INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 06:45 UTC

Identity Hijacking at Scale: Attackers Weaponize MFA, Help-Desk Processes, and Legitimate Infrastructure in 2025-2026 Campaigns

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0197
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft 365 (Direct Send feature), Cisco Duo, IAM platforms (generic), enterprise help-desk workflows
Published	2026-04-21T12:00:08+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Throughout 2025 and into early 2026, threat actors shifted from stealing credentials to fully hijacking employee identities by exploiting help-desk trust, resetting MFA factors, and registering attacker-controlled devices under legitimate accounts. Microsoft 365 Direct Send misconfigurations allowed spoofed internal email to bypass filtering, enabling social engineering at scale against finance and payroll workflows. Organizations face direct financial loss through fraudulent wire transfers and payroll redirection, compounded by prolonged attacker persistence via legitimate remote management tools that evade standard detection.

Technical Analysis

This campaign cluster exploits organizational trust mechanisms across a multi-stage identity compromise chain. Initial access relied on spear-phishing (T1566.001, T1566.002), accounting for approximately 40% of incidents per source reporting. Attackers exploited Microsoft 365 Direct Send misconfigurations to send spoofed internal email that bypasses standard mail filtering, enabling convincing impersonation of internal senders. MFA bypass techniques included MFA fatigue attacks against push-based systems (T1621) and SIM-swapping, with Cisco Duo deployments specifically identified as targeted. Post-authentication, attackers reset MFA factors (T1556, T1556.006) and registered attacker-controlled devices to legitimate identities (T1098.005), establishing durable footholds. Lateral movement used legitimate RMM tools (T1219) and living-off-the-land binaries (T1218) to blend with normal IT operations, defeating behavioral baselines. Financial fraud was executed by impersonating

employees to help-desk staff to redirect payroll and wire transfers (T1534). Relevant CWEs include CWE-287 (improper authentication), CWE-306 (missing authentication for critical function), CWE-940 (improper verification of source of communication channel), CWE-1390 (weak authentication), and CWE-522 (insufficiently protected credentials). Threat actors associated with similar identity hijacking campaigns include groups tracked as MuddyWater, OilRig, APT33, Agrius, CyberAv3ngers, and affiliated clusters; specific attribution of this 2025-2026 activity cluster requires verification against primary threat intelligence sources. No CVE identifier applies; the attack surface is misconfiguration and process exploitation, not a patchable software vulnerability. Sources: Microsoft Security Blog (January 2026, T1), Cisco Talos Blog (T3), The Register (February 2026, T3), WeLiveSecurity (T3).

Action Checklist

1. Containment: Audit Microsoft 365 Direct Send connectors immediately - disable or restrict any connector not explicitly required for business operations.
2. Containment: Enforce Sender Policy Framework (SPF) on all domains.
3. Containment: Deploy DomainKeys Identified Mail (DKIM) on all domains.
4. Containment: Configure DMARC with reject policy on all domains.
5. Containment: Block unauthenticated SMTP relay from internal IP ranges.
6. Containment: Review Cisco Duo policies to disable push-based MFA where possible and enforce number-matching or phishing-resistant MFA (FIDO2/hardware tokens) per CISA guidance on MFA phishing resistance.
7. Detection: Query Azure AD / Entra ID audit logs for MFA factor resets not initiated by the account owner.
8. Detection: Flag new device registrations against existing identities within 24 hours of a help-desk interaction.
9. Detection: Alert on RMM tool installations (AnyDesk, TeamViewer, ScreenConnect) outside approved software inventory.
10. Detection: Review M365 message trace logs for mail sent via Direct Send connectors with mismatched From/Return-Path headers.
11. Detection: Monitor for after-hours payroll or wire transfer change requests submitted via email.
12. Eradication: Remove unauthorized registered devices from all identities in Entra ID / Active Directory.
13. Eradication: Revoke and reissue MFA factors for any account where a reset cannot be verified as user-initiated.
14. Eradication: Disable or reconfigure M365 Direct Send connectors per Microsoft's January 2026 guidance (see Microsoft Security Blog source).
15. Eradication: Uninstall unauthorized RMM tools and block their network endpoints at the perimeter and via application control policy.
16. Recovery: Validate MFA enrollment for all privileged accounts and accounts with access to financial systems.
17. Recovery: Confirm payroll and wire transfer destination accounts against records predating the incident window.
18. Recovery: Re-baseline behavioral analytics with RMM tool usage now explicitly tracked.

