INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-03 06:18 UTC

CORDIAL SPIDER and SNARKY SPIDER Conduct SaaS-Focused Vishing and AiTM Campaigns Against Enterprise Identity Infrastructure

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0263
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	SSO/IdP platforms (generic), SaaS applications (generic), CrowdStrike Falcon Shield (detection/defense context)
Discovery Source	Rss:T1 Threatintel

Executive Summary

Since October 2025, two financially motivated threat actors, CORDIAL SPIDER and SNARKY SPIDER, have conducted targeted campaigns combining voice phishing, credential harvesting, and MFA abuse to gain persistent access to enterprise SaaS environments via compromised identity infrastructure. Both actors operate exclusively through SSO-integrated SaaS applications, bypassing endpoint detection controls entirely. The primary business risks are unauthorized data access, rapid exfiltration, and extortion against organizations that rely on federated identity for SaaS access.

Technical Analysis

CORDIAL SPIDER and SNARKY SPIDER, attributed by CrowdStrike as distinct entities within the broader SPIDER threat cluster, conduct multi-stage identity attacks against SSO/IdP platforms and SaaS applications. Attack chain: vishing to socially engineer victims or helpdesk staff (T1598, T1566), adversary-in-the-middle (AiTM) proxy sessions to harvest session tokens and bypass MFA (T1557, T1111), rogue device registration to establish persistence (T1556.006, T1621), followed by SaaS data access and email collection (T1530, T1114.003). Both actors exploit valid credential abuse (T1078), session and token reuse (T1539, T1550.001, T1550.004), and email hiding rules (T1564.008) to operate within legitimate SaaS sessions, producing minimal endpoint telemetry. CWE mapping: CWE-287 (improper authentication), CWE-308 (single-factor authentication reliance), CWE-359 (exposure of private information). No CVE is associated. No patch exists; this is a tradecraft and configuration risk, not a software vulnerability. CrowdStrike Falcon Shield is cited as a detection control for SaaS session visibility. Source: CrowdStrike blog (T3, vendor attribution).

Action Checklist

1. Containment, Immediately audit active SSO sessions and SaaS OAuth grants for anomalous logins: unexpected geographic origins, new device registrations in the past 90 days, or helpdesk-initiated MFA resets not tied to verified tickets. Suspend suspicious sessions and revoke unrecognized device registrations in your IdP (Okta, Entra ID, Ping) without waiting for full investigation.
2. Detection, Query IdP logs for: MFA push fatigue sequences (T1621, multiple rapid MFA requests), new authenticator device registrations outside normal provisioning windows (T1556.006), and SaaS OAuth token issuance to unrecognized clients (T1550.001). Review inbound call logs and helpdesk tickets for vishing indicators: callers impersonating employees requesting MFA resets or account recovery. Monitor SaaS audit logs (Microsoft 365, Google Workspace, Salesforce) for bulk email access or file download events (T1114.003, T1530).
3. Eradication, Enforce phishing-resistant MFA (FIDO2/passkeys) as the exclusive MFA method across all SSO-connected SaaS applications; decommission SMS and voice-based MFA options entirely. Where organizational constraints prevent this, implement strict conditional access policies requiring device compliance and geolocation verification before MFA is accepted. Revoke all active sessions and tokens for any account confirmed or suspected in scope. Require re-authentication from a managed, compliant device.
4. Recovery, Validate that re-registered MFA devices belong to confirmed employees via out-of-band identity verification (not helpdesk calls alone). Monitor affected accounts for 30 days post-remediation for re-compromise indicators: new device registrations, anomalous SaaS API calls, or resumption of bulk data access patterns. Confirm no persistent OAuth applications or delegated mail rules remain from the intrusion period.
5. Post-Incident, Conduct a gap assessment against MITRE ATT&CK techniques T1078, T1356.006, T1557, and T1621. Evaluate whether your current detection stack has SaaS-layer visibility independent of endpoint telemetry. Update incident response playbooks to include identity-only intrusion scenarios. Implement a strict helpdesk verification protocol (manager callback, HR cross-check) before any MFA reset or account recovery action.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, Legal, and external IR retainer immediately if any confirmed in-scope account has access to PII, PHI, or PCI-scoped data (triggering GDPR 72-hour, HIPAA 60-day, or applicable state breach notification timelines), or if evidence of bulk data exfiltration (T1530, T1114.003) is confirmed in SaaS audit logs, or if the team lacks SaaS-native IdP log access and cannot independently verify session revocation completeness.

