INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-02 06:45 UTC

Vishing-Powered SSO Hijacking: Two Threat Clusters Drain SaaS Environments in Under an Hour

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0258
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Google Workspace, Microsoft SharePoint, HubSpot, Salesforce, Identity Providers (IdP/SSO platforms)
Published	2026-05-01T10:26:00
Discovery Source	Rss

Executive Summary

Two financially motivated cybercrime groups are actively combining phone-based social engineering with session-hijacking infrastructure to compromise corporate identity providers and drain connected SaaS environments, including Google Workspace, Microsoft SharePoint, HubSpot, and Salesforce, within a single authenticated session. Attackers bypass multi-factor authentication entirely by stealing live session tokens, not passwords, leaving minimal forensic evidence because no malware touches endpoints. Organizations relying on traditional endpoint and network controls are effectively blind to this attack; data exfiltration can begin in under 60 minutes from first contact with an employee.

Technical Analysis

Financially motivated cybercrime groups conduct SaaS-focused extortion campaigns using a combined vishing and adversary-in-the-middle (AiTM) phishing chain. Attack flow: (1) Attacker calls a target employee impersonating IT support (T1656, Impersonation, T1566.004, Spearphishing Voice); (2) victim is directed to an AiTM reverse-proxy phishing page that transparently proxies authentication to the legitimate IdP, capturing both credentials and live session cookies (T1621, MFA Request Generation, T1539, Steal Web Session Cookie, T1550.001, Application Access Token); (3) the captured session token authenticates the attacker directly to the IdP, bypassing MFA entirely; (4) the attacker pivots laterally across federated SaaS platforms within that single SSO session (T1534, Internal Spearphishing, T1199, Trusted Relationship, T1078/T1078.004, Valid Accounts: Cloud Accounts); (5) data is exfiltrated via SaaS-native channels (T1567, Exfiltration Over Web Service, T1048,

Exfiltration Over Alternative Protocol, T1114.003, Email Forwarding Rule, T1530, Data from Cloud Storage). No malware is deployed; no endpoint execution occurs. Attackers have been observed completing exfiltration in under 60 minutes. Relevant CWEs: CWE-287 (Improper Authentication), CWE-308 (Use of Single-Factor Authentication), CWE-522 (Insufficiently Protected Credentials), CWE-1390 (Weak Authentication). No CVE applies; this is a technique-based campaign, not a software vulnerability. Patch status: not applicable; mitigations are architectural and procedural.