19. Recovery: Require out-of-band (phone, in-person) verification for any future MFA reset or financial account change request.

20. Post-Incident: Conduct a tabletop exercise specifically against help-desk social engineering scenarios.

21. Post-Incident: Implement a formal identity verification protocol for help-desk MFA resets - require manager approval plus secondary verification before any MFA factor change.

22. Post-Incident: Map your MFA deployment against CISA's phishing-resistant MFA guidance and establish a migration timeline away from push-based SMS or app-push factors for privileged and finance roles.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and financial institution contacts immediately if Entra ID audit logs confirm any MFA factor was successfully reset and a new device registered under a finance or payroll role, or if M365 message trace confirms a wire transfer or payroll change request was sent via a Direct Send connector — both conditions indicate confirmed identity hijacking with probable financial fraud, triggering breach notification assessment under applicable state laws and potential GLBA or SOX obligations.
Recovery Notes	After eradication, maintain elevated monitoring of Entra ID Identity Protection (Risky Sign-Ins and Risky Users blades) for a minimum of 30 days, as threat actors in this campaign have demonstrated persistence by pre-staging secondary device registrations or shadow accounts during the initial access window. Validate all payroll and ACH destination account numbers against records from 90 days prior to the incident and obtain written confirmation from your financial institution that no unauthorized transactions were processed. Re-run the MFA enrollment audit weekly for the first month post-recovery, specifically targeting finance, HR, payroll, and privileged IT roles, as these were the primary targets of help-desk social engineering in the 2025–2026 campaign activity.
Forensic Artifacts	Entra ID Unified Audit Log — filter ActivityType 'Update StrongAuthenticationMethod' and 'Register device' where InitiatedBy actor differs from TargetResource UPN; these entries document each attacker-executed MFA reset and device registration with timestamp, source IP, and actor identity | M365 Message Trace and Exchange Online mail headers — specifically the X-MS-Exchange-Organization-SCL, Return-Path, and Authentication-Results headers from messages transiting Direct Send connectors; mismatched From/Return-Path and 'dmarc=fail' in Authentication-Results confirm spoofed internal sender identity | Cisco Duo Administrator Audit Log and Authentication Log — filter for 'factor_changed', 'enrollment', and 'bypass_created' events correlated against help-desk ticket timestamps; push approval events from unexpected geolocations or new device IDs indicate attacker-controlled factor usage | Sysmon Event ID 1 (Process Create) logs on endpoints where RMM tools were installed — parent/child process chain showing how AnyDesk, TeamViewer, or ScreenConnect was launched (e.g., spawned by a browser or email client process confirms social engineering delivery), plus Event ID 3 (Network Connection) showing outbound relay connections to RMM infrastructure | Entra ID Registered Devices list export and Azure AD Sign-In Logs — cross-correlate DeviceId, enrollmentType 'azureADRegistered', operatingSystem, and approximateLastSignInDateTime against the help-desk interaction window; attacker-registered devices will show a short first-seen to first-used delta and often source from VPN exit nodes or residential proxy IP ranges inconsistent with the legitimate user's historical sign-in geography

Per-Action IR Details

Containment — Audit Microsoft 365 Direct Send connectors immediately: disable or restrict any connector not explicitly required for business operations, enforce sender policy framework (SPF), DomainKeys Identified Mail (DKIM), and DMARC with reject policy on all domains, and block unauthenticated SMTP relay from internal IP ranges. Review Cisco Duo policies to disable push-based MFA where possible and enforce number-matching or phishing-resistant MFA (FIDO2/hardware tokens) per CISA guidance on MFA phishing resistance.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-8 (Transmission Confidentiality and Integrity), NIST SI-10 (Information Input Validation), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Use the Microsoft 365 Admin Center > Settings > Mail Flow > Connectors to enumerate all Direct Send connectors and export via PowerShell: 'Get-InboundConnector | Select Name,ConnectorType,SenderIPAddresses,Enabled | Export-Csv connectors.csv'. For SPF/DKIM/DMARC validation without a paid tool, query current DNS records with 'Resolve-DnsName -Type TXT -Name yourdomain.com' and cross-check against MXToolbox (free tier). For Duo, navigate to Duo Admin Panel > Policies > Global Policy and set 'Require number matching' — no license upgrade required for push policy changes on existing Duo deployments.

