INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-18 06:14 UTC

Financial Services Threat Landscape 2026: Hands-On Intrusions Surge 43%, DPRK Steals $2.02B, eCrime Leak Site Listings Up 27%

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0330
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Financial services organizations broadly; cryptocurrency exchanges; fintech platforms; traditional banks; insurance entities; Microsoft 365 environments (MURKY PANDA activity)
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Financial Services Threat Landscape Report documents a 43% global increase in hands-on intrusions targeting financial institutions, with DPRK-affiliated actors stealing $2.02 billion in digital assets and eCrime groups listing 423 financial entities on ransomware leak sites, a 27% year-over-year rise. The report covers April 2025 through March 2026 and spans cryptocurrency exchanges, fintech platforms, traditional banks, and insurance entities. Organizations face overlapping nation-state and eCrime actor threats that exploit shared credential theft and social engineering techniques, meaning siloed threat response programs leave common attack paths unaddressed.

Technical Analysis

The report documents three primary threat categories operating against financial services. First, hands-on-keyboard (interactive) intrusions increased 43% globally and 48% in North America over two years, reflecting adversary preference for Windows administration tools and system utilities (LOLBins) over detectable malware. Second, DPRK-nexus actors within the Lazarus cluster employed spear-phishing (T1566), fraudulent IT worker insertion schemes (T1591, T1204), and supply chain compromise (T1195.002) to steal $2.02 billion from cryptocurrency exchanges and fintech platforms; initial access methods map to CWE-287 (authentication bypass) and CWE-494 (download of code without integrity checks). Third, eCrime ransomware and extortion operators applied dual-extortion pressure against 423 financial entities, leveraging valid account abuse (T1078), data exfiltration over web services (T1567), and ransomware deployment (T1486). MURKY PANDA, documented in CrowdStrike threat intelligence, targeted Microsoft 365 environments via OAuth abuse and

credential harvesting (T1114.002, T1555), consistent with CWE-346 origin validation failures. Tradecraft convergence between nation-state and eCrime actors is documented across initial access broker use (T1588.001), adversary-in-the-middle positioning (T1090.003), and session token theft (T1539). No CVEs are associated with this campaign report; CWE patterns are analytical attributions consistent with observed intrusion methods.

Action Checklist

1. Containment: Audit Microsoft 365 OAuth application grants and conditional access policies immediately; revoke unrecognized delegated permissions and disable legacy authentication protocols to cut off credential harvesting entry points.
2. Detection: Query identity provider logs for anomalous OAuth consent grants, impossible-travel sign-ins, and Exchange Online mailbox delegation events (T1114.002); correlate endpoint telemetry for LOLBin abuse (certutil, mshta, wscript) consistent with hands-on-keyboard intrusion patterns.
3. Eradication: Remove unauthorized IT worker accounts and contractor identities with privileged access; verify software supply chain integrity for any third-party integrations touching cryptocurrency custody or fintech payment rails (T1195.002, CWE-494); enforce code signing and dependency integrity checks.
4. Recovery: Validate MFA enforcement across all privileged and external-facing accounts; restore from known-clean backups for any systems touched by ransomware operators; confirm no persistent backdoors remain via full credential rotation and reviewed service account inventory.
5. Post-Incident: Review threat intelligence program structure for nation-state and eCrime convergence gaps; ensure SOC playbooks address dual-extortion scenarios and DPRK IT worker insertion red flags; map detection coverage against MITRE ATT&CK techniques T1078, T1566, T1195.002, T1539, and T1574.001 to identify blind spots.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and regulatory liaison immediately if: confirmed ransomware deployment on financial systems (eCrime leak site listing imminent, GLBA breach notification clock starts), evidence of DPRK IT worker with privileged access to cryptocurrency custody or payment rail systems (potential $2B-scale asset theft vector), or M365 OAuth persistence indicating active MURKY PANDA credential harvesting still in progress — any of these conditions triggers mandatory FFIEC/OCC notification timelines and potential FinCEN SAR filing obligations.
Recovery Notes	Restore only from backups with a confirmed clean timestamp predating the earliest identified IOC in Entra ID sign-in logs; do not trust backups created after the initial OAuth consent grant anomaly. Post-restoration, monitor Entra ID risky sign-ins, Exchange Online inbox rule creation events, and LOLBin process telemetry at elevated frequency (minimum hourly review) for 30 days, as DPRK and eCrime operators commonly re-establish access within weeks of partial remediation. Treat all service account credentials and OAuth client secrets that existed during the intrusion window as fully compromised regardless of whether direct access evidence exists, and enforce complete rotation before returning any payment or custody systems to production.

