INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-20 06:43 UTC

Financial Sector Under Compound Pressure: Nation-State Theft, eCrime Escalation, and AI-Accelerated Attacks Define 2025-2026 Threat Landscape

SECURITY ANALYSIS | **HIGH** | CVSS 7.5

SCC Item ID	SCC-STY-2026-0146
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Financial services organizations broadly; cryptocurrency and fintech platforms; Microsoft 365 environments (MURKY PANDA targeting); insurance entities; legal and financial services firms
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Financial Services Threat Landscape Report documents a 43% rise in hands-on-keyboard intrusions against financial institutions over two years, with DPRK-nexus actors attributed to $2.02 billion in cryptocurrency theft and ransomware operators recording a 27% increase in financial sector leak site victims. Three structurally distinct threat categories, nation-state theft, eCrime extortion, and China-nexus espionage, are converging on the financial sector simultaneously, compressing the time security teams have to detect and respond. AI adoption by adversaries is accelerating attack tempo across all three categories, indicating that defenses built around historical dwell times are no longer calibrated to the current threat environment.

Technical Analysis

The CrowdStrike 2026 Financial Services Threat Landscape Report identifies three distinct but concurrent threat tracks targeting financial institutions, each with different objectives, tooling, and defensive requirements.

The DPRK-nexus track centers on cryptocurrency and digital asset theft at scale. Attributed actors are responsible for $2.02 billion in cryptocurrency theft, with targeting focused on cryptocurrency exchanges, fintech platforms, and digital asset custodians. The techniques documented map to T1657 (Financial Theft), T1486 (Data Encrypted for Impact), T1566 (Phishing), and T1078 (Valid Accounts), consistent with a pattern of social

engineering followed by credential compromise and asset liquidation. CWE-494 (Download of Code Without Integrity Check) and CWE-506 (Embedded Malicious Code) appear as recurring vulnerability classes, suggesting supply chain and software integrity vectors remain active in DPRK-linked campaigns. The state-nexus framing matters operationally: these actors do not follow eCrime incentive structures and are unlikely to be deterred by takedowns targeting criminal infrastructure.

The China-nexus track is represented by MURKY PANDA, which CrowdStrike documents conducting trusted-relationship attacks (T1199) against Microsoft 365 cloud environments to conduct economic espionage. Observed techniques include cloud service discovery via T1538, email collection via T1114, spearphishing links via T1566.002, and data archival via T1560. The trusted-relationship vector, mapped to T1199, is particularly significant because it exploits legitimate business relationships, managed service providers, legal counsel, or financial advisors with cloud tenant access, rather than forcing entry through perimeter controls. CWE-287 (Authentication Failures) is the underlying weakness class, pointing to gaps in conditional access policy, multi-tenant trust boundaries, and third-party access governance in M365 environments. The espionage objective, consistent with CrowdStrike's broader China-nexus attribution methodology, is economic intelligence rather than disruption, meaning affected organizations may not observe obvious operational impact during the intrusion window.

The eCrime track shows a 27% increase in financial sector victims on ransomware leak sites, with hands-on-keyboard intrusion volume up 43% across the two-year reporting period. Techniques documented include external remote services (T1133), valid account abuse (T1078), scripting interpreter execution (T1059), lateral movement via remote services (T1021), and supply chain compromise (T1195.002). DLL hijacking (T1574.001) appears in the technique set, indicating post-access persistence and defense evasion tradecraft consistent with sophisticated ransomware affiliate operations. The 43% intrusion increase combined with the 27% leak site increase suggests operators are both gaining access more frequently and converting intrusions to extortion outcomes at an increasing rate.

AI acceleration is assessed as a cross-cutting factor. CrowdStrike's reporting indicates adversaries are using AI to compress the timeline between initial access and mission execution, reducing the detection and response window available to defenders. The compression of dwell time has been documented in recent CrowdStrike reporting, and AI-assisted reconnaissance and lure generation (T1598.003) extend the reach of all three threat categories simultaneously.

The defensive implication is that these three tracks require distinct response postures. DPRK targeting demands software supply chain integrity controls and digital asset platform hardening. MURKY PANDA activity demands M365 conditional access hardening, third-party access audits, and cloud audit log coverage. eCrime operators demand endpoint detection coverage, external access control, and lateral movement detection. A unified 'financial sector' defensive posture that does not account for these distinctions will be miscalibrated for at least two of the three tracks at any given time.