Evidence: Before modifying any connector, export the full M365 connector configuration including SenderIPAddresses, SmartHosts, and TLSSettings via 'Get-InboundConnector | ConvertTo-Json | Out-File inbound_connectors_evidence.json' and 'Get-OutboundConnector | ConvertTo-Json | Out-File outbound_connectors_evidence.json'. Capture current DMARC/SPF/DKIM DNS records as a timestamped snapshot. Preserve Cisco Duo Admin Panel authentication logs showing all push approvals and denials for the 30 days preceding discovery, specifically filtering for accounts whose MFA factors were reset within 24 hours of a help-desk ticket.

Detection — Query Azure AD / Entra ID audit logs for MFA factor resets not initiated by the account owner, new device registrations against existing identities within 24 hours of a help-desk interaction, and RMM tool installations (AnyDesk, TeamViewer, ScreenConnect) outside approved software inventory. Review M365 message trace logs for mail sent via Direct Send connectors with mismatched From/Return-Path headers. Monitor for after-hours payroll or wire transfer change requests submitted via email.

NIST Phase: Detection Analysis

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

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

Compensating: Query Entra ID audit logs directly via Microsoft Graph API or the free Entra ID portal: filter 'AuditLogs > DirectoryLogs' for ActivityType 'Update user' and 'Update StrongAuthenticationMethod' where InitiatedBy actor UPN does not match TargetResource UPN — this isolates admin-initiated or help-desk-initiated MFA resets. For device registrations, run: 'Get-MgAuditLogDirectoryAudit -Filter "activityDisplayName eq \'Register device\'" | Where-Object { $_.InitiatedBy.User.UserPrincipalName -ne $_.TargetResources[0].UserPrincipalName }'. For RMM detection on endpoints without EDR, deploy Sysmon with the SwiftOnSecurity config and query Event ID 1 (Process Create) for anydesk.exe, TeamViewer.exe, ScreenConnect.ClientService.exe. Use the free Sigma rule 'proc_creation_win_anydesk_execution.yml' from the SigmaHQ repository to parse Sysmon logs via grep or PowerShell.

Evidence: Preserve Entra ID Sign-In Logs and Audit Logs for the full 30-day retention window immediately — these are overwritten and cannot be recovered after the retention period expires. Specifically capture: (1) Entra ID Audit Log entries for 'Reset user password' and 'Update user' filtered on StrongAuthenticationMethod changes, noting InitiatedBy actor, timestamp, and IP; (2) M365 Message Trace export (Admin Center > Exchange > Mail Flow > Message Trace) for all messages transiting Direct Send connectors, filtering for From/Return-Path header mismatch which indicates spoofed sender; (3) Entra ID 'Registered Device' audit entries cross-correlated against help-desk ticketing system

timestamps; (4) Duo authentication logs showing the specific accounts that received and approved push notifications, with source IP geolocation.

Eradication — Remove unauthorized registered devices from all identities in Entra ID / Active Directory. Revoke and reissue MFA factors for any account where a reset cannot be verified as user-initiated. Disable or reconfigure M365 Direct Send connectors per Microsoft's January 2026 guidance (see Microsoft Security Blog source). Uninstall unauthorized RMM tools and block their network endpoints at the perimeter and via application control policy.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-2 (Baseline Configuration), CIS 2.3 (Address Unauthorized Software), CIS 5.3 (Disable Dormant Accounts), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Remove unauthorized Entra ID devices via: 'Get-MgDevice | Where-Object { $_.ApproximateLastSignInDateTime -eq $null -or (conditions) } | Remove-MgDevice'. Revoke all active sessions and MFA tokens for compromised accounts: 'Revoke-MgUserSignInSession -UserId upn@domain.com' followed by 'Update-MgUser -UserId upn@domain.com -AccountEnabled:$false' then re-enable after MFA re-enrollment via verified out-of-band call. Block AnyDesk, TeamViewer, and ScreenConnect relay endpoints using Windows Firewall GPO targeting known relay IP ranges (AnyDesk: relay.anydesk.com; ScreenConnect: instance-specific cloud URLs). For application control without a paid solution, use Windows Defender Application Control (WDAC) policy in audit mode first, then enforce to block unsigned RMM binaries.