Forensic Artifacts	Azure AD / Entra ID Unified Audit Log — OAuth consent grant events (RecordType: AzureActiveDirectory, Operation: 'Consent to application') and impossible-travel sign-in records: primary evidence for MURKY PANDA credential harvesting via illicit OAuth consent phishing targeting M365 environments | Exchange Online mailbox audit log — 'AddFolderPermissions', 'UpdateInboxRules', and 'MailItemsAccessed' operations: direct forensic evidence of T1114.002 (Email Collection: Remote Email Collection) used by hands-on-keyboard intrusion operators to stage financial data exfiltration | Windows Sysmon Event ID 1 (Process Create) logs showing process ancestry chains — specifically certutil.exe, mshta.exe, or wscript.exe spawned from M365 desktop client or browser processes: fingerprint of LOLBin abuse consistent with post-compromise hands-on-keyboard activity documented in the 43% intrusion surge | Git repository commit history and CI/CD pipeline build logs for third-party integrations touching cryptocurrency custody or fintech payment APIs — look for unexplained dependency version bumps, new package additions, or modified build scripts in the intrusion window: forensic evidence of T1195.002 supply chain compromise used to target digital asset custody systems | Azure AD external/guest account creation and role assignment audit logs correlated with HR contractor onboarding records — mismatches between account creation events and documented hiring actions are the primary forensic indicator of DPRK IT worker insertion, and this artifact bundle is essential for both internal investigation and potential law enforcement / OFAC referral given the $2.02B theft attribution

Per-Action IR Details

Containment — Audit Microsoft 365 OAuth application grants and conditional access policies immediately; revoke unrecognized delegated permissions and disable legacy authentication protocols to cut off MURKY PANDA-style credential harvesting entry points.

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 SI-4 (System Monitoring), CIS 6.2 (Establish an Access Revoking Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: Run the free Microsoft 365 tool 'Microsoft Entra ID PowerShell' (Az module): `Get-AzureADServicePrincipal -All $true | Get-AzureADServicePrincipalOAuth2PermissionGrant` to enumerate all OAuth grants. Cross-reference output against a known-good baseline. For legacy auth blocking without Conditional Access Premium, use Exchange Online PowerShell: `Set-AuthenticationPolicy -AllowBasicAuthActiveSync $false -AllowBasicAuthImap $false -AllowBasicAuthPop $false` and assign via `Set-User -Identity -AuthenticationPolicy`. A 2-person team can complete the full tenant audit in 2–4 hours using the free Microsoft 365 Admin Center OAuth app consent report under Azure AD > Enterprise Applications > User Consent.

Evidence: Before revoking any permissions, export and preserve: (1) Azure AD Sign-In Logs filtered for 'Legacy Authentication Client' and 'OAuth2 token issuance' events from the 30 days prior — download as CSV from Entra ID > Monitoring > Sign-in logs; (2) Full OAuth permission grant list via `Get-AzureADOAuth2PermissionGrant` capturing AppId, ConsentType, Scope, and PrincipalId for every delegated grant; (3) Exchange Online mailbox audit logs for 'MailboxLogin', 'AddFolderPermissions', and 'UpdateInboxRules' operations (Admin Audit Log via `Search-UnifiedAuditLog -Operations MailboxLogin,AddFolderPermissions,UpdateInboxRules`); (4) Conditional Access policy export (JSON) via Entra ID > Security > Conditional Access > Policies > Export, capturing the pre-remediation policy state; (5) Azure AD App Registrations list with reply URLs, to detect MURKY PANDA-style adversary-registered lookalike apps used in OAuth phishing.

