INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-26 06:08 UTC

Financial Services Under Siege: DPRK Steals $2B, Ransomware Surges 27%, and China-Nexus Groups Expand Espionage Operations

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0364
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Financial institutions, cryptocurrency exchanges, fintech platforms, insurance entities, traditional banks; Microsoft 365 environments (MURKY PANDA targeting); global financial sector infrastructure
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Financial Services Threat Landscape Report documents a sharp escalation across three simultaneous threat categories targeting the financial sector: DPRK-nexus actors stole $2.02 billion in digital assets over the past 12 months, ransomware operators listed 423 financial entities on data leak sites (a 27% year-over-year increase), and China-nexus group MURKY PANDA conducted cloud espionage via compromised third-party access. Financial institutions, cryptocurrency exchanges, fintech platforms, and traditional banks face concurrent pressure from criminal extortion, state-sponsored theft, and sustained intelligence collection, often within the same environment. The convergence of these threat categories, combined with a 43% year-over-year rise in hands-on-keyboard intrusions and AI-assisted adversary tradecraft, results in documented financial loss, regulatory penalties (DORA, FFIEC, PCI-DSS breach notifications), and operational disruption consistent with 90+ day dwell times observed in MURKY PANDA intrusions.

Technical Analysis

This item reflects a campaign-level threat landscape report, not a discrete vulnerability. No CVEs are cited; the CVSS 9.5 figure in the source data is an editorial severity estimate. Three CWEs are mapped by the source data: CWE-346 (Origin Validation Error, relevant to trusted-relationship intrusions where third-party access is not properly scoped), CWE-287 (Improper Authentication, relevant to account compromise and web shell deployment), and CWE-306 (Missing Authentication for Critical Function, relevant to cloud access paths

exploited by MURKY PANDA). Key MITRE ATT&CK techniques include T1199 (Trusted Relationship) and T1550.004 (Web Session Cookie) for MURKY PANDA cloud intrusions; T1486 (Data Encrypted for Impact) and T1657 (Financial Theft) for ransomware and DPRK operators; T1195.002 (Compromise Software Supply Chain), T1586/T1586.002 (Compromise Accounts, Email), T1114.002 (Remote Email Collection), and T1566 (Phishing) for initial access vectors across all three actor categories. T1090.003 (Proxy, Multi-hop Proxy) and T1583 (Acquire Infrastructure) reflect DPRK operational security patterns. Hands-on-keyboard intrusion volume increased 43% year-over-year globally per CrowdStrike telemetry, indicating greater adversary dwell time and interactive post-exploitation activity. MURKY PANDA specifically targeted Microsoft 365 environments via compromised third-party (trusted-relationship) access, consistent with T1199. AI-assisted tradecraft is reported across actor categories but specific tooling is not disclosed in available source data.

Action Checklist

1. Containment: Audit all third-party and vendor access to cloud environments (Microsoft 365, Azure AD/Entra ID, AWS, GCP) immediately. Revoke or suspend any third-party OAuth grants, service accounts, and delegated admin permissions that cannot be attributed to an active, documented business need. Prioritize review of accounts with mailbox access (relevant to MURKY PANDA T1114.002 remote email collection). Reference NIST AC-20 (Use of External Systems) and CIS 6.2 (Establish an Access Revoking Process).

2. Detection: Search Microsoft 365 audit logs and Azure AD sign-in logs for anomalous third-party application consent grants, OAuth token issuance from unfamiliar tenants, and mailbox access by non-owner accounts. For ransomware pre-staging, review EDR telemetry for T1059 (Command and Scripting Interpreter) execution chains, lateral movement from service accounts, and volume shadow copy deletion commands. For DPRK cryptocurrency targeting, monitor for T1574.001 (DLL Search Order Hijacking) indicators and outbound connections to newly registered domains. Enable Unified Audit Log in Microsoft 365 if not already active (NIST AU-2, AU-12; CIS 8.2). Cross-reference D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) for host-level detection.