Evidence: Before removing any device registration, capture the full device object including deviceId, displayName, enrollmentType, operatingSystem, registeredOwner, and approximateLastSignInDateTime via 'Get-MgDevice -DeviceId | ConvertTo-Json'. Before revoking MFA factors, export the account's current authentication methods via 'Get-MgUserAuthenticationMethod -UserId upn@domain.com | ConvertTo-Json' as this documents the attacker-registered factor for later forensic and legal review. On endpoints where RMM tools were installed, collect Sysmon Event ID 11 (File Create) and Event ID 13 (Registry Value Set) artifacts showing installation path, parent process, and any persistence mechanism (e.g., HKLM\SYSTEM\CurrentControlSet\Services entries for ScreenConnect.ClientService).

Recovery — Validate MFA enrollment for all privileged accounts and accounts with access to financial systems. Confirm payroll and wire transfer destination accounts against records predating the incident window. Re-baseline behavioral analytics with RMM tool usage now explicitly tracked. Require out-of-band (phone, in-person) verification for any future MFA reset or financial account change request.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST IA-5 (Authenticator Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Validate MFA enrollment state for all privileged and finance-role accounts using: 'Get-MgUserAuthenticationMethod -UserId upn@domain.com' — confirm only FIDO2 or Microsoft Authenticator (with number-match) entries exist; flag any phone/SMS entries on privileged accounts for immediate re-enrollment. For payroll destination validation, pull ACH/wire change records from your HR system and cross-reference against banking records using the oldest available pre-incident export — this is a manual reconciliation step requiring finance team involvement. Establish a free osquery scheduled query to detect AnyDesk, TeamViewer, and ScreenConnect process execution going forward: query 'processes' table for name LIKE '%anydesk%' OR '%screenconnect%' and alert on any match outside approved asset list.

Evidence: Before re-enabling any previously compromised account, verify that Entra ID Sign-In Risk is cleared (Identity Protection blade > Risky Users) and document the risk dismissal with analyst justification. Capture a post-eradication snapshot of all registered MFA methods across privileged accounts as a recovery baseline. Review

M365 mailbox audit logs (via 'Search-UnifiedAuditLog -Operations SendAs,SendOnBehalf,MailItemsAccessed' filtered to compromised accounts) to identify any payroll or finance emails sent by the attacker during the dwell period — these are required evidence for any financial fraud claim or regulatory notification.

Post-Incident — Conduct a tabletop exercise specifically against help-desk social engineering scenarios. Implement a formal identity verification protocol for help-desk MFA resets: require manager approval plus secondary verification before any MFA factor change. Map your MFA deployment against CISA's phishing-resistant MFA guidance and establish a migration timeline away from push-based SMS or app-push factors for privileged and finance roles.

NIST Phase: Post Incident

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

Controls: NIST IR-3 (Incident Response Testing), NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST IA-5 (Authenticator Management), CIS 5.2 (Use Unique Passwords), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Tabletop scenario should walk help-desk staff through a scripted caller posing as a remote employee claiming a locked account and lost phone — include a deepfake voice or spoofed callback number variant to reflect 2025–2026 attacker TTPs. For the identity verification protocol, implement a Jira or ServiceNow (free tier) workflow that requires a ticket field 'Manager Approval UPN' to be populated and auto-emails the manager before any MFA reset ticket can be closed. For CISA phishing-resistant MFA gap analysis, use CISA's published 'Phishing-Resistant MFA Fact Sheet' (cisa.gov) as the scoring rubric and document current Duo push or SMS usage against each privileged role — this gap register becomes the migration roadmap.

Evidence: The lessons-learned report must include: (1) a timeline correlating help-desk ticket timestamps with Entra ID MFA reset audit events to document attacker dwell time; (2) the full list of Entra ID devices registered by the attacker with registration timestamps and source IPs; (3) M365 message trace evidence of Direct Send connector abuse including spoofed From headers and targeted recipient roles (finance, payroll, HR); and (4) Duo authentication logs showing which push-based approvals were fraudulently granted. This evidence package supports both internal process improvement and potential regulatory notification obligations under state breach notification laws if PII or financial account data was accessed.

Detection Guidance

Key detection signals across log sources: (1) Entra ID / Azure AD Sign-In Logs - flag authentication events where MFA method changed within the same session or within 24 hours of a new device registration; look for device compliance state 'Unknown' on newly registered devices. (2) M365 Message Trace - filter for messages delivered via Send Connector where the From domain matches your internal domain; cross-reference sending IP against your published SPF record to identify IPs not in your authorized range. Inspect message headers for mismatched From/Return-Path. (3) Endpoint and RMM logs - alert on installation or execution of AnyDesk, TeamViewer, ScreenConnect, or similar RMM binaries (MITRE T1219) where the process parent is a user-interactive shell rather than an approved deployment system. (4) HR/Payroll system audit logs - flag any direct deposit or payment destination change submitted within 48 hours of a help-desk ticket for account recovery or MFA reset on the same identity. (5) Help-desk ticket correlation - cross-reference MFA reset tickets against subsequent authentication anomalies (new device, new geo, new IP) on the same account within 72 hours. Behavioral indicator: a low-suspicion event chain of phishing email received, help-desk contact, MFA reset, new device registration, and RMM tool launch on the same identity within a short window is the primary detection signature for this campaign pattern.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Direct Send connector abuse via internal SMTP relay — no specific IP/domain IOC published`	M365 Direct Send misconfigurations used to send spoofed internal email; detection relies on mail header analysis rather than static IOCs	LOW

Framework Mappings

MITRE-ATTACK

- **T1484** — Domain or Tenant Policy Modification
- **T1199** — Trusted Relationship
- **T1621** — Multi-Factor Authentication Request Generation
- **T1485** — Data Destruction
- **T1078** — Valid Accounts
- **T1590** — Gather Victim Network Information
- **T1566.001** — Spearphishing Attachment
- **T1566.002** — Spearphishing Link
- **T1531** — Account Access Removal
- **T1021.001** — Remote Desktop Protocol
- **T1556** — Modify Authentication Process
- **T1218** — System Binary Proxy Execution
- **T1534** — Internal Spearphishing
- **T1650** — Acquire Access
- **T1219** — Remote Access Tools
- **T1556.006** — Multi-Factor Authentication
- **T1098.005** — Device Registration
- **T1195** — Supply Chain Compromise
- **T1566** — Phishing
- **T1195.002** — Compromise Software Supply Chain

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **CA-7** — Continuous Monitoring
- **CM-7** — Least Functionality
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design

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
- **5.2** — Use Unique Passwords
- **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
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1484	Domain or Tenant Policy Modification	Defense-Evasion

Technique ID	Technique Name	Tactic
T1199	Trusted Relationship	Initial-Access
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1485	Data Destruction	Impact
T1078	Valid Accounts	Defense-Evasion
T1590	Gather Victim Network Information	Reconnaissance
T1566.001	Spearphishing Attachment	Initial-Access
T1566.002	Spearphishing Link	Initial-Access
T1531	Account Access Removal	Impact
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1556	Modify Authentication Process	Credential-Access
T1218	System Binary Proxy Execution	Defense-Evasion
T1534	Internal Spearphishing	Lateral-Movement
T1650	Acquire Access	Resource-Development
T1219	Remote Access Tools	Command-And-Control
T1556.006	Multi-Factor Authentication	Credential-Access
T1098.005	Device Registration	Persistence
T1195	Supply Chain Compromise	Initial-Access
T1566	Phishing	Initial-Access
T1195.002	Compromise Software Supply Chain	Initial-Access

Sources

Source	URL	Tier
Cisco Talos Blog	https://blog.talosintelligence.com/phishing-and-mfa-exploitation-ta...	T3
	https://www.welivesecurity.com/en/business-security/cyber-fallout-i...	T3
	https://www.theregister.com/2026/02/11/payroll_pirates_business_soc...	T3
	https://www.cpomagazine.com/cyber-security/supply-chain-attack-infe...	T3

Source	URL	Tier
Phishing actors exploit complex routing and misconfigurations to ...	https://www.microsoft.com/en-us/security/blog/2026/01/06/phishing-a...	T1

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-22 06:45 UTC by TJS Security Command Center