer, not just at the application API layer, as key material accessible during a hands-on-keyboard intrusion may have been exfiltrated rather than simply used.
Forensic Artifacts	Entra ID / Azure AD Unified Audit Log — 'ApplicationManagement' and 'UserManagement' categories: specifically operations 'Consent to application', 'Add delegated permission grant', 'New-InboxRule', and 'Add member to role' — these are the primary artifact class for MURKY PANDA M365 intrusion activity (T1213, T1098.005) and must be preserved in immutable storage before any remediation action modifies the tenant state | M365 mailbox inbox rule export across all executive, finance, and IT admin mailboxes via 'Get-InboxRule -Mailbox ' — MURKY PANDA and similar espionage actors create forwarding rules to attacker-controlled external addresses or deletion rules targeting security alert emails as a collection and defense-evasion mechanism that persists across password resets | Sysmon Event ID 7 (ImageLoaded) logs from endpoints running financial applications — specifically logging unsigned or recently created DLLs loaded from writable directories adjacent to core financial application executables, which is the primary host-based forensic artifact for DLL side-loading (T1574.001) used in financial sector intrusions documented in this campaign | Crypto/fintech platform API access logs showing all non-interactive (non-browser) API calls during the suspected intrusion window — filter for calls to withdrawal, transfer, and key-management endpoints from IPs not matching the institution's operational egress IP baseline; DPRK-affiliated actors specifically target these endpoints as the terminal action in their $2B+ digital asset theft operations | Windows Security Event Log Event ID 4648 (Logon using explicit credentials) and Event ID 4624 (Successful logon, Type 3 — Network) correlated with Event ID 4688 (Process Creation) on financial application servers — this event sequence is the primary Windows artifact for valid account abuse (T1078) following credential theft, distinguishing nation-state hands-on-keyboard activity from legitimate administrative sessions by examining the parent process chain and logon originating workstation fields

Per-Action IR Details

Step 1: Containment — Audit all Microsoft 365 OAuth application grants, conditional access policies, and third-party integrations immediately; revoke any unrecognized or over-privileged delegated permissions to

limit MURKY PANDA's access to cloud data repositories (NIST AC-3, AC-6; CIS 5.4). For crypto and fintech environments, freeze any withdrawal or transfer processes initiated via non-standard API calls or newly registered endpoints pending review.

NIST Phase: Containment

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AC-20 (Use of External Systems), NIST IR-4 (Incident Handling), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without enterprise CASB or Defender for Cloud Apps, run Microsoft's free 'Get-MgApplication' and 'Get-MgServicePrincipal' PowerShell cmdlets (Microsoft Graph SDK) to enumerate all OAuth app registrations and their delegated/application permission scopes — pipe output to CSV and manually flag any grant with Mail.Read, Files.ReadWrite.All, or Directory.ReadWrite.All assigned to apps registered in the last 90 days or not in your approved app registry. For crypto/fintech API freezing with no dedicated API gateway: coordinate with the platform's operations team to temporarily disable API keys created within the suspected intrusion window via the exchange admin console; document timestamps and key IDs as forensic evidence before disabling.

Evidence: Capture BEFORE revoking any grants: (1) Full export of Entra ID audit log category 'ApplicationManagement' — filter operations 'Consent to application' and 'Add delegated permission grant' for the past 90 days, noting actor UPNs, IP addresses, and user-agent strings associated with MURKY PANDA's known M365 targeting pattern. (2) Export of all current OAuth app permission grants via Microsoft Graph: GET /v1.0/oauth2PermissionGrants and GET /v1.0/servicePrincipals — preserve as JSON snapshots before any revocation. (3) For crypto platforms: full API access logs from the exchange platform showing all non-browser API calls (identify by User-Agent absence of standard browser strings) within the intrusion window, preserving originating IPs, endpoint paths, and any transfer or withdrawal request payloads.

Step 2: Detection — Query Azure AD / Entra ID audit logs for anomalous application consent grants, mail rule creation, and bulk data access from unfamiliar IPs or user agents (addresses MURKY PANDA TTPs: T1213, T1071). Hunt for DLL side-loading artifacts (T1574.001) in financial application directories and review process creation logs for unexpected scripting interpreters (T1059). Monitor for MFA fatigue or push-bombing patterns in authentication logs (T1621) — correlate with NIST AU-6, AU-12, CIS 8.2. Flag all software update or package installation events against an approved hash baseline to detect CWE-494 and CWE-506 exploitation attempts (D3-FMBV, D3-SFA).