Detection — Query identity provider logs for anomalous OAuth consent grants, impossible-travel sign-ins, and Exchange Online mailbox delegation events (T1114.002); correlate endpoint telemetry for LOLBin abuse (certutil, mshta, wscript) consistent with hands-on-keyboard intrusion patterns.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without SIEM: (1) OAuth/impossible-travel — Use Microsoft Entra ID free tier's 'Risky Sign-ins' report (Entra ID > Security > Risky Sign-ins) and export to CSV; run `Search-UnifiedAuditLog -RecordType AzureActiveDirectory -Operations 'Consent to application'` in Exchange Online PowerShell to surface all OAuth consent events. (2) T1114.002 mailbox delegation — Run `Search-UnifiedAuditLog -Operations 'AddMailboxPermission','AddFolderPermissions','Set-MailboxFolderPermission' -StartDate -EndDate `. (3) LOLBin detection on endpoints — Deploy Sysmon with SwiftOnSecurity's public config (github.com/SwiftOnSecurity/sysmon-config); query Windows Event Log for Sysmon Event ID 1 (Process Create) where ParentImage contains the vulnerable M365 sync or Office process and Image matches certutil.exe, mshta.exe, or wscript.exe: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -match 'certutil|mshta|wscript'}`. Use the public Sigma rule 'proc_creation_win_lolbin_certutil' mapped to ATT&CK T1105 and T1140 for offline log matching.

Evidence: Preserve before any remediation: (1) Entra ID Unified Audit Log export covering the full 90-day retention window for RecordTypes AzureActiveDirectory, ExchangeAdmin, and ExchangeItem — critical for establishing MURKY PANDA dwell time; (2) Sysmon Event ID 1 logs from endpoints showing process ancestry chains where certutil.exe, mshta.exe, or wscript.exe spawned from Office or browser processes (hands-on-keyboard intrusion fingerprint); (3) Exchange Online message trace logs (`Get-MessageTrace`) for the suspected compromise window, capturing sender, recipient, and delivery status to identify exfiltration via forwarding rules (T1114.002); (4) Windows Security Event Log Event ID 4688 (Process Creation with command line) from endpoints where M365 desktop clients or browser-based SSO sessions were active, filtering on LOLBin command lines; (5) Network flow data (if available via Wireshark or NetFlow) for outbound connections from LOLBin processes to non-Microsoft IPs, particularly during business hours consistent with DPRK operator time zones (UTC+9).

Eradication — Remove unauthorized IT worker accounts and contractor identities with privileged access; verify software supply chain integrity for any third-party integrations touching cryptocurrency custody or fintech payment rails (T1195.002, CWE-494); enforce code signing and dependency integrity checks.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SA-12 (Supply Chain Protection), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For DPRK IT worker account removal without IAM tooling: (1) Export all Azure AD guest and external member accounts via `Get-AzureADUser -Filter 'userType eq Guest'`; cross-reference creation dates, manager assignments, and last sign-in against HR records — DPRK IT workers often have no manager assigned, implausible geographic inconsistencies, or creation dates coinciding with contractor onboarding spikes. (2) For supply chain integrity of fintech integrations, run `pip audit` (Python) or `npm audit` against all dependency manifests in payment rail codebases; use the free OWASP Dependency-Check CLI (`dependency-check.sh --project --scan `) to flag CWE-494 (Download of Code Without Integrity Check) patterns. (3) Enforce code signing checks using sigcheck.exe (Sysinternals, free) on all third-party DLLs and executables in custody/payment processing paths: `sigcheck -u -e ` lists all unsigned binaries. (4) Verify npm package integrity via `npm ci` with a locked package-lock.json and compare SHA-512 hashes against the public registry.