Recovery Notes	Post-containment recovery for this campaign must include a 30-day active monitoring window on all previously compromised accounts specifically watching for re-registration of new MFA devices, new OAuth application grants, and resumption of bulk MailItemsAccessed or Drive download events — CORDIAL SPIDER has demonstrated re-entry via residual OAuth tokens that survive password resets if not explicitly revoked. Verify via Entra ID or Okta that no refresh tokens older than your revocation action timestamp remain valid, as OAuth refresh tokens for SaaS applications can persist independently of SSO session state and represent the primary re-entry vector. Confirm with each affected SaaS platform (M365, Google Workspace, Salesforce) that their own session stores have been flushed, since some SaaS platforms maintain independent session caches that do not immediately honor IdP-level revocation.
Forensic Artifacts	Okta System Log (JSON export) — specifically eventType sequences of user.mfa.factor.deactivate followed by user.mfa.factor.activate within a short window for the same actor, which is the forensic signature of SNARKY/CORDIAL's vishing-enabled MFA swap via T1556.006 | Microsoft Entra ID NonInteractiveUserSignInLogs and Audit Logs — OAuth token issuance events (Add OAuth2PermissionGrant) to unrecognized client application IDs are the primary artifact of T1550.001 use; these logs capture the AiTM-harvested token being used to mint persistent OAuth grants invisible to the victim | Microsoft 365 Unified Audit Log — MailItemsAccessed records with non-interactive ClientInfoString values (RESTConnector, EWS, or unknown OAuth client) during the intrusion window document T1114.003 email collection; bulk access of >100 items per session from a single token is a high-confidence exfiltration indicator specific to this campaign | Helpdesk ticketing system records and VoIP/PBX call detail records (CDRs) — the vishing component of CORDIAL SPIDER leaves a social engineering artifact trail in call logs and ticket titles that is unique to this campaign and absent from purely technical intrusions; these records establish the initial access vector and attacker caller ID spoofing pattern | SaaS platform OAuth application consent logs (Google Workspace Admin Reports > Token, Salesforce Connected App OAuth Usage, M365 Enterprise App consent logs) — attacker-consented OAuth applications with broad scopes (Mail.Read, Files.ReadWrite.All, offline_access) registered during the intrusion window are the persistence mechanism for T1550.001 and will survive IdP password resets if not explicitly revoked at the SaaS layer

Per-Action IR Details

Containment — Immediately audit active SSO sessions and SaaS OAuth grants for anomalous logins: unexpected geographic origins, new device registrations in the past 90 days, or helpdesk-initiated MFA resets not tied to verified tickets. Suspend suspicious sessions and revoke unrecognized device registrations in your IdP (Okta, Entra ID, Ping) without waiting for full investigation.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST IA-11 (Re-Authentication), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export active Okta session list via Okta System Log API: GET /api/v1/logs?filter=eventType+eq+"user.session.start"&since= and pipe to jq to isolate sessions with client.geographicalContext.country values outside your baseline. For Entra ID, run: Get-MgAuditLogSignIn -Filter "createdDateTime ge " | Where-Object {$_.RiskLevelDuringSignIn -ne 'none' -or $_.IsInteractive -eq $false} in PowerShell with the Microsoft.Graph module (free). For Ping Identity, pull audit logs from PingFederate's audit.log at /opt/pingfederate/log/audit.log and grep for AUTHN_ATTEMPT events with unfamiliar IP ranges.

Evidence: Before suspending sessions, preserve: (1) Full Okta System Log export (JSON) for the past 90 days filtered on user.authentication.auth_via_mfa, user.mfa.factor.update, and user.session.start events — these capture the

CORDIAL/SNARKY MFA reset and new device registration chain. (2) Entra ID Sign-In Logs and Audit Logs from the Microsoft Entra admin center or via MS Graph API, specifically NonInteractiveUserSignInLogs for OAuth token issuance events. (3) Screenshot or API export of all currently registered authenticator devices per user account in scope, timestamped, before any revocation action — this preserves the forensic record of attacker-registered FIDO/TOTP devices added during the vishing phase.

Detection — Query IdP logs for: MFA push fatigue sequences (T1621 — multiple rapid MFA requests), new authenticator device registrations outside normal provisioning windows (T1556.006), and SaaS OAuth token issuance to unrecognized clients (T1550.001). Review inbound call logs and helpdesk tickets for vishing indicators: callers impersonating employees requesting MFA resets or account recovery. Monitor SaaS audit logs (Microsoft 365, Google Workspace, Salesforce) for bulk email access or file download events (T1114.003, T1530).

NIST Phase: Detection Analysis

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

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

Compensating: MFA fatigue (T1621): In Okta System Log, run: GET /api/v1/logs?filter=eventType+eq+"user.mfa.challenge.issued"&since=, group by actor.alternateId, and flag any user with >5 challenges in a 10-minute window using a simple Python counter script. New device registration (T1556.006): In Entra ID, run: Get-MgAuditLogDirectoryAudit -Filter "activityDisplayName eq 'Register device'" | Select-Object ActivityDateTime, InitiatedBy, TargetResources and cross-reference against your HR provisioning ticket system manually. OAuth token abuse (T1550.001): In Microsoft 365 Unified Audit Log, run Search-UnifiedAuditLog -Operations "Consent to application","Add OAuth2PermissionGrant" -StartDate -EndDate and flag grants to apps not in your approved inventory. For Google Workspace, export token audit data from Admin Console > Reports > Token. Vishing correlation: Pull helpdesk ticket titles