Action Checklist

1. Assess exposure, determine whether your organization operates cryptocurrency custody, exchange, or fintech infrastructure (DPRK primary targeting surface), uses Microsoft 365 with third-party or managed service provider delegated access (MURKY PANDA vector), or has external remote access services exposed (eCrime initial access vector T1133)
2. Review controls, for DPRK track: audit software integrity verification for all code deployed to financial platforms (CWE-494, CWE-506); for MURKY PANDA track: audit Microsoft 365 conditional access

policies, review all delegated admin relationships and third-party tenant trust configurations, confirm cloud audit logging (Unified Audit Log) is enabled and retained; for eCrime track: verify MFA enforcement on all VPN and RDP endpoints (T1133, T1078), confirm EDR coverage on all hosts with lateral movement telemetry (T1021), and review DLL search order hardening (T1574.001)

3. Update threat model, add MURKY PANDA trusted-relationship intrusion pattern to your threat register with M365 and third-party access as the primary attack surface; add DPRK digital asset targeting as a priority scenario if your organization holds or transacts in cryptocurrency; incorporate AI-accelerated attack tempo as a factor reducing assumed detection windows in tabletop exercises

4. Communicate findings, brief the CISO and relevant business leaders on which of the three threat tracks applies to your organization based on your assessed exposure; quantify the $2.02 billion in cumulative DPRK-attributed cryptocurrency theft documented in the CrowdStrike 2026 report and the 27% ransomware victim increase as concrete sector-level benchmarks; avoid framing this as a generic 'financial sector threat' briefing, specify which track(s) are directly relevant

5. Monitor developments, track CrowdStrike's published MURKY PANDA intelligence for updated indicators and technique refinements; monitor CISA advisories for DPRK cryptocurrency theft campaigns (CISA has previously co-issued advisories on DPRK digital asset theft with FBI and Treasury); watch for follow-on regulatory guidance from financial sector regulators responding to the documented intrusion volume increase

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if M365 UAL review surfaces any of the following: new delegated admin relationships not authorized through change management, service principal credential additions outside normal provisioning windows, or cross-tenant application consent events — any of these represent active MURKY PANDA indicators requiring incident declaration under NIST 800-61r3 §3 (DE.AE-08); additionally, escalate if any cryptocurrency hot wallet or signing key access is detected outside of authorized operational windows, as this may trigger FinCEN SAR filing obligations under 31 U.S.C. § 5318(g) and CISA breach notification coordination.
Recovery Notes	For any confirmed MURKY PANDA or DPRK intrusion, recovery must include full revocation and re-provisioning of all M365 delegated admin relationships and service principal credentials — not just the compromised ones — because MURKY PANDA's persistence model involves establishing multiple redundant trust relationships that may not all surface during initial investigation (NIST 800-61r3 §3.5 — Recovery). For cryptocurrency theft incidents, coordinate with the blockchain analytics firms (Chainalysis, TRM Labs) used by FBI and Treasury to trace fund movement before any public disclosure, as premature disclosure can accelerate laundering through mixers. Monitor M365 UAL daily for a minimum of 90 days post-remediation, with specific attention to re-appearance of revoked service principal credentials or new delegated admin invitations from previously identified MSP or third-party tenants.

Forensic Artifacts	Microsoft 365 Unified Audit Log — filter on operations 'Add delegated permission', 'Add service principal credentials', 'Consent to application', 'Update application', and 'Add member to role' for the past 90 days; these are the specific UAL event types generated by MURKY PANDA's technique of abusing third-party delegated admin relationships to establish persistent M365 access | Azure AD Sign-In Logs and Conditional Access audit logs — specifically entries showing successful authentications from service principal identities or partner tenant identities outside of expected geographic locations or outside business hours, which represent MURKY PANDA operational tradecraft for avoiding detection during tenant enumeration (MITRE T1078.004 — Valid Accounts: Cloud Accounts) | Blockchain transaction records and hot wallet access logs from cryptocurrency custody platforms — specifically any unsigned or anomalously-signed transactions, API key usage events outside authorized windows, and wallet drain sequences consistent with DPRK's documented technique of accessing custody platforms via trojanized software updates (CWE-494) and then exfiltrating private keys before initiating bulk transfers | Windows Security Event Log Event ID 4624 (logon type 10 — RemoteInteractive) and Event ID 4625 (failed logon) on all internet-facing RDP and VPN gateway hosts — these are the primary authentication artifacts for eCrime T1133 (External Remote Services) and T1078 (Valid Accounts) initial access, and a spike in 4625 events followed by a successful 4624 from the same external IP is the canonical brute-force-to-access pattern used by ransomware operators targeting financial sector remote access | Sysmon Event ID 7 (Image Loaded) logs on financial platform hosts — filter for DLL load events where the loaded DLL path does not match the application's expected installation directory, which is the primary forensic indicator of T1574.001 (DLL Search Order Hijacking) used by eCrime operators for persistence and privilege escalation after initial access via T1133