Action Checklist

1. **Containment (Immediate):** Audit active SSO/IdP sessions across Google Workspace, Microsoft Entra ID, Okta, and Ping Identity for anomalous sign-in locations, impossible travel, or session age inconsistencies; revoke suspicious sessions and force reauthentication. Isolate any user accounts reported as targets of unsolicited IT support calls.
2. **Detection (Ongoing):** Query IdP logs for session tokens used from IPs inconsistent with the authenticating device; look for authentication events where MFA was satisfied but no push notification or TOTP was recorded by the user (common AiTM indicator). In Microsoft Entra ID audit logs, monitor for 'Sign-ins from unfamiliar locations' and 'Atypical travel' alerts. In Google Workspace Admin, review Token Audit for unexpected OAuth grants. Flag rapid sequential access to multiple SaaS platforms (SharePoint, HubSpot, Salesforce) within minutes of a single IdP authentication event.
3. **Eradication (Within 30 days):** Enforce phishing-resistant MFA (FIDO2/WebAuthn hardware keys or passkeys) for all IdP and SaaS authentication; remove SMS and voice OTP as fallback options. Review and revoke any OAuth tokens or email forwarding rules created during the suspected compromise window (T1114.003, T1556.006). Validate that conditional access policies require device compliance, not just session token presence.
4. **Recovery (Post-Containment):** After revoking compromised sessions, audit all SaaS platforms for data exfiltration indicators: new email forwarding rules, bulk file downloads from SharePoint or Google Drive, new OAuth application grants in Salesforce or HubSpot, and API access logs for anomalous volume. Confirm MFA enforcement changes are applied and not bypassable by legacy authentication protocols. Re-verify IdP conditional access policies are active.
5. **Post-Incident (Ongoing):** This campaign exposes a structural gap: CASB and SIEM deployments that lack SaaS-native log ingestion will miss the entire attack chain. Implement continuous SaaS audit log ingestion into your SIEM for all affected platforms. Formalize a vishing response procedure: employees should have a verified out-of-band callback number for any unsolicited IT support contact. Conduct tabletop exercises simulating the vishing-to-AiTM chain against your IdP.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to legal, privacy counsel, and executive leadership immediately if audit logs confirm adversary access to HubSpot contact databases, Salesforce CRM records, SharePoint document libraries, or Gmail/Exchange mailboxes containing PII, PHI, or regulated financial data, as this triggers breach notification obligations under GDPR Article 33 (72-hour clock), HIPAA §164.412, or applicable US state notification statutes; additionally escalate if the vishing target was a privileged administrator account, as lateral movement to on-premises AD via Entra ID hybrid join is a documented escalation path for financially motivated actors using this TTPs.
Recovery Notes	After session revocation and MFA policy hardening, maintain elevated monitoring of all previously compromised accounts and their associated SaaS activity for a minimum of 30 days, as Cordial Spider and Snarky Spider are documented to establish OAuth persistent access grants and API tokens that survive session revocation and can enable delayed secondary access to Salesforce and HubSpot. Verify that FIDO2 enforcement is applied to all authentication paths including legacy protocols by running Entra ID sign-in log queries for any 'clientAppUsed: Exchange ActiveSync' or 'clientAppUsed: Other Clients' authentications post-hardening, which indicate legacy auth bypass paths that these actors exploit. Confirm with business owners of affected SaaS platforms that no bulk data exports, new third-party OAuth integrations, or anomalous API consumer registrations remain active before returning accounts to normal operational status.
Forensic Artifacts	Microsoft Entra ID Sign-in Logs (Portal > Azure AD > Sign-in logs): Filter for 'tokenIssuerType: AzureAD' with 'riskEventType: unfamiliarFeatures' or 'impossibleTravel' — AiTM proxy infrastructure used in this campaign produces sign-in events where the session token IP differs from the MFA-completing device IP, a gap visible in the 'ipAddress' vs. 'deviceDetail.trustType' field combination. | Okta System Log (Admin > Reports > System Log): Filter for 'eventType: user.authentication.sso' events where 'client.ipAddress' does not match the IP from the preceding 'user.session.start' event within the same sessionId — this IP delta is the primary forensic signature of the AiTM relay used by Cordial Spider and Snarky Spider. | Google Workspace Token Audit Log (Admin Console > Reports > Audit > Token): OAuth application grants created within the 60-minute window following initial SSO authentication represent persistence artifacts specific to this campaign; each grant record includes 'app_name', 'scope', and 'client_id' fields that can be cross-referenced against known malicious OAuth app names in threat intelligence feeds. | Exchange Online / Microsoft 365 Unified Audit Log: Query for 'New-InboxRule' and 'Set-InboxRule' operations (MITRE T1114.003) using PowerShell 'Search-UnifiedAuditLog -Operations New-InboxRule,Set-InboxRule -StartDate [incident_window_start] -EndDate [incident_window_end]' — these inbox rule creation events are a high-confidence artifact of this specific campaign's post-compromise persistence phase. | Salesforce Event Monitoring API — 'Login' and 'API' event log files: The 'LOGIN_KEY' field links all API activity to the originating SSO session, enabling reconstruction of which CRM records or reports were accessed or exported during the compromised session; bulk 'REPORT_EXPORT' events within minutes of federation from a new IP are a campaign-specific exfiltration indicator.

Per-Action IR Details

Containment — Immediately audit active SSO/IdP sessions across Google Workspace, Microsoft Entra ID, Okta, and Ping Identity for anomalous sign-in locations, impossible travel, or session age inconsistencies; revoke suspicious sessions and force reauthentication. Isolate any user accounts reported as targets of unsolicited IT support calls.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without enterprise CASB: use Microsoft Entra ID's free 'Revoke-AzureADUserAllRefreshToken' PowerShell cmdlet to invalidate all refresh tokens for a targeted user ('Revoke-AzureADUserAllRefreshToken -ObjectId '). For Google Workspace, use the Admin SDK Directory API or Admin Console > Users > [user] > Security > Sign out of all sessions. For Okta, run 'POST /api/v1/users/{userId}/sessions' clear via Okta API with an admin token. Maintain a running log of every account acted upon with timestamps for chain-of-custody.