NIST Phase: Detection Analysis

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

Controls: 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)

Compensating: For teams without SIEM: (1) MURKY PANDA M365 hunting — use PowerShell 'Search-UnifiedAuditLog -Operations "New-InboxRule","Set-InboxRule","Add-MailboxPermission"' scoped to the past 30 days; separately query 'Search-UnifiedAuditLog -Operations "FileDownloaded","FilePreviewed"' filtering on >500 events per user per day to surface bulk SharePoint/OneDrive exfiltration (T1213). (2) DLL side-loading (T1574.001): deploy Sysmon with SwiftOnSecurity config — hunt Event ID 7 (ImageLoaded) for unsigned or low-prevalence DLLs loaded from writable directories (e.g., %APPDATA%, %TEMP%, application install subdirectories of fintech software). Use 'Get-AuthenticodeSignature' in PowerShell against DLLs in financial application directories. (3) MFA fatigue (T1621): query Entra ID Sign-In logs for users with >5 MFA push denials in a 1-hour window — export via 'Get-MgAuditLogSignIn' filtering on 'authenticationRequirement' and 'mfaDetail.authMethod'. (4) Supply chain integrity (CWE-494/506): build a SHA-256 hash baseline of all installed package binaries using 'Get-FileHash' on application directories; compare against vendor-published checksums or VirusTotal MALPEDIA hashes via free API.

Evidence: Capture BEFORE tuning or modifying any detection rules: (1) Entra ID Sign-In logs for the past 90 days — export via Microsoft Graph 'GET /v1.0/auditLogs/signIns' filtering on 'riskState: confirmedCompromised' or 'riskLevel: high', preserving IP geolocation, device compliance state, and conditional access policy applied/not-applied outcomes that would indicate MURKY PANDA operating from infrastructure not matching expected M365 tenant geolocations. (2)

Sysmon Event ID 1 (Process Creation) logs from financial workstations — filter for cmd.exe, powershell.exe, wscript.exe, or cscript.exe with parent processes matching the institution's core financial application executables (e.g., trading platform, core banking software processes). (3) Windows Application Event Log entries for MSI/installer events (Event ID 1033, 1034) and Windows Update log (%windir%\Logs\WindowsUpdate\WindowsUpdate.etl) to establish a baseline for CWE-494 supply chain insertion timing. (4) Entra ID audit log entries for 'Update application' and 'Update service principal' operations which MURKY PANDA may use to modify existing trusted app registrations rather than creating new ones.

Step 3: Eradication — Enforce phishing-resistant MFA (FIDO2/hardware tokens) on all externally exposed and administrative accounts — especially Microsoft 365 and crypto platform admin consoles — per CIS 6.3, 6.4, 6.5 and NIST IA controls; this directly counters T1621 and CWE-287. Implement software supply chain integrity verification for all third-party packages and update mechanisms (CWE-494, CWE-506; T1195.002): require signed packages and validate checksums against vendor manifests before deployment. Rotate all credentials and API keys for any accounts with anomalous access patterns (D3-CRO, D3-CH).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-2 (Identification and Authentication — Organizational Users), NIST IA-5 (Authenticator Management), NIST SA-12 (Supply Chain Protection), NIST CM-7 (Least Functionality), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For FIDO2 enrollment without enterprise MDM: use Microsoft's free Entra ID combined registration portal (https://aka.ms/mysecurityinfo) and enforce via a Conditional Access policy requiring 'Authentication strength: Phishing-resistant MFA' — this is available on Entra ID P1/P2 and blocks push-based MFA methods that DPRK and MURKY PANDA actors exploit via T1621. For supply chain integrity without a commercial SCA tool: implement a pre-deployment PowerShell script that computes SHA-256 of each package binary and compares against the vendor's published checksum (embed the comparison in your CI/CD pipeline or run manually before any production deployment); additionally configure Windows Defender Application Control (WDAC) policy in audit mode to log any unsigned binary execution attempts in financial application directories — free, included in Windows 10/11 Enterprise. For credential rotation across M365 and crypto API keys: use the 'Revoke-MgUserSignInSession' and 'Reset-MgUserPassword' PowerShell cmdlets for M365 accounts; for crypto exchange API keys, revoke via the exchange admin API and regenerate with IP-allowlist restrictions scoped to known operational egress IPs only.