Per-Action IR Details

Assess exposure — determine whether your organization operates cryptocurrency custody, exchange, or fintech infrastructure (DPRK primary targeting surface), uses Microsoft 365 with third-party or managed service provider delegated access (MURKY PANDA vector), or has external remote access services exposed (eCrime initial access vector T1133)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing IR capability and identifying organizational attack surface before incidents occur

Controls: NIST IR-4 (Incident Handling) — establish handling capability scoped to the three identified threat tracks, NIST IR-8 (Incident Response Plan) — ensure the plan explicitly addresses cryptocurrency infrastructure, M365 delegated access, and external remote access as distinct scenarios, NIST RA-3 (Risk Assessment) — formally document DPRK digital asset targeting, MURKY PANDA third-party trust abuse, and eCrime T1133 exploitation as prioritized risk scenarios, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — inventory must tag assets by category: crypto custody nodes, M365 tenants with delegated admin relationships, and internet-facing RDP/VPN endpoints, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — scope the vulnerability management process to explicitly include third-party MSP access reviews and external remote access services

Compensating: Run a PowerShell query against Azure AD to enumerate all delegated admin relationships: `Get-MsolPartnerInformation` and `Get-MsolCompanyInformation` (requires MSOnline module). For external remote access, use Shodan's free tier to search your ASN for exposed RDP (port 3389) and common VPN ports (4443, 8443, 10443). For crypto infrastructure, manually enumerate all wallet signing services, hot wallet APIs, and exchange connector endpoints in a spreadsheet, tagging each with its internet exposure status.

Evidence: Before scoping begins, snapshot the current state of your Microsoft 365 Unified Audit Log (UAL) to establish a baseline — specifically export the last 90 days of `Add delegated permission` and `Add app role assignment to service principal` operations via the UAL search (`auditLogSearch` under compliance.microsoft.com). Capture Shodan/Censys export of your organization's externally exposed services as a point-in-time reference. For

crypto platforms, preserve the current list of authorized signing keys and wallet access credentials in escrow before any changes are made.

Review controls — for DPRK track: audit software integrity verification for all code deployed to financial platforms (CWE-494, CWE-506); for MURKY PANDA track: audit Microsoft 365 conditional access policies, review all delegated admin relationships and third-party tenant trust configurations, confirm cloud audit logging (Unified Audit Log) is enabled and retained; for eCrime track: verify MFA enforcement on all VPN and RDP endpoints (T1133, T1078), confirm EDR coverage on all hosts with lateral movement telemetry (T1021), and review DLL search order hardening (T1574.001)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: acquiring tools, establishing logging, and hardening systems to support detection and response across all three threat tracks

Controls: NIST SI-2 (Flaw Remediation) — for DPRK track, apply to software supply chain integrity: verify all code packages deployed to financial platforms are signed and hash-verified against vendor manifests (CWE-494 untrusted code download, CWE-506 embedded malicious code), NIST SI-7 (Software, Firmware, and Information Integrity) — deploy integrity verification for all executables and libraries on cryptocurrency custody and fintech platform hosts, NIST SI-4 (System Monitoring) — for MURKY PANDA track, confirm Unified Audit Log is enabled at E3/E5 level with 180-day minimum retention; for eCrime track, confirm EDR lateral movement telemetry covers T1021 (SMB, WMI, RDP-based movement), NIST AC-17 (Remote Access) — enforce MFA on all VPN and RDP endpoints to close the T1133/T1078 initial access vector used by eCrime operators, NIST CM-7 (Least Functionality) — enforce DLL search order hardening via registry key `HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode = 1` to mitigate T1574.001, CIS 6.3 (Require MFA for Externally-Exposed Applications) — MFA enforcement on all VPN and RDP endpoints is a foundational IG1 control directly closing the eCrime T1133 vector, CIS 6.5 (Require MFA for Administrative Access) — MURKY PANDA leverages delegated admin relationships; MFA on all admin accounts in M365 limits the blast radius of compromised MSP credentials, CIS 8.2 (Collect Audit Logs) — Unified Audit Log enablement for M365 is the minimum required to detect MURKY PANDA tenant enumeration and delegated permission abuse