Evidence: Before revoking sessions, export and preserve the full active session list from each IdP. In Microsoft Entra ID: export Sign-in logs (Portal > Azure AD > Sign-in logs, filter last 72 hours) and capture 'sessionId', 'ipAddress', 'deviceDetail', and 'conditionalAccessStatus' fields — AiTM sessions will show a compliant device claim with a foreign IP. In Okta: capture System Log export ('GET /api/v1/logs') filtering for 'session.started' and 'user.authentication.sso' events with mismatched 'client.ipAddress' vs. enrolled device. In Google Workspace: Admin Console > Reports > Audit > Login audit, filter for 'login_success' with 'is_suspicious: true' or unexpected 'login_challenge_method: none' entries indicating token reuse without challenge.

Detection — Query IdP logs for session tokens used from IPs inconsistent with the authenticating device; look for authentication events where MFA was satisfied but no push notification or TOTP was recorded by the user (common AiTM indicator). In Microsoft Entra ID audit logs, monitor for 'Sign-ins from unfamiliar locations' and 'Atypical travel' alerts. In Google Workspace Admin, review Token Audit for unexpected OAuth grants. Flag rapid sequential access to multiple SaaS platforms (SharePoint, HubSpot, Salesforce) within minutes of a single IdP authentication event.

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 SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use Microsoft Entra ID's free KQL query in Log Analytics (if diagnostic settings are enabled to a Log Analytics workspace at no per-query cost): 'SigninLogs | where TimeGenerated > ago(72h) | where AuthenticationRequirement == "multiFactorAuthentication" | where DeviceDetail.isCompliant == true | summarize count() by UserPrincipalName, IPAddress, DeviceDetail.displayName | where count_ > 1 and IPAddress !startswith "". For Google Workspace without SIEM, use the Reports API ('GET https://admin.googleapis.com/admin/reports/v1/activity/users/all/applications/token') and pipe output through 'jq' to filter OAuth grants created in the last 24 hours. Use the free Sigma rule 'azure_ad_aitm_phishing_token_theft.yml' (available in SigmaHQ repository) converted to native Entra KQL for AiTM-specific detection.

Evidence: Capture the following before any log rotation occurs: (1) Microsoft Entra ID Sign-in logs filtered for 'riskEventType: impossibleTravel' and 'riskEventType: unfamiliarFeatures' — AiTM proxy IPs used by Cordial Spider and Snarky Spider will appear as residential or hosting-provider IPs with no prior org history; (2) Okta System Log entries for 'policy.evaluate_sign_on' where 'outcome.result: CHALLENGE' is immediately followed by 'user.authentication.sso' with a different IP in the same session — this indicates the AiTM relay forwarded the MFA challenge response; (3) Google Workspace Token Audit log for OAuth application grants created between the initial login event and first SaaS access event — adversaries frequently auto-grant persistent OAuth scopes to maintain access after session token expiry; (4) HubSpot and Salesforce API access logs for 'GET /contacts' or bulk export calls within minutes of the SSO federation event, as these represent the data-drain phase specific to this campaign.

Eradication — Enforce phishing-resistant MFA (FIDO2/WebAuthn hardware keys or passkeys) for all IdP and SaaS authentication; remove SMS and voice OTP as fallback options. Review and revoke any OAuth tokens or email forwarding rules created during the suspected compromise window (T1114.003, T1556.006). Validate that conditional access policies require device compliance, not just session token presence.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without MDM/Intune enforcing device compliance: implement Entra ID Conditional Access (free P1 license feature) with a Named Locations policy blocking all authentication from IPs outside known corporate egress ranges — this disrupts AiTM relay infrastructure that operates from residential proxy networks. To enumerate and revoke email forwarding rules (MITRE T1114.003) without an enterprise tool, run the Exchange Online PowerShell command: 'Get-Mailbox -ResultSize Unlimited | Get-InboxRule | Where-Object {$_.ForwardTo -ne $null -or $_.RedirectTo -ne $null} | Select-Object Name,MailboxOwnerID,ForwardTo,RedirectTo | Export-Csv forwarding_rules_audit.csv'. For Google Workspace, use Admin SDK: 'GET https://www.googleapis.com/gmail/v1/users/{userId}/settings/forwardingAddresses' for each affected user. Revoke persistent OAuth grants in Google Workspace via Admin Console > Security > API Controls > App Access Control.