3. Eradication: For confirmed MURKY PANDA-pattern intrusions: rotate all credentials (passwords, OAuth secrets, API keys) for affected cloud tenants; revoke and reissue certificates where applicable (D3-CRO, Credential Rotation; D3-CH, Credential Hardening). Remove unauthorized third-party application registrations from Azure AD/Entra ID. For ransomware exposure: isolate affected segments, rebuild from known-good images rather than decrypting where feasible, and remove attacker-deployed persistence mechanisms identified via T1574.001 and T1583 infrastructure review. Apply principle of least privilege to all service and application accounts (NIST AC-6; CIS 5.4).

4. Recovery: Validate that all revoked sessions and credentials cannot be reused (check for cached tokens, browser-stored session cookies per T1550.004). Confirm Microsoft 365 audit logging and SIEM ingestion are complete and continuous (NIST AU-9, AU-11; CIS 8.2). Re-enable services in isolated segments only after verifying clean-image rebuild. Monitor post-recovery environment for re-intrusion indicators; adversary re-entry within 30 days is consistent with hands-on-keyboard operator patterns. Validate MFA enforcement is active on all externally exposed applications and remote access paths (CIS 6.3, 6.4, 6.5; D3-MFA).

5. Post-Incident: Conduct a third-party access review against documented business justification for every external connection. Map control gaps against NIST AC-20, AC-17, and AC-5 (Separation of Duties); MURKY PANDA's use of trusted-relationship access (T1199) indicates over-permissioned vendor accounts as a structural gap. Review cryptocurrency custody and transfer authorization procedures if your

organization holds or transacts digital assets. Evaluate AI-assisted social engineering exposure by updating phishing simulation programs to include AI-generated lure content. Document findings and update incident response playbooks to include cloud-specific containment steps.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO, Legal, and external IR retainer if any of the following are confirmed: MailItemsAccessed UAL entries show non-owner access to executive or finance team mailboxes (potential MURKY PANDA exfiltration triggering GLBA or NY DFS 72-hour notification clock), ransomware staging artifacts (shadow copy deletion, lateral movement from service accounts) are detected in production financial systems, any unauthorized transfer or staging of digital assets is identified in cryptocurrency custody environments (DPRK pattern), or the third-party vendor identified as the initial access vector (T1199) serves multiple financial sector clients (indicating potential supply-chain incident requiring regulatory coordination).
Recovery Notes	Re-enable production financial services only after confirming that rebuilt images are cryptographically verified against known-good hashes stored offline, all Entra ID Conditional Access policies enforce MFA with no legacy authentication exceptions, and a 30-day post-recovery monitoring window is active with daily review of Entra ID risky sign-ins and Microsoft 365 UAL MailItemsAccessed events. Given that DPRK-nexus operators have demonstrated multi-month dwell times and hands-on-keyboard re-entry within 30 days of eviction, maintain heightened monitoring of outbound connections from trading platforms and cryptocurrency custody systems to newly registered domains for a minimum of 90 days post-recovery. Verify that all digital asset transfer authorization controls have been reviewed and hardened before restoring any cryptocurrency transaction capabilities, as DPRK actors will re-target the same organization if custody controls remain exploitable.
Forensic Artifacts	Microsoft 365 Unified Audit Log — MailItemsAccessed operations (Operation: MailItemsAccessed, LogonType: Delegate, ClientIPAddress outside corporate egress ranges): direct evidence of MURKY PANDA T1114.002 remote email collection via compromised third-party OAuth credentials. | Entra ID Audit Log — 'Consent to application' and 'Add OAuth2PermissionGrant' events with unfamiliar AppId values and cross-tenant initiating principals: primary artifact of MURKY PANDA trusted-relationship access (T1199) via compromised vendor tenant. | Sysmon Event ID 7 (Image Load) logs from cryptocurrency trading platform and wallet application host processes — unsigned DLLs loaded from user-writable paths (%APPDATA%, %TEMP%, application root directories): direct forensic evidence of DPRK T1574.001 DLL Search Order Hijacking targeting financial software. | Windows Security Event ID 4688 (Process Creation) sequence showing vssadmin.exe, wmic.exe, or bcdedit.exe spawned by a service account context within the same logon session: forensic evidence of ransomware operator pre-encryption staging following lateral movement from compromised financial services service accounts. | DNS query logs (Windows DNS debug log or Sysmon Event ID 22, DNS query) for domains with registration age under 30 days resolving from financial workstations or trading platform servers: evidence of DPRK C2 beaconing consistent with post-DLL-hijacking implant callback patterns observed in DPRK cryptocurrency targeting campaigns.

