INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-16 18:52 UTC

# Financial Sector Under Siege: AI-Accelerated Adversaries Drive Record Intrusions and Billion-Dollar Theft in 2025-2026

**THREAT CAMPAIGN** | **HIGH** | CVSS 9.5

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0325 |
| **Type** | Threat Campaign |
| **Severity** | HIGH |
| **CVSS Base Score** | 9.5 |
| **Affected Products** | Financial institutions (global), cryptocurrency exchanges, fintech platforms, insurance entities, Microsoft 365 environments (MURKY PANDA targeting) |
| **Discovery Source** | Rss:T1 Threatintel |

## Executive Summary

Adversaries, led by North Korean state-linked actors and organized eCrime groups, executed a sustained, AI-assisted assault on global financial institutions throughout 2025, stealing $2.02 billion in digital assets and driving a 43% rise in hands-on intrusions against the sector (per CrowdStrike 2026 Financial Services Threat Landscape Report). AI tooling is now compressing attacker dwell time and enabling synthetic identity fraud at scale, including deepfake-assisted social engineering targeting bank employees and fintech platforms. Financial institutions relying on perimeter controls and signature-based detection face significant exposure to adversaries operating faster than traditional alert-response cycles.

## Technical Analysis

Source: CrowdStrike 2026 Financial Services Threat Landscape Report (T1 vendor threat intelligence, crowdstrike.com). Campaign attribution and theft metrics sourced to this report. No CVE applies; this is a campaign-level intelligence item. Relevant CWEs: CWE-287 (Improper Authentication), CWE-284 (Improper Access Control), CWE-494 (Download of Code Without Integrity Check), CWE-346 (Origin Validation Error). Attack vectors span multiple MITRE ATT&CK techniques: T1586.002 (Compromise Accounts: Email Accounts), T1566/T1566.004 (Phishing variants), T1621 (Multi-Factor Authentication Request Generation), T1539 (Steal Web Session Cookie), T1550.001 (Use Alternate Authentication Material: Application Access Token), T1078 (Valid Accounts), T1021 (Remote Services), T1090.003 (Proxy: Multi-hop Proxy), T1574.001 (DLL Search Order Hijacking), T1071/T1071.001 (Application Layer Protocol), T1059 (Command and Scripting Interpreter), T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain), T1657 (Financial Theft), T1486

(Data Encrypted for Impact), T1069 (Permission Groups Discovery), T1204 (User Execution), T1598.003 (Spearphishing Link), T1588 (Obtain Capabilities). MURKY PANDA is actively targeting Microsoft 365 environments; attack paths include federated SSO abuse, cloud identity provider compromise, and fintech API surface exploitation. DPRK-nexus actors (Lazarus Group / TraderTraitor cluster, high-confidence attribution) are using insider placement, social engineering, and cryptocurrency mixer services for obfuscation.
Hands-on-keyboard intrusion rates rose 43% globally and 48% in North America over a two-year window, indicating living-off-the-land tradecraft replacing automated malware. AI is operationalized to synthesize personas, automate vishing via deepfake voice and video, and accelerate lateral movement.

## Action Checklist

1. Detection Priority, Query Microsoft 365 Unified Audit Log for anomalous sign-ins (impossible travel, new device registration, MFA fatigue events matching T1621); hunt for T1539 and T1550.001 indicators including unexpected session token reuse and application access token issuance from unfamiliar IP ranges; cross-reference against CrowdStrike Falcon Intelligence, Recorded Future, or MISP feeds for DPRK and MURKY PANDA infrastructure indicators.
2. Immediate Containment & Triage, Audit all federated SSO configurations and cloud identity provider trust relationships in Microsoft 365 and connected fintech platforms; review Entra ID audit logs and conditional access policies; revoke anomalous OAuth tokens and suspicious delegated permissions immediately.
3. Eradication, Enforce phishing-resistant MFA (FIDO2/passkeys) across all privileged and externally facing financial system accounts; eliminate SMS and voice-call MFA fallback paths; audit and harden API authentication surfaces on fintech integrations, enforcing origin validation controls (CWE-346) and integrity checks on third-party code dependencies (CWE-494).
4. Recovery & Validation, Validate that all revoked sessions and tokens have not been re-issued; confirm conditional access policies are enforcing compliant device requirements; restore operations only after confirming no persistence mechanisms (scheduled tasks, rogue OAuth apps, backdoor accounts) remain in the M365 tenant and connected cloud infrastructure.
5. Post-Incident & Resilience, Conduct a tabletop exercise simulating AI-assisted vishing against finance and HR personnel; review insider threat detection coverage against the TraderTraitor placement pattern; assess whether current detection tooling can identify living-off-the-land lateral movement at machine-assisted tempo, and close gaps with behavioral analytics or EDR telemetry tuning.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate immediately to executive leadership, legal counsel, and your primary financial regulator (FinCEN, OCC, NYDFS, or equivalent) if confirmed unauthorized access to customer account data, wire transfer systems, or digital asset custody infrastructure is detected, or if DPRK/OFAC-sanctioned entity infrastructure is confirmed in attack path — the latter triggers mandatory OFAC reporting obligations independent of breach notification thresholds. |