Evidence: Capture BEFORE rotating credentials or enforcing new MFA policies: (1) Complete export of all active M365 user refresh tokens and session tokens via 'Get-MgUserAuthenticationMethod' — document what authentication methods are currently registered per account, especially any SMS/voice methods that MURKY PANDA or DPRK actors may have registered during the intrusion period as persistence mechanisms (T1098.005). (2) List of all API keys and their last-used timestamps from crypto/fintech platform admin consoles — keys used from IPs not matching your operational baseline are primary indicators of DPRK-affiliated unauthorized access to digital asset platforms. (3) File system snapshots (using free 'FTK Imager' or 'dd') of directories containing third-party financial application binaries before any package rotation — this preserves evidence of any tampered or trojanized components inserted via CWE-494/T1195.002 supply chain compromise for later forensic hash comparison against known-good vendor builds.

Step 4: Recovery — Validate that conditional access policies enforce compliant device requirements and named location restrictions across Microsoft 365 tenants. Confirm audit logging is fully enabled and retention meets policy minimums (NIST AU-11, AU-4; CIS 8.2). Re-validate asset and software inventories (CIS 1.1, 2.1) to confirm no unauthorized software or accounts persist. Monitor post-remediation for resumed lateral movement, new OAuth grants, or resumed C2 beacon patterns (T1071, T1090.003) using SIEM alerting tuned to the behavioral indicators above.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-4 (Audit Storage Capacity), NIST AU-11 (Audit Record Retention), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CM-2 (Baseline Configuration), CIS 1.1 (Establish and Maintain Detailed

Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 8.2 (Collect Audit Logs)

Compensating: Without a commercial SIEM: (1) Conditional access validation — run 'Get-MgIdentityConditionalAccessPolicy' and pipe to a script that checks each policy for 'grantControls.builtInControls' containing 'compliantDevice' and 'includeLocations' scoped to named locations; flag any policy missing these controls against M365 admin, Exchange, and SharePoint workloads. (2) Logging completeness — use the free Microsoft 365 'Office 365 Management Activity API' to verify that all workloads (AzureActiveDirectory, Exchange, SharePoint, Teams) are returning events; gaps indicate logging misconfiguration or deliberate MURKY PANDA log suppression. (3) Post-remediation C2 beacon hunting (T1071, T1090.003): deploy free Zeek (formerly Bro) or Wireshark long-term capture on egress points and apply the free Emerging Threats OPEN ruleset (Suricata-compatible) — specifically ET rules for known HTTPS C2 beaconing intervals and domain fronting patterns used by China-nexus actors; run captures for a minimum of 30 days post-remediation given nation-state actors' documented patience in re-establishing footholds. (4) New OAuth grant alerting without SIEM: configure a free Microsoft Sentinel free-tier workspace or use Logic Apps (consumption tier) to trigger on Entra ID audit log event 'Consent to application' and send an email alert to the security team.

Evidence: Capture during recovery validation to establish a clean-state baseline: (1) Full Entra ID Conditional Access policy export (JSON) via Microsoft Graph 'GET /v1.0/identity/conditionalAccess/policies' — timestamped and signed as the verified post-remediation policy state for audit and regulatory purposes. (2) Microsoft 365 Unified Audit Log retention configuration screenshot and storage quota from the Compliance portal — confirm 90-day minimum (1-year for E3/E5) is active, as MURKY PANDA intrusions targeting M365 data repositories may require extended retention to support regulatory breach notification timelines under applicable financial services regulations. (3) Network flow logs (NetFlow/IPFIX from perimeter devices, or Zeek conn.log) covering all egress traffic from systems accessed during the intrusion window — baseline legitimate HTTPS connection intervals to M365 endpoints (*.office365.com, *.sharepoint.com) to establish a jitter profile that will make resumed C2 beaconing using domain fronting (T1090.003) statistically detectable.

Step 5: Post-Incident — Conduct a tabletop exercise simulating simultaneous ransomware and nation-state intrusion, given the documented convergence of eCrime and espionage actors in this sector. Formally assess supply chain vendor security practices against CIS 2.2 and NIST CM controls. Review separation of duties across financial transaction approval workflows (NIST AC-5) to limit blast radius from valid account abuse (T1078). Evaluate AI-generated social engineering detection capabilities — current email gateway rules tuned to legacy phishing signatures may not detect AI-synthesized lures (T1598.003, T1566).

NIST Phase: Post Incident

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

Controls: NIST AC-5 (Separation of Duties), NIST CM-7 (Least Functionality), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For a 2-person team conducting the tabletop without a dedicated IR simulation platform: use CISA's free 'Tabletop Exercise Packages' (CTEP) — specifically the Financial Sector package — and inject the CrowdStrike-documented scenario of simultaneous DPRK digital asset theft and MURKY PANDA M365 espionage as injects, testing the team's ability to triage competing priorities without cross-contaminating containment actions. For supply chain vendor assessment without a vendor risk management platform: build a one-page questionnaire based on CIS 2.2 and NIST SP 800-161 (C-SCRM) key practices and send to top-10 software vendors by risk criticality; score responses against whether vendors provide signed releases, SBOMs, and vulnerability disclosure programs. For AI-generated phishing detection (T1566, T1598.003) without a commercial AI email security product: configure free rules in your email gateway using header analysis (check for mismatches between Display Name, SMTP envelope sender, and DKIM/DMARC alignment) and deploy the free 'Microsoft Defender for Office 365 Evaluation Mode' — additionally, subscribe to CISA's free phishing report feed and update gateway block lists weekly.