Evidence: Preserve before account removal: (1) Full Azure AD audit log entries for each suspicious account — specifically 'Add member to role', 'Add user', and 'Update user' operations with actor identity and IP (Search-UnifiedAuditLog -Operations 'Add member to role','Add user'); (2) Access review history showing what privileged resources (Key Vaults, payment API credentials, custody wallet service principals) the suspected DPRK IT worker accounts touched — export from Entra ID Access Reviews or manually via `Get-AzureADUserAppRoleAssignment`; (3) Git commit history and CI/CD pipeline logs for any third-party integrations modified during the suspected intrusion window — look for dependency version bumps or new package additions in package.json, requirements.txt, or pom.xml that don't correspond to approved change tickets; (4) Hash values

(SHA-256) of all third-party libraries in cryptocurrency custody or payment rail environments, captured pre-remediation via `Get-FileHash -Algorithm SHA256 -Path -Recurse`, for post-remediation integrity comparison; (5) HR and contractor onboarding records cross-referenced against account creation events to document the DPRK worker insertion vector for regulatory reporting.

Recovery — Validate MFA enforcement across all privileged and external-facing accounts; restore from known-clean backups for any systems touched by ransomware operators; confirm no persistent backdoors remain via full credential rotation and reviewed service account inventory.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST SI-6 (Security and Privacy Function Verification), 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), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords)

Compensating: For teams without enterprise PAM or backup orchestration: (1) MFA validation — Run `Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0}` (MSOnline module, free) to list all accounts lacking MFA; prioritize accounts with Exchange Online, SharePoint, or Azure Key Vault access. (2) Backdoor persistence check — Use Autoruns (Sysinternals, free) with VirusTotal integration enabled on all restored systems: `autorunsc.exe -a * -c -h -s '*' -vt > autoruns_output.csv`; flag any entries not present in a known-good baseline. For M365 persistence specifically, re-run the OAuth grant audit post-restoration and check for re-added inbox rules via `Get-InboxRule -Mailbox `. (3) Service account inventory — Export all Azure AD service principals with credentials: `Get-AzureADServicePrincipal -All $true | Where-Object {$_.KeyCredentials -ne $null -or $_.PasswordCredentials -ne $null}`; rotate all secrets and certificates that were accessible during the intrusion window. (4) For ransomware-touched systems, verify backup integrity with a test restore to an isolated VM before returning to production; use Veeam Free or Windows Server Backup for SMB environments.

Evidence: Preserve before and during recovery: (1) Ransomware operator TTPs evidence — Windows VSS shadow copy deletion logs (Event ID 524 in System log, or Sysmon Event ID 1 showing vssadmin.exe/wmic.exe with 'delete shadows' arguments) confirming which systems were in scope for the eCrime operators; (2) Full service account credential exposure scope — Azure Key Vault access logs (if enabled) or local Windows Credential Manager exports via `cmdkey /list` on affected systems, establishing which secrets were potentially harvested; (3) Pre-restoration disk images (forensic-grade, E01 format preferred) of any system confirmed touched by ransomware operators, captured before restoration, to support regulatory breach notification and potential law enforcement referral; (4) MFA registration audit log (Entra ID > Security > Authentication Methods > User Registration Details) exported pre- and post-remediation to document the MFA gap that existed during the intrusion; (5) Backup system access logs confirming the last known-clean backup timestamp predates the initial access indicator, establishing a defensible recovery point for audit purposes.

Post-Incident — Review threat intelligence program structure for nation-state/eCrime convergence gaps; ensure SOC playbooks address dual-extortion scenarios and DPRK IT worker insertion red flags; map detection coverage against MITRE ATT&CK techniques T1078, T1566, T1195.002, T1539, and T1574.001 to identify blind spots.

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 IR-2 (Incident Response Training), NIST IR-3 (Incident Response Testing), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a dedicated CTI platform: (1) ATT&CK coverage mapping — Use the free MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) to layer current detection capabilities against T1078 (Valid Accounts), T1566 (Phishing), T1195.002 (Compromise Software Supply Chain), T1539 (Steal Web Session Cookie), and T1574.001 (DLL Search Order Hijacking); highlight gaps in red and assign Sysmon or Sigma rule

coverage to each. (2) DPRK IT worker playbook additions — Document specific red flags from this campaign: contractor accounts with no manager, resume inconsistencies, requests for VPN split tunneling, unusual working hours for stated location, and reluctance to appear on video calls; add to contractor onboarding checklist. (3) Dual-extortion playbook — Use the free CISA Ransomware Response Checklist (cisa.gov) as a baseline; add a financial services-specific decision tree for leak site notification triggers under GLBA and relevant state breach laws. (4) Subscribe to free ISAC threat feeds — FS-ISAC (Financial Services ISAC) offers member threat bulletins; CISA's free TAXII/STIX feed at cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools provides DPRK-attributed IOCs.