Per-Action IR Details

Containment — Audit all third-party and vendor access to cloud environments (Microsoft 365, Azure AD/Entra ID, AWS, GCP) immediately. Revoke or suspend any third-party OAuth grants, service accounts, and delegated admin permissions that cannot be attributed to an active, documented business need. Prioritize review of accounts with mailbox access (relevant to MURKY PANDA T1114.002 remote email collection). Reference NIST AC-20 (Use of External Systems) and CIS 6.2 (Establish an Access Revoking Process).

NIST Phase: Containment

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

Controls: NIST AC-20 (Use of External Systems), NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), CIS 6.2 (Establish an Access Revoking Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Run the following Microsoft Graph PowerShell command to enumerate all OAuth app consent grants in Entra ID: `Get-MgOauth2PermissionGrant -All | Select ClientId, ConsentType, PrincipalId, Scope | Export-Csv oauth_grants.csv`. Cross-reference ClientId values against your documented vendor list. For service accounts with mailbox access, run: `Get-MailboxPermission -Identity * | Where-Object {$_.AccessRights -eq 'FullAccess' -and $_.IsInherited -eq $false} | Export-Csv mailbox_perms.csv`. Revoke unrecognized grants immediately via `Remove-MgOauth2PermissionGrant -OAuth2PermissionGrantId `.

Evidence: Before revoking, export the full Entra ID audit log for the past 90 days filtering on 'Consent to application' and 'Add OAuth2PermissionGrant' operations — these are the exact log events MURKY PANDA's trusted-relationship access (T1199) and OAuth abuse would generate. Capture Microsoft 365 Unified Audit Log entries for MailItemsAccessed operations (Operation: MailItemsAccessed, LogonType: Delegate or Owner with non-owner ClientIPAddress) which directly evidence T1114.002 remote mailbox collection. Preserve Azure AD sign-in logs for all service principal authentications in the 30 days prior to discovery — MURKY PANDA lateral movement through compromised third-party tenants will appear as cross-tenant sign-ins with unfamiliar AppId values.

Detection — Search Microsoft 365 audit logs and Azure AD sign-in logs for anomalous third-party application consent grants, OAuth token issuance from unfamiliar tenants, and mailbox access by non-owner accounts. For ransomware pre-staging, review EDR telemetry for T1059 (Command and Scripting Interpreter) execution chains, lateral movement from service accounts, and volume shadow copy deletion commands. For DPRK cryptocurrency targeting, monitor for T1574.001 (DLL Search Order Hijacking) indicators and outbound connections to newly registered domains. Enable Unified Audit Log in Microsoft 365 if not already active (NIST AU-2, AU-12; CIS 8.2). Cross-reference D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) for host-level detection.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For Microsoft 365 without a SIEM: use the free Microsoft 365 Compliance Center Audit search (or PowerShell `Search-UnifiedAuditLog`) to query for `Operations: MailItemsAccessed,FileAccessed,ConsentToApplication` over the past 90 days. For ransomware pre-staging detection without EDR: deploy Sysmon with SwiftOnSecurity config and query Event ID 4688 (Process Creation) for `vssadmin.exe delete shadows`, `wmic shadowcopy delete`, and `cmd.exe /c bcdedit /set {default} recoveryenabled No` spawned from service account contexts. For DPRK DLL hijacking (T1574.001): use Sysmon Event ID 7 (Image Load) to identify unsigned DLLs loaded from user-writable paths (e.g., `%APPDATA%`, `%TEMP%`) by financial application processes such as trading platforms or crypto wallet software. Use the free Sigma rule `proc_creation_win_vssadmin_delete_shadows.yml` against collected Sysmon logs.