Evidence: Collect and preserve for lessons-learned documentation: (1) Timeline reconstruction from Entra ID audit logs, M365 Unified Audit Log, and any available network flow data — specifically mapping the MURKY PANDA intrusion progression from initial consent grant through data repository access (T1213) to identify dwell time, which in China-nexus espionage campaigns typically ranges from weeks to months and is critical for breach notification scoping under financial services regulations (GLBA, state-level requirements). (2) Full export of all inbox rules created or

modified during the intrusion window across impacted M365 mailboxes — MURKY PANDA and similar actors commonly create forwarding or deletion rules (T1564.008) as persistence and collection mechanisms that survive credential rotation if not explicitly identified. (3) Transaction audit logs from financial platforms covering the intrusion window — specifically any high-value transfer approvals, API-initiated transactions, or workflow exceptions that may indicate T1078 (Valid Accounts) abuse within transaction approval workflows, which would constitute a separate financial fraud investigation thread requiring escalation to the institution's fraud operations and potentially to FinCEN under BSA/SAR obligations.

Detection Guidance

Priority detection across three actor clusters: (1) MURKY PANDA / Microsoft 365 espionage, query Entra ID audit logs for new OAuth app consent events, inbox rule creation by non-admin accounts, and bulk mailbox export operations; alert on mail access from IPs not associated with known corporate egress ranges. Behavioral indicator: access to SharePoint/OneDrive repositories at unusual hours or from new device fingerprints (T1213). (2) DPRK supply chain and valid account abuse, monitor software deployment pipelines for unsigned or hash-mismatched packages (CWE-494; D3-FMBV); alert on process execution chains where a legitimate financial application spawns an unexpected child process (T1059, T1574.001); flag new API keys or service accounts created in crypto/fintech platforms with immediate high-value transaction permissions (T1078). (3) Ransomware precursors, detect archive creation utilities running under service accounts (T1560), scheduled task creation by non-standard processes (T1574.001), and outbound connections to anonymizing infrastructure (T1090.003). Cross-cluster: enable NIST AU-2 event categories covering account management, privilege use, and object access; ensure timestamps are synchronized per AU-8 to support cross-source correlation. D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) are recommended countermeasures. No public IOCs (IPs, domains, hashes) are included in the source report as summarized; confirm against the CrowdStrike primary report URL for any appended IOC appendix.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1621** — Multi-Factor Authentication Request Generation
- **T1550.004** — Web Session Cookie
- **T1588** — Obtain Capabilities
- **T1598.003** — Spearphishing Link
- **T1195** — Supply Chain Compromise
- **T1213** — Data from Information Repositories
- **T1059** — Command and Scripting Interpreter
- **T1574.001** — DLL
- **T1560** — Archive Collected Data
- **T1071** — Application Layer Protocol
- **T1090.003** — Multi-hop Proxy
- **T1486** — Data Encrypted for Impact
- **T1195.002** — Compromise Software Supply Chain

- **T1566** — Phishing

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **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

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)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

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

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1550.004	Web Session Cookie	Defense-Evasion
T1588	Obtain Capabilities	Resource-Development
T1598.003	Spearphishing Link	Reconnaissance
T1195	Supply Chain Compromise	Initial-Access
T1213	Data from Information Repositories	Collection
T1059	Command and Scripting Interpreter	Execution
T1574.001	DLL	Persistence
T1560	Archive Collected Data	Collection
T1071	Application Layer Protocol	Command-And-Control
T1090.003	Multi-hop Proxy	Command-And-Control
T1486	Data Encrypted for Impact	Impact
T1195.002	Compromise Software Supply Chain	Initial-Access
T1566	Phishing	Initial-Access

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/3-ways-small-businesses-big-...	T3

Source	URL	Tier
	https://www.crowdstrike.com/en-us/blog/crowdstrike-named-leader-in-...	T3
Financial Services Under Siege: DPRK Steals $2B, Ransomware	https://techjacksolutions.com/scc-intel/financial-services-under-si...	T3

Generated 2026-05-28 06:45 UTC by TJS Security Command Center