| | |
|---|---|
| **Recovery Notes** | Before restoring any financial transaction processing systems, complete a full service principal and OAuth application audit against a pre-incident baseline and obtain signed confirmation from the system owner that no persistence mechanisms remain — given TraderTraitor's documented pattern of maintaining parallel access paths, a single revocation pass is insufficient. Monitor Entra ID sign-in logs, Exchange Online mail flow, and API gateway access logs continuously for a minimum of 30 days post-recovery at elevated frequency (daily manual review or automated alerting), specifically for re-authentication attempts from the same ASNs and IP ranges identified during the incident. Coordinate with your correspondent banks, payment processors, and fintech integration partners to notify them of the incident scope so they can independently review their own trust relationships with your tenant — lateral movement from a compromised financial institution to its integration partners is a documented tactic in organized eCrime campaigns targeting the financial sector. |
| **Forensic Artifacts** | Microsoft 365 Unified Audit Log entries for Operations 'UserLoggedIn', 'MailItemsAccessed', 'Add delegation', 'Consent_to_application', and 'Add-AppRoleAssignment' — these are the specific audit events generated by DPRK/MURKY PANDA OAuth abuse and session token theft (T1539, T1550.001) in M365 environments; preserve full JSON including ClientIP, UserAgent, SessionId, and ResultStatus fields before the 30/90-day rolling retention window expires. \| Entra ID Identity Protection risk detections export ('Get-MgRiskDetection') capturing 'impossibleTravel', 'anonymizedIPAddress', 'maliciousIPAddress', and 'newCountry' riskEventTypes — these are the machine-generated signals that correlate directly to AI-accelerated attacker infrastructure rotation and the impossible travel patterns produced when adversaries relay through compromised residential proxies to bypass geo-based conditional access. \| Exchange Online inbox rules and mail forwarding configurations for all accounts ('Get-InboxRule' across all mailboxes) — external auto-forwarding rules are a primary data exfiltration and persistent access mechanism used in MURKY PANDA M365 targeting of financial institutions, and these rules survive password resets if not explicitly removed. \| Entra ID service principal credential history including all PasswordCredentials and KeyCredentials with their StartDateTime and EndDateTime fields — DPRK actors (TraderTraitor) have documented tradecraft of adding long-lived client secrets to existing legitimate enterprise application service principals to maintain persistent authentication without triggering new app registration alerts. \| HR system and KYC platform audit logs covering new employee onboarding actions, identity document submissions, and account privilege escalation requests from the 90 days preceding incident discovery — TraderTraitor's documented use of fraudulent IT worker placement means the initial access vector may originate in HR/onboarding workflows rather than technical exploitation, and synthetic identity documents (AI-generated) submitted during this period are primary forensic artifacts. |

### Per-Action IR Details

**Containment — Audit all federated SSO configurations and cloud identity provider trust relationships in Microsoft 365 and connected fintech platforms; revoke anomalous OAuth tokens and suspicious delegated permissions immediately using Entra ID audit logs and conditional access policy review.**

**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 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

**Compensating:** For teams without Entra ID P2 or a SIEM: use the free Microsoft Graph PowerShell SDK to enumerate and revoke OAuth tokens — run 'Get-MgUserOauth2PermissionGrant -UserId ' for each privileged account, then 'Remove-MgOauth2PermissionGrant' on anomalous entries. Export the full Unified Audit Log via

'Search-UnifiedAuditLog -Operations Add_delegation,Add-AppRoleAssignment,Consent_to_application' scoped to the last 90 days and parse in Excel or Python pandas for unfamiliar app IDs. Cross-reference discovered app IDs against the CISA guidance on malicious OAuth application activity.