Evidence: Preserve for lessons-learned and program improvement: (1) Complete incident timeline reconstruction from Entra ID, Exchange Online, and endpoint logs establishing initial access to detection gap — this documents the dwell time metric required for NIST 800-61r3 §4 post-incident review and any GLBA/FFIEC examination response; (2) All IOCs identified during the incident (OAuth app IDs, suspicious IP addresses, LOLBin command line strings, unauthorized account UPNs) formatted as STIX 2.1 objects for sharing with FS-ISAC and CISA; (3) ATT&CK Navigator layer file (JSON) saved from the coverage mapping exercise, documenting which of T1078, T1566, T1195.002, T1539, and T1574.001 had no detection rule at time of incident — this becomes the evidence base for the SOC tooling investment case; (4) Redlined copies of SOC playbooks showing gaps identified during this incident (e.g., no dual-extortion decision tree, no DPRK IT worker insertion criteria) alongside the updated versions, for audit trail purposes; (5) Tabletop exercise after-action report (if conducted) documenting whether the team could detect MURKY PANDA-style OAuth phishing and DPRK IT worker insertion under simulation — required for NIST IR-3 (Incident Response Testing) compliance evidence.

Detection Guidance

Microsoft 365 and Entra ID: Alert on OAuth app consent grants outside approved inventory, risky sign-ins flagged by Identity Protection, and new mailbox delegation or forwarding rules (T1114.002). Endpoint: Hunt for hands-on-keyboard indicators, interactive sessions spawning LOLBins (certutil, mshta, rundll32), PowerShell with encoded commands, and unexpected use of remote management tools. Network: Monitor for anomalous outbound exfiltration volumes via cloud storage services (T1567) and Tor exit node communication (T1090.003). Identity: Flag accounts with valid credentials authenticating from new geographies or devices without MFA challenge, particularly contractor and third-party vendor accounts (T1078). Supply chain: Verify package integrity hashes against known-good repositories for any CI/CD-integrated dependencies; alert on unsigned or hash-mismatched downloads (CWE-494, T1195.002). Session tokens: Detect token replay attacks by correlating session creation events with originating IP and device fingerprint divergence (T1539). DPRK IT worker insertion: Review contractor identity verification processes; flag accounts created recently with limited employment history or inconsistent professional profiles performing privileged actions (T1591).

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1204** — User Execution
- **T1591** — Gather Victim Org Information
- **T1567** — Exfiltration Over Web Service
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1114.002** — Remote Email Collection

- **T1555** — Credentials from Password Stores
- **T1195.002** — Compromise Software Supply Chain
- **T1598** — Phishing for Information
- **T1199** — Trusted Relationship
- **T1090.003** — Multi-hop Proxy
- **T1539** — Steal Web Session Cookie
- **T1534** — Internal Spearphishing
- **T1588.001** — Malware
- **T1657** — Financial Theft
- **T1574.001** — DLL

NIST-800-53R5

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

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1204	User Execution	Execution
T1591	Gather Victim Org Information	Reconnaissance
T1567	Exfiltration Over Web Service	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1114.002	Remote Email Collection	Collection
T1555	Credentials from Password Stores	Credential-Access
T1195.002	Compromise Software Supply Chain	Initial-Access

Technique ID	Technique Name	Tactic
T1598	Phishing for Information	Reconnaissance
T1199	Trusted Relationship	Initial-Access
T1090.003	Multi-hop Proxy	Command-And-Control
T1539	Steal Web Session Cookie	Credential-Access
T1534	Internal Spearphishing	Lateral-Movement
T1588.001	Malware	Resource-Development
T1657	Financial Theft	Impact
T1574.001	DLL	Persistence

Sources

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

Generated 2026-05-18 06:14 UTC by TJS Security Command Center