Evidence: Capture Entra ID sign-in logs filtering on `Cross-tenant access type: B2B collaboration` and `Risk state: atRisk` — MURKY PANDA's use of compromised third-party vendor accounts produces exactly these log characteristics. Export Microsoft 365 Unified Audit Log for `ClientAppUsed: Other clients` and `AuthenticationRequirement: multiFactorAuthentication` failures — OAuth token issuance from unfamiliar tenants

bypassing MFA is a MURKY PANDA TTI. For ransomware pre-staging, capture Windows Security Event ID 4672 (Special Privileges Assigned) for service accounts followed within minutes by Event ID 4688 showing `net.exe` or `wmic.exe` child processes — this sequence indicates lateral movement from service account compromise preceding encryption. For DPRK cryptocurrency targeting, capture DNS query logs (Windows DNS debug log or Sysmon Event ID 22) for domains registered within the past 30 days resolving to DPRK-associated ASNs, and collect process memory dumps of any crypto wallet or trading application processes showing anomalous DLL load sequences.

Eradication — For confirmed MURKY PANDA-pattern intrusions: rotate all credentials (passwords, OAuth secrets, API keys) for affected cloud tenants; revoke and reissue certificates where applicable (D3-CRO — Credential Rotation; D3-CH — Credential Hardening). Remove unauthorized third-party application registrations from Azure AD/Entra ID. For ransomware exposure: isolate affected segments, rebuild from known-good images rather than decrypting where feasible, and remove attacker-deployed persistence mechanisms identified via T1574.001 and T1583 infrastructure review. Apply principle of least privilege to all service and application accounts (NIST AC-6; CIS 5.4).

NIST Phase: Eradication

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

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), NIST CM-7 (Least Functionality), NIST IA-5 (Authenticator Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: Enumerate and remove unauthorized Entra ID application registrations using: `Get-MgApplication -All | Where-Object {$_.CreatedDateTime -gt (Get-Date).AddDays(-90)} | Select DisplayName, AppId, CreatedDateTime | Export-Csv new_app_registrations.csv` — flag any registrations not matching your change management records. Revoke all refresh tokens for affected accounts with: `Revoke-MgUserSignInSession -UserId ` (requires Microsoft.Graph.Users module). For DLL hijacking persistence cleanup (T1574.001): use Sysinternals Autoruns with the VirusTotal integration enabled to identify and remove unsigned DLLs in application directories of crypto/trading software. For ransomware persistence mechanisms, query Sysmon Event ID 13 (Registry Value Set) for modifications to `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options` and `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` made by the ransomware staging process.

Evidence: Before credential rotation, forensically image Entra ID application registration details including `KeyCredentials` and `PasswordCredentials` arrays for all third-party apps — MURKY PANDA persistence via compromised OAuth client secrets will appear here. Capture the full list of Conditional Access policy modifications from Entra ID audit logs (Operation: `Update conditional access policy`) in the 90 days prior to discovery — adversaries frequently disable MFA requirements or add trusted location exclusions as a persistence enabler. For T1574.001 cleanup, collect file system metadata (creation/modification timestamps via `fsutil file queryextents` and `Get-Item -Path | Select LastWriteTime, CreationTime`) for all flagged DLLs before removal to preserve forensic chain of custody. For ransomware, document all identified T1583 adversary infrastructure (C2 domains and IPs from DNS/proxy logs) before eradicating beaconing malware, as this data supports downstream threat intelligence sharing under NIST 800-61r3 §4 post-incident activities.