**Evidence:** Before revoking any token, snapshot the full Entra ID sign-in log (Azure Portal → Entra ID → Sign-in logs, export as CSV) preserving IP, ASN, device ID, token issuance timestamps, and conditional access result fields. Capture 'Get-MgAuditLogSignIn' output filtering on RiskState eq 'atRisk' and RiskDetail fields. Export all current OAuth application permission grants via 'Get-MgServicePrincipalOauth2PermissionGrant' — this is the forensic baseline that proves which apps held delegated access before revocation. Screenshot or export the Conditional Access policy state from Entra ID before any policy changes are made, preserving the pre-incident configuration as evidence.

**Detection — Query Microsoft 365 Unified Audit Log for anomalous sign-ins (impossible travel, new device registration, MFA fatigue events matching T1621); hunt for T1539 and T1550.001 indicators including unexpected session token reuse and application access token issuance from unfamiliar IP ranges; cross-reference against known DPRK and eCrime infrastructure where available from your TI feeds.**

**NIST Phase:** Detection Analysis

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

**Controls:** NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without a SIEM, query the Unified Audit Log directly via PowerShell: 'Search-UnifiedAuditLog -Operations UserLoggedIn,UserLoginFailed -StartDate (Get-Date).AddDays(-30) -ResultSize 5000 | Where-Object {$_.AuditData -match "MFADenied|FreshTokenNeeded|DeviceNotCompliant"}' to surface MFA push fatigue (T1621) events. For T1550.001 (Pass-the-Cookie), hunt for session reuse anomalies by exporting 'Search-UnifiedAuditLog -Operations MailItemsAccessed' and comparing SessionId values against device and IP consistency — a single SessionId appearing from two geographically distinct IPs within minutes is the indicator. Pull DPRK/TraderTraitor and MURKY PANDA IP IOCs from CISA advisories and the OFAC SDN list, then grep the exported CSV: 'Import-Csv auditlog.csv | Where-Object {$_.ClientIP -in $iocList}'.

**Evidence:** Export the full Unified Audit Log for the Operations 'UserLoggedIn', 'Add delegation', 'MailItemsAccessed', 'FileAccessed', and 'TeamsMemberAdded' covering at minimum 90 days — DPRK actors (TraderTraitor TTPs) commonly maintain long dwell periods before theft events. Capture Entra ID Identity Protection risk detections via 'Get-MgRiskDetection' — preserve the 'detectionTimingType', 'ipAddress', 'location', and 'riskEventType' fields which will document impossible travel and anomalous token events tied to MURKY PANDA M365 targeting. If Microsoft Defender for Cloud Apps is licensed, export the activity log for app governance anomaly alerts. Preserve raw sign-in log JSON before any remediation — log truncation after 30 days (basic Entra) or 90 days (P2) means this evidence is time-sensitive.

**Eradication — Enforce phishing-resistant MFA (FIDO2/passkeys) across all privileged and externally facing financial system accounts; eliminate SMS and voice-call MFA fallback paths; audit and harden API authentication surfaces on fintech integrations, enforcing origin validation controls (CWE-346) and integrity checks on third-party code dependencies (CWE-494).**

**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 SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SI-10 (Information Input Validation), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

**Compensating:** For teams that cannot immediately deploy FIDO2 hardware tokens: enforce number matching and additional context in Microsoft Authenticator (free, configurable in Entra ID Authentication Methods policy) as an interim control against MFA fatigue (T1621) — this does not eliminate the risk but significantly raises attacker effort. For API origin validation (CWE-346) on fintech integrations without a WAF budget, implement HMAC request signing at the API gateway layer and validate the 'Origin' and 'Referer' headers server-side using free middleware. For CWE-494 (third-party code integrity), run 'pip-audit' or 'npm audit' against all fintech integration dependencies and implement

Subresource Integrity (SRI) hashes on any externally loaded scripts — the DPRK supply chain playbook (as seen in TraderTraitor activity) specifically targets this attack surface.

**Evidence:** Before modifying authentication configurations, export the current Entra ID Authentication Methods policy state via 'Get-MgPolicyAuthenticationMethodPolicy' — this documents which legacy MFA methods (SMS, voice) were active and for which user populations, establishing the pre-incident attack surface for regulatory reporting. Run 'Get-MgUserAuthenticationMethod -UserId ' across all privileged accounts to inventory existing authenticator registrations and identify accounts with only SMS/voice methods — this list defines the scope of the eradication action. For API surface hardening, capture current API gateway access logs (APIM diagnostic logs or equivalent) showing all third-party integration traffic patterns before policy enforcement, as these baselines are required to distinguish legitimate traffic from anomalous post-enforcement attempts.

**Recovery — Validate that all revoked sessions and tokens have not been re-issued; confirm conditional access policies are enforcing compliant device requirements; restore operations only after confirming no persistence mechanisms (scheduled tasks, rogue OAuth apps, backdoor accounts) remain in the M365 tenant and connected cloud infrastructure.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST CA-2 (Control Assessments), NIST CM-2 (Baseline Configuration), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 5.3 (Disable Dormant Accounts)

**Compensating:** For M365 tenant persistence hunting without Microsoft Sentinel: run the free CISA-recommended 'Sparrow' tool (PowerShell-based, GitHub: cisagov/Sparrow) or 'Hawk' (GitHub: T0pCyber/hawk) to enumerate rogue OAuth applications, mail forwarding rules, mailbox delegation anomalies, and service principal credential additions — these are the exact persistence mechanisms documented in DPRK/MURKY PANDA M365 intrusions. For scheduled task persistence on endpoints connected to the tenant, run 'Get-ScheduledTask | Where-Object {$_.TaskPath -notlike "\Microsoft*"} | Select TaskName, TaskPath, @{N="Actions";E={$_.Actions.Execute}}' on all Windows endpoints and compare against a known-good baseline. Validate no new Entra ID directory roles have been granted by running 'Get-MgDirectoryRole | ForEach {Get-MgDirectoryRoleMember -DirectoryRoleId $_.Id}' and diffing against pre-incident exports.

**Evidence:** Capture a full export of all Entra ID enterprise application service principals including credential expiry dates and owner assignments via 'Get-MgServicePrincipal -All | Select DisplayName, AppId, AccountEnabled, PasswordCredentials, KeyCredentials' — DPRK actors have been documented adding long-lived credentials to existing service principals as persistence rather than registering new obvious apps. Pull Exchange Online mail forwarding rules for all accounts: 'Get-Mailbox -ResultSize Unlimited | Get-InboxRule | Where-Object {$_.ForwardTo -ne $null -or $_.RedirectTo -ne $null}' — data exfiltration via auto-forwarding to external addresses is a documented TraderTraitor and MURKY PANDA tactic. Document the conditional access named locations and trusted IP ranges at recovery time as a signed artifact for post-incident review.

**Post-Incident — Conduct a tabletop exercise simulating AI-assisted vishing against finance and HR personnel; review insider threat detection coverage against the TraderTraitor placement pattern; assess whether current detection tooling can identify living-off-the-land lateral movement at machine-assisted tempo, and close gaps with behavioral analytics or EDR telemetry tuning.**

**NIST Phase:** Post Incident

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

**Controls:** NIST IR-2 (Incident Response Training), NIST IR-3 (Incident Response Testing), NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-4 (System Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** For tabletop simulation of AI-assisted vishing without a commercial red team: use publicly available deepfake audio samples or the free ElevenLabs free tier to create a synthetic voice clone of a known executive (with legal authorization) and run a controlled call to a finance team member requesting a wire transfer or credential

confirmation — this directly replicates the social engineering vector documented in 2025 financial sector campaigns. For TraderTraitor insider placement detection without a UEBA platform, implement Sysmon with the SwiftOnSecurity config and write targeted Sigma rules (free, GitHub: SigmaHQ/sigma) for anomalous developer account behaviors: bulk repository cloning, access to CI/CD secrets, and SSH key additions outside business hours. For living-off-the-land detection gap assessment, run the free Atomic Red Team (GitHub: redcanaryco/atomic-red-team) test T1059.001 (PowerShell) and T1218 (Signed Binary Proxy Execution) against a test endpoint and verify your current tooling generates alerts — if it does not, tune Sysmon EventID 1 (Process Creation) rules to alert on LOLBin parent-child chains.

**Evidence:** Preserve the complete lessons-learned documentation from this incident including dwell time measurement, initial access vector confirmation, and identity of all compromised accounts — NIST 800-61r3 §4 requires this for IR capability improvement and it constitutes the evidentiary basis for regulatory reporting under FinCEN SAR obligations and potential NYDFS Part 500 breach notification. Retain all Entra ID audit logs, Unified Audit Logs, and endpoint telemetry for a minimum of 12 months given the financial sector regulatory retention requirements and the likelihood of parallel DPRK intrusion threads that may surface in future investigations. Document the specific AI-generated artifacts observed (deepfake call recordings if captured, synthetic identity documents submitted to HR or KYC processes) as these establish precedent indicators for future TraderTraitor and AI-assisted fraud detection rule development.

## Detection Guidance

Priority detection signals for this campaign cluster: (1) Microsoft 365 Unified Audit Log, filter for AuditLog events 'UserLoggedIn' with DeviceTrustType=null from new ASNs, combined with rapid MFA push sequences (T1621 pattern); (2) Entra ID Sign-in Logs, flag sign-ins with unfamiliar application IDs receiving delegated token grants, particularly to finance or HR applications (T1550.001); (3) EDR telemetry, hunt for LOLBin execution chains (T1059) originating from Office processes or browser contexts on endpoints with financial system access; (4) Network/proxy logs, identify multi-hop proxy patterns (T1090.003) from endpoints communicating with cryptocurrency exchange APIs; (5) Email gateway, hunt spearphishing (T1566, T1598.003) targeting finance, treasury, and HR roles with voice/video call lures consistent with AI-generated deepfake vishing campaigns; (6) Insider threat signals, monitor for new employees or contractors with privileged financial system access exhibiting unusual after-hours access patterns or bulk data staging (T1069, T1588 combinations). Per CrowdStrike 2026 Financial Services Threat Landscape Report, no public IOC set accompanies this advisory. Consult CrowdStrike Falcon Intelligence, Recorded Future, or MISP community feeds for actor-specific indicators against MURKY PANDA and TraderTraitor infrastructure.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| URL | `Not available` | No specific IOCs have been publicly released with the CrowdStrike 2026 Financial Services Threat Landscape Report at this time. Consult CrowdStrike Falcon Intelligence or your contracted TI feed for MURKY PANDA and TraderTraitor-specific indicators. | LOW |

## Framework Mappings

### MITRE-ATTACK

- **T1090.003** — Multi-hop Proxy
- **T1586.002** — Email Accounts
- **T1059** — Command and Scripting Interpreter
- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing
- **T1588** — Obtain Capabilities
- **T1550.001** — Application Access Token
- **T1071** — Application Layer Protocol
- **T1621** — Multi-Factor Authentication Request Generation
- **T1539** — Steal Web Session Cookie
- **T1598.003** — Spearphishing Link
- **T1204** — User Execution
- **T1574.001** — DLL
- **T1021** — Remote Services
- **T1657** — Financial Theft
- **T1078** — Valid Accounts
- **T1195.002** — Compromise Software Supply Chain
- **T1566.004** — Spearphishing Voice
- **T1071.001** — Web Protocols
- **T1069** — Permission Groups Discovery

### NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management

- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **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
- **A01:2021** — Broken Access Control
- **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
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **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
- **164.312(a)(1)** — Access Control
- **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.5.23** — Information security for use of cloud services

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1090.003 | Multi-hop Proxy | Command-And-Control |
| T1586.002 | Email Accounts | Resource-Development |
| T1059 | Command and Scripting Interpreter | Execution |
| T1486 | Data Encrypted for Impact | Impact |
| T1566 | Phishing | Initial-Access |
| T1588 | Obtain Capabilities | Resource-Development |
| T1550.001 | Application Access Token | Defense-Evasion |
| T1071 | Application Layer Protocol | Command-And-Control |
| T1621 | Multi-Factor Authentication Request Generation | Credential-Access |
| T1539 | Steal Web Session Cookie | Credential-Access |
| T1598.003 | Spearphishing Link | Reconnaissance |
| T1204 | User Execution | Execution |
| T1574.001 | DLL | Persistence |
| T1021 | Remote Services | Lateral-Movement |
| T1657 | Financial Theft | Impact |
| T1078 | Valid Accounts | Defense-Evasion |
| T1195.002 | Compromise Software Supply Chain | Initial-Access |
| T1566.004 | Spearphishing Voice | Initial-Access |
| T1071.001 | Web Protocols | Command-And-Control |
| T1069 | Permission Groups Discovery | Discovery |

## 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://cxotoday.com/cybersecurity/the-billion-dollar-heist-north-k... | T3 |
| | https://www.crowdstrike.com/en-us/blog/crowdstrike-expands-real-tim... | T3 |

| Source | URL | Tier |
|---|---|---|
| **Financial threats amplify: rising concerns in the industry** | https://digitalisationworld.com/news/72319/financial-threats-amplif... | T3 |



Generated 2026-05-16 18:52 UTC by TJS Security Command Center