Compensating: DPRK track — use free FOSSA or in-house scripting (`sha256sum` on Linux, `Get-FileHash` in PowerShell) to hash all deployed financial platform binaries against vendor-published manifests; run weekly as a cron job or scheduled task. MURKY PANDA track — use the free Microsoft 365 Secure Score portal and export delegated admin relationships via `Get-MsolPartnerContract | Export-CSV`. Confirm UAL is active via Security & Compliance Center > Audit > Start recording. eCrime track — deploy Sysmon with the SwiftOnSecurity config to capture process creation (Event ID 1), network connections (Event ID 3), and DLL image loads (Event ID 7) on all hosts with RDP/VPN exposure; forward to Windows Event Forwarding (WEF) for centralized collection at no cost.

Evidence: DPRK: Capture current file hashes of all executables and libraries on cryptocurrency platform hosts using `Get-FileHash -Algorithm SHA256 -Path C:\AppDir\* -Recurse | Export-CSV` before any patching, to establish a pre-change baseline for comparison if trojanized code (CWE-506) is later suspected. MURKY PANDA: Export the full Microsoft 365 Unified Audit Log for the past 90 days, filtering on operations `Add delegated permission`, `Consent to application`, `Add service principal credentials`, and `Update application` — these are the artifact classes MURKY PANDA activity generates in M365 audit trails. eCrime: Before hardening RDP/VPN, capture Sysmon Event ID 3 (network connection) logs and Windows Security Event Log Event ID 4624 (successful logon, logon type 10 = RemoteInteractive) to document the current remote access baseline.

Update threat model — add MURKY PANDA trusted-relationship intrusion pattern to your threat register with M365 and third-party access as the primary attack surface; add DPRK digital asset targeting as a priority scenario if your organization holds or transacts in cryptocurrency; incorporate AI-accelerated attack tempo as a factor reducing assumed detection windows in tabletop exercises

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: updating organizational threat models and exercising IR capability against realistic threat scenarios including reduced detection windows

Controls: NIST IR-8 (Incident Response Plan) — the IR plan must be updated to include MURKY PANDA trusted-relationship intrusion as a named scenario with M365 delegated access as the attack path, and DPRK cryptocurrency theft as a named scenario with wallet exfiltration as the impact, NIST IR-3 (Incident Response Testing) — tabletop exercises must incorporate AI-accelerated attack tempo as a variable, explicitly compressing the assumed time between initial access and impact to reflect CrowdStrike's documented reduction in dwell time, NIST RA-3 (Risk Assessment) — formally register MURKY PANDA (MITRE ATT&CK T1199 — Trusted Relationship) and DPRK cryptocurrency theft (MITRE ATT&CK T1657 — Financial Theft) as prioritized threat scenarios with likelihood and impact ratings, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — the threat register update must feed the vulnerability management process so MURKY PANDA-relevant M365 misconfigurations and DPRK-relevant software integrity gaps are prioritized in remediation queues

Compensating: Use the free MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) to build a layer file annotating MURKY PANDA techniques (T1199 Trusted Relationship, T1078.004 Cloud Accounts, T1114 Email Collection) and DPRK techniques (T1195 Supply Chain Compromise, T1657 Financial Theft, T1553 Subvert Trust Controls) against your current detective controls, producing a visual gap map at no cost. Use this output as the threat register artifact. For tabletop exercises, use CISA's free Tabletop Exercise Package (CTEP) framework and inject an AI-accelerated timeline by halving assumed dwell times in all decision points.

Evidence: Prior to updating the threat model, collect any existing threat intelligence already held by the organization: previous CrowdStrike or vendor threat intel reports, prior CISA advisories on DPRK cryptocurrency theft (e.g., AA22-108A, AA23-049A), and any historical M365 UAL anomalies involving delegated admin operations. These form the evidential basis for the threat model entries and support risk rating justification during audit or regulatory review.