Recovery — Validate that all revoked sessions and credentials cannot be reused (check for cached tokens, browser-stored session cookies per T1550.004). Confirm Microsoft 365 audit logging and SIEM ingestion are complete and continuous (NIST AU-9, AU-11; CIS 8.2). Re-enable services in isolated segments only after verifying clean-image rebuild. Monitor post-recovery environment for re-intrusion indicators — adversary re-entry within 30 days is consistent with hands-on-keyboard operator patterns. Validate MFA enforcement is active on all externally exposed applications and remote access paths (CIS 6.3, 6.4, 6.5; D3-MFA).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), NIST AC-12 (Session Termination), NIST AC-7 (Unsuccessful Logon Attempts), CIS 8.2 (Collect Audit Logs), 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: Validate session token invalidation by checking Entra ID sign-in logs for any successful authentications using `tokenIssuedAt` timestamps predating your revocation window — use PowerShell: `Get-MgAuditLogSignIn -Filter "createdDateTime ge " | Where-Object {$_.AuthenticationDetails.authenticationMethod -eq 'Previously satisfied'}`. For cached Kerberos/NTLM tokens (T1550.004) on rebuilt Windows endpoints, run `klist purge` post-rebuild and verify with `klist` that no residual tickets exist. Confirm UAL ingestion completeness by running `Search-UnifiedAuditLog -StartDate -EndDate -RecordType AzureActiveDirectory -ResultSize 1` — a null result indicates a logging gap requiring immediate investigation. Deploy a free Sigma rule (`azure_ad_mfa_bypass_attempt.yml`) against Entra ID logs to catch re-entry attempts using legacy authentication protocols that bypass MFA, which is a known MURKY PANDA TTI.

Evidence: Before re-enabling isolated segments, snapshot the current state of all Windows Event logs on rebuilt systems (Security, System, Application) using `wevtutil epl Security C:\forensics\Security_prerecovery.evtx` to establish a clean baseline for detecting post-recovery re-intrusion. Capture baseline Entra ID Conditional Access policy state and export all Named Locations and Trusted IP configurations — re-intrusion by MURKY PANDA or affiliated actors frequently begins with policy tampering to re-establish persistence before operational activity resumes. For post-recovery monitoring of DPRK re-entry patterns, establish a 30-day watchlist in your DNS logs for any re-resolution of previously identified C2 domains or newly registered lookalike domains targeting your cryptocurrency custody or trading platform hostnames.

Post-Incident — Conduct a third-party access review against documented business justification for every external connection. Map control gaps against NIST AC-20, AC-17, and AC-5 (Separation of Duties) — MURKY PANDA's use of trusted-relationship access (T1199) indicates over-permissioned vendor accounts as a structural gap. Review cryptocurrency custody and transfer authorization procedures if your organization holds or transacts digital assets. Evaluate AI-assisted social engineering exposure by updating phishing simulation programs to include AI-generated lure content. Document findings and update incident response playbooks to include cloud-specific containment steps.

NIST Phase: Post Incident

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

Controls: NIST AC-20 (Use of External Systems), NIST AC-17 (Remote Access), NIST AC-5 (Separation of Duties), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Produce a third-party access register using the exported `oauth_grants.csv` and `mailbox_perms.csv` from the containment phase — map each entry against your vendor contracts and documented integration requirements; any unmatched entry is a structural gap requiring AC-5 separation of duties remediation. For cryptocurrency custody procedure review without a commercial DLP tool: implement a manual four-eyes authorization workflow (two-person approval documented in a change log) for any digital asset transfer above your organization's defined threshold, aligning with DPRK targeting patterns that focus on large single-transaction exfiltration. For AI-generated phishing simulation, use free GoPhish with prompts crafted to mimic the AI-generated financial sector lures described in the CrowdStrike 2026 report — test specifically for impersonation of your known vendor contacts, as MURKY PANDA's trusted-relationship initial access relies on vendor identity spoofing.

Evidence: Compile a final forensic timeline from the Entra ID audit logs, Microsoft 365 UAL, and Sysmon telemetry collected throughout the incident to establish the full attacker dwell time — CrowdStrike reporting indicates China-nexus operators maintain persistent access for months before detection, so your timeline should extend 90-180 days prior to the first indicator. Preserve all collected OAuth grant exports, sign-in anomaly reports, and DLL forensic images in an evidence package for regulatory disclosure readiness — financial sector incidents involving cloud environment compromise and potential PII exfiltration via T1114.002 mailbox collection trigger breach notification obligations under GLBA, NY DFS 23 NYCRR 500, and applicable state laws. Document the specific MURKY PANDA TTPs observed (T1199, T1114.002, cross-tenant OAuth abuse) and contribute sanitized IOCs to FS-ISAC to support sector-wide threat intelligence sharing per NIST 800-61r3 §4 post-incident recommendations.