Evidence: Before modifying authentication policies, preserve: (1) A full export of all OAuth application grants in Google Workspace (Admin Console > Security > API Controls) and Salesforce (Setup > Connected Apps OAuth Usage) timestamped to capture grants created during the compromise window — these represent MITRE T1556.006 persistence mechanisms specific to this campaign; (2) Exchange Online or Google Workspace inbox rules export (see compensating control commands above) to document T1114.003 artifacts before deletion; (3) Entra ID Conditional Access policy configuration snapshot ('Get-AzureADMSConditionalAccessPolicy | ConvertTo-Json | Out-File ca_policy_baseline.json') to document the pre-incident policy state that the attackers successfully bypassed, which informs the gap analysis.

Recovery — After revoking compromised sessions, audit all SaaS platforms for data exfiltration indicators: new email forwarding rules, bulk file downloads from SharePoint or Google Drive, new OAuth application grants in Salesforce or HubSpot, and API access logs for anomalous volume. Confirm MFA enforcement changes are applied and not bypassable by legacy authentication protocols. Re-verify IdP conditional access policies are active.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-11 (Audit Record Retention), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: To audit SharePoint for bulk downloads without a CASB, use the Microsoft Purview Audit (Standard, free) search: filter for 'FileDownloaded' and 'FileSyncDownloaded' operations in the SharePoint workload, grouped by UserId, for the 72-hour compromise window — a single user downloading >50 files in Integrations > Connected Apps and Settings > Account > Audit Log for any export or API token creation events during the compromise window. To verify legacy authentication is blocked in Entra ID, run: 'Get-AzureADPolicy | Where-Object {$_.Type -eq "HomeRealmDiscoveryPolicy"}' and confirm 'AllowCloudPasswordValidation' is false.

Evidence: Before restoring full SaaS access, collect and preserve: (1) SharePoint Unified Audit Log export filtered for 'FileDownloaded', 'PageViewed', and 'SearchQueryPerformed' by the compromised account during the session window — Cordial Spider and Snarky Spider are documented to perform targeted document searches before bulk download, leaving a 'PageViewed' trail before the download burst; (2) Salesforce API usage logs from Event Monitoring showing 'SOQL_EXECUTE' or 'REPORT_EXPORT' events — bulk CRM data exfiltration in this campaign typically presents as report exports rather than individual record views; (3) Google Drive audit log ('GET https://admin.googleapis.com/admin/reports/v1/activity/users/all/applications/drive') filtered for 'download' and 'view' events on files tagged as sensitive or in shared drives; (4) HubSpot audit log export for any new 'Private App' or API key creation events, which represent persistence mechanisms the actors create for post-session access.

Post-Incident — This campaign exposes a structural gap: CASB and SIEM deployments that lack SaaS-native log ingestion will miss the entire attack chain. Implement continuous SaaS audit log ingestion into your SIEM for all affected platforms. Formalize a vishing response procedure: employees should have a verified out-of-band callback number for any unsolicited IT support contact. Conduct tabletop exercises simulating the vishing-to-AiTM chain against your IdP.

NIST Phase: Post Incident

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

Controls: NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST IR-3 (Incident Response Testing), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a commercial SIEM, deploy the free Microsoft Sentinel connector for Google Workspace (via the GWorkspace data connector) or use the open-source 'google-workspace-audit-log-forwarder' to push Google Workspace audit logs to an ELK stack. For Salesforce, use the open-source 'Salesforce-SIEM-Connector' Python library to stream Event Monitoring logs to any syslog-compatible destination. To formalize the vishing callback procedure without a ticketing system, create a laminated 'IT Support Verification Card' for all employees with a single verified callback number and a 3-step verbal verification protocol — this directly counters the Cordial Spider and Snarky Spider social engineering pre-text of impersonating IT helpdesk. For tabletop exercises, use the MITRE ATT&CK Navigator to build an adversary emulation plan using T1566.004 (Spearphishing Voice), T1539 (Steal Web Session Cookie), T1550.004 (Web Session Cookie), T1114.003 (Email Forwarding Rule), and T1556.006 (Multi-Factor Authentication) as the attack chain skeleton.

Evidence: Preserve for lessons-learned and regulatory reporting: (1) A complete timeline reconstruction correlating vishing call records (if available from telephony system CDRs) with the first anomalous IdP authentication event — this establishes the social engineering-to-compromise dwell time specific to this campaign and is required for breach notification timelines under GDPR Article 33 or US state notification laws if PII was accessed in HubSpot, Salesforce, or email; (2) Final export of all OAuth grants, forwarding rules, and API tokens created during the compromise window before they are deleted — these serve as forensic artifacts for threat intelligence sharing via ISAC or law enforcement referral; (3) Conditional Access policy diff between pre-incident and post-incident state to document the specific configuration gap (e.g., legacy auth not blocked, device compliance not required) that enabled the AiTM bypass, supporting both the after-action report and any regulatory audit response.

Detection Guidance

Primary detection surface is IdP and SaaS audit logs; endpoint and network telemetry will not capture this attack. Key behavioral indicators: (1) Authentication events where a session token is reused from a different IP or ASN within seconds of creation, indicating AiTM proxy relay; (2) MFA 'satisfied' events not correlated with a user-reported push or TOTP entry, monitor Okta System Log for 'user.authentication.auth_via_mfa' without corresponding 'system.push.send_factor_verify_push'; (3) Sequential access to 3 or more SaaS platforms within 5 minutes of a single IdP login from an unfamiliar IP; (4) New email forwarding rules or inbox filter creation in Google Workspace or Microsoft 365 shortly after authentication, query Microsoft 365 Unified Audit Log for 'Set-Mailbox' and 'New-InboxRule' operations; (5) Bulk download or sharing events in SharePoint or Google Drive from an authenticated session with no prior access history to those files; (6) New connected application OAuth grants in Salesforce or HubSpot from an account not previously using those integrations. SIEM correlation rule: alert on any account that triggers IdP login + MFA satisfaction + 3+ distinct SaaS platform access events within a 10-minute window from an IP not in the organization's known egress range. For current campaign IOCs (malicious IPs, phishing domains, infrastructure details), consult your threat intelligence platform, sector ISAC feeds, or request a full technical report from your threat intelligence provider. This advisory focuses on behavioral indicators available from IdP and SaaS logs.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	[not available]	AiTM phishing infrastructure domains associated with Cordial Spider and Snarky Spider campaigns are not present in the provided source data. Consult current threat intelligence feeds or your ISAC for active IOCs.	LOW

Framework Mappings

MITRE-ATTACK

- **T1534** — Internal Spearphishing
- **T1199** — Trusted Relationship
- **T1539** — Steal Web Session Cookie
- **T1530** — Data from Cloud Storage
- **T1621** — Multi-Factor Authentication Request Generation
- **T1550.001** — Application Access Token
- **T1556.006** — Multi-Factor Authentication
- **T1567** — Exfiltration Over Web Service
- **T1566.004** — Spearphishing Voice
- **T1048** — Exfiltration Over Alternative Protocol
- **T1114.003** — Email Forwarding Rule
- **T1598.004** — Spearphishing Voice
- **T1656** — Impersonation
- **T1078** — Valid Accounts
- **T1078.004** — Cloud Accounts

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AT-2** — Literacy Training and Awareness
- **SI-4** — System Monitoring

OWASP-TOP10-2021

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

CIS-V8

- **5.2** — Use Unique Passwords
- **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
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1534	Internal Spearphishing	Lateral-Movement
T1199	Trusted Relationship	Initial-Access
T1539	Steal Web Session Cookie	Credential-Access
T1530	Data from Cloud Storage	Collection
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1550.001	Application Access Token	Defense-Evasion
T1556.006	Multi-Factor Authentication	Credential-Access
T1567	Exfiltration Over Web Service	Exfiltration
T1566.004	Spearphishing Voice	Initial-Access

Technique ID	Technique Name	Tactic
T1048	Exfiltration Over Alternative Protocol	Exfiltration
T1114.003	Email Forwarding Rule	Collection
T1598.004	Spearphishing Voice	Reconnaissance
T1656	Impersonation	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1078.004	Cloud Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/cybercrime-groups-using-vishing-a...	T3
Respond to Salesforce SSO Compromise with Containment ...	https://www.linkedin.com/posts/ameykulk_protecting-salesforce-data-...	T3
Disrupting active exploitation of on-premises SharePoint ... - Microsoft	https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting...	T1
How Does Single Sign-On (SSO) Secure HubSpot for Agencies and ...	https://www.struto.io/blog/how-does-single-sign-on-sso-secure-hubsp...	T3
The SharePoint Zero-Day: Why Identity Security Requires Cross ...	https://mesh.security/security/the-sharepoint-zero-day-why-identity/	T3

Generated 2026-05-02 06:45 UTC by TJS Security Command Center