Communicate findings — brief the CISO and relevant business leaders on which of the three threat tracks applies to your organization based on your assessed exposure; quantify the $2.02 billion DPRK theft figure and 27% ransomware victim increase as concrete sector-level benchmarks; avoid framing this as a generic 'financial sector threat' briefing — specify which track(s) are directly relevant

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing communication structures and ensuring organizational leadership is briefed on threat-specific risk prior to incident declaration

Controls: NIST IR-6 (Incident Reporting) — internal reporting structures must be established so CISO and business leaders receive threat-track-specific briefings mapped to organizational exposure, not generic sector alerts, NIST IR-7 (Incident Response Assistance) — identify in advance which external parties (FS-ISAC, CrowdStrike IR retainer, CISA CISA Services) would be engaged per threat track, and communicate those escalation paths to leadership, NIST IR-8 (Incident Response Plan) — the communication plan within the IR plan must specify different notification chains for a DPRK cryptocurrency theft event (likely requiring Treasury/FinCEN notification) versus a MURKY PANDA espionage intrusion versus a ransomware extortion event, CIS 7.2 (Establish and Maintain a Remediation Process) — leadership briefings must result in a prioritized, track-specific remediation commitment with documented timelines, not a generic awareness acknowledgment

Compensating: Prepare a one-page executive briefing template with three sections (one per threat track) using the FS-ISAC TLP:WHITE reporting format. Populate the DPRK section with the $2.02B theft figure and applicable CISA advisory references. Populate the MURKY PANDA section with M365 UAL findings from the control review step. Populate the eCrime section with current MFA enforcement gaps and EDR coverage percentage from the asset inventory. Deliver as a PDF with a signature line to create a documented acknowledgment record — critical for regulatory defensibility under DORA, SEC cybersecurity disclosure rules, or OCC examination.

Evidence: Before the briefing, compile the following as supporting exhibits: (1) output of the M365 delegated admin relationship export showing all active third-party tenant trust configurations, (2) the asset inventory excerpt showing cryptocurrency custody/exchange infrastructure scope, (3) the Shodan/Censys export of externally exposed remote access services with MFA enforcement status annotated. These are the organization-specific data points that differentiate this briefing from a generic sector report and demonstrate due diligence if regulatory inquiry follows.

Monitor developments — track CrowdStrike's published MURKY PANDA intelligence for updated indicators and technique refinements; monitor CISA advisories for DPRK cryptocurrency theft campaigns (CISA has previously co-issued advisories on DPRK digital asset theft with FBI and Treasury); watch for follow-on

regulatory guidance from financial sector regulators responding to the documented intrusion volume increase

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: using threat intelligence and lessons learned to improve detection capability and update organizational defenses on an ongoing basis

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — formally subscribe to CISA advisories, FS-ISAC feeds, and CrowdStrike intelligence publications; assign a named owner responsible for triaging and distributing DPRK and MURKY PANDA-specific publications, NIST IR-4 (Incident Handling) — update incident handling procedures whenever new MURKY PANDA technique refinements or DPRK TTPs are published, without waiting for a full annual IR plan review cycle, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — establish a recurring M365 UAL review cadence (minimum monthly) specifically hunting for MURKY PANDA-associated operations: new delegated permissions, service principal credential additions, and cross-tenant application consents, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — integrate CISA KEV (Known Exploited Vulnerabilities) catalog monitoring and DPRK/MURKY PANDA advisory feeds into the vulnerability management process as standing input sources

Compensating: Subscribe to CISA's free email alert service (cisa.gov/subscribe-updates-cisa) and FS-ISAC's free TLP:WHITE feed for financial sector threat intelligence. Create a free MITRE ATT&CK Navigator saved layer for MURKY PANDA and DPRK techniques and update it each time a new advisory is published, using the delta to identify new detection gaps. For M365 hunting, use a scheduled PowerShell script running `Search-UnifiedAuditLog -Operations 'Add delegated permission','Add service principal credentials','Consent to application' -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date)` weekly to surface MURKY PANDA-relevant activity without a SIEM.

Evidence: Maintain a running intelligence log documenting each new CISA DPRK advisory (e.g., updates to AA22-108A series), each CrowdStrike MURKY PANDA publication, and each regulatory guidance issuance, with a dated entry recording what was reviewed, what changed in the threat landscape, and what organizational action was taken in response. This log serves as the primary evidence of ongoing due diligence under NIST IR-5 (Incident Monitoring) and supports regulatory examination defense under DORA Article 17 or OCC Heightened Standards if the organization is later subject to inquiry following a sector-level incident.

Detection Guidance

Detection priorities differ by threat track and should be scoped accordingly.

For MURKY PANDA / M365 espionage activity: Review Microsoft 365 Unified Audit Log for anomalous mail access patterns consistent with T1114, specifically mailbox access by service principals or delegated accounts outside normal business hours or from unexpected geographies. Hunt for T1538 cloud service discovery activity, specifically bulk enumeration of tenant resources beyond the permissions granted to the third-party application identity, with particular attention to enumeration of users or groups not required for the stated business function of the delegated application. Audit all delegated admin relationships in Microsoft Entra ID (formerly Azure AD) and identify any with excessive permissions relative to their stated business purpose. Flag conditional access policies that do not enforce device compliance or location restrictions for third-party access. Monitor for T1560 archival activity, staged data collection to cloud storage or external endpoints, as a late-stage indicator.

For DPRK digital asset targeting: Inspect build pipelines and software deployment workflows for unsigned or inadequately verified code packages (CWE-494). Review npm, PyPI, or other dependency chains for packages with embedded execution logic not present in prior versions (CWE-506, T1195.002). Monitor for spearphishing with file attachments or links targeting developer and finance staff (T1566, T1598.003), particularly lures themed around cryptocurrency job offers or investment opportunities, consistent with documented DPRK social engineering patterns.

For eCrime ransomware operators: Review external remote access logs (VPN, RDP, Citrix) for authentication anomalies consistent with valid account abuse (T1078, T1133). Hunt for T1059 scripting interpreter execution (PowerShell, cmd, WMI) spawned from unusual parent processes or user contexts. Monitor lateral movement telemetry for T1021 remote service activity between workstations, which is atypical in most financial environments. Inspect DLL load events for search order hijacking patterns (T1574.001), particularly in directories writable by standard user accounts. Correlate endpoint telemetry against known ransomware affiliate TTPs documented in CrowdStrike's eCrime reporting.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to CrowdStrike 2026 Financial Services Threat Landscape Report and MURKY PANDA blog post for published indicators`	CrowdStrike's reporting references specific MURKY PANDA indicators, DPRK-linked payload hashes, and eCrime infrastructure; the actual IOC values are not reproduced in the source material provided. Retrieve indicators directly from the CrowdStrike Adversary Intelligence portal or the published blog posts listed in the source URLs.	LOW

Framework Mappings

MITRE-ATTACK

- **T1199** — Trusted Relationship
- **T1486** — Data Encrypted for Impact
- **T1114** — Email Collection
- **T1598.003** — Spearphishing Link
- **T1059** — Command and Scripting Interpreter
- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1560** — Archive Collected Data
- **T1021** — Remote Services
- **T1657** — Financial Theft
- **T1566.002** — Spearphishing Link
- **T1538** — Cloud Service Dashboard
- **T1195.002** — Compromise Software Supply Chain
- **T1574.001** — DLL
- **T1133** — External Remote Services

NIST-800-53R5

- **CP-9** — System Backup

- **CP-10** — System Recovery and Reconstitution
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **AC-20** — Use of External Systems
- **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
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

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

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1199	Trusted Relationship	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1114	Email Collection	Collection
T1598.003	Spearphishing Link	Reconnaissance
T1059	Command and Scripting Interpreter	Execution
T1566	Phishing	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1560	Archive Collected Data	Collection
T1021	Remote Services	Lateral-Movement
T1657	Financial Theft	Impact
T1566.002	Spearphishing Link	Initial-Access
T1538	Cloud Service Dashboard	Discovery
T1195.002	Compromise Software Supply Chain	Initial-Access
T1574.001	DLL	Persistence
T1133	External Remote Services	Persistence

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-financial-s...	T3

Source	URL	Tier
	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/how-to-mature-your-threat-in...	T3
MURKY PANDA: Trusted-Relationship Cloud Threat | CrowdStrike	https://www.crowdstrike.com/en-us/blog/murky-panda-trusted-relation...	T3

Generated 2026-05-20 06:43 UTC by TJS Security Command Center