Detection Guidance

Three detection tracks apply, corresponding to the three threat categories in the report. Track 1, MURKY PANDA (cloud espionage): Query Microsoft 365 Unified Audit Log for MailItemsAccessed operations by non-owner service principals; alert on OAuth application consent grants issued outside change-management windows; monitor Azure AD Entra ID for impossible-travel sign-in events from third-party tenant IDs. Relevant MITRE techniques: T1114.002, T1550.004, T1199. D3FEND countermeasure: D3-LAM (Local Account Monitoring), D3-ACA (Active Certificate Analysis for anomalous service principal certificates). Track 2, BGH Ransomware: Alert on bulk file rename operations, shadow copy deletion (vssadmin.exe delete shadows), and WMI/PowerShell execution from service accounts (T1059, T1486). Monitor for data staging to unusual outbound destinations prior to encryption events. Review EDR process trees for living-off-the-land binaries (LOLBins) executing from user-writable paths (T1574.001). Track 3, DPRK cryptocurrency theft: Monitor for process injection into browser or wallet application processes; alert on unexpected outbound connections from financial application servers to newly registered or low-reputation domains (T1090.003); review code-signing anomalies in software update paths (T1195.002). Across all tracks: enforce NIST AU-6 (Audit Record Review, Analysis, and Reporting) with automated correlation, and validate that AU-8 (Time Stamps) is synchronized across all log sources to support timeline reconstruction. Source: CrowdStrike 2026 Financial Services Threat Landscape Report (vendor threat intelligence; recommended human verification before operationalizing specific detection thresholds in production environments).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-financial-services-threat-landscape-report/`	Primary source — CrowdStrike 2026 Financial Services Threat Landscape Report. Verify this URL resolves before operationalizing; labeled as search-retrieved, human validation recommended.	MEDIUM
URL	`https://www.crowdstrike.com/en-us/blog/murky-panda-trusted-relationship-threat-in-cloud/`	CrowdStrike blog post on MURKY PANDA trusted-relationship cloud intrusion campaign. Verify this URL resolves before operationalizing; labeled as search-retrieved, human validation recommended.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1574.001** — DLL
- **T1199** — Trusted Relationship
- **T1090.003** — Multi-hop Proxy
- **T1586** — Compromise Accounts

- **T1586.002** — Email Accounts
- **T1059** — Command and Scripting Interpreter
- **T1486** — Data Encrypted for Impact
- **T1657** — Financial Theft
- **T1588** — Obtain Capabilities
- **T1583** — Acquire Infrastructure
- **T1550.004** — Web Session Cookie
- **T1078** — Valid Accounts
- **T1195.002** — Compromise Software Supply Chain
- **T1114.002** — Remote Email Collection
- **T1566** — Phishing

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
- **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-3** — Supply Chain Controls and Processes
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication 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

- **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)(6)(ii)** — Response and Reporting

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1574.001	DLL	Persistence
T1199	Trusted Relationship	Initial-Access
T1090.003	Multi-hop Proxy	Command-And-Control
T1586	Compromise Accounts	Resource-Development
T1586.002	Email Accounts	Resource-Development
T1059	Command and Scripting Interpreter	Execution
T1486	Data Encrypted for Impact	Impact
T1657	Financial Theft	Impact
T1588	Obtain Capabilities	Resource-Development
T1583	Acquire Infrastructure	Resource-Development
T1550.004	Web Session Cookie	Defense-Evasion

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access
T1114.002	Remote Email Collection	Collection
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/how-to-mature-your-threat-in...	T3
	https://www.crowdstrike.com/en-us/blog/3-ways-small-businesses-big-...	T3
MURKY PANDA: Trusted-Relationship Cloud Threat | CrowdStrike	https://www.crowdstrike.com/en-us/blog/murky-panda-trusted-relation...	T3

Generated 2026-05-26 06:08 UTC by TJS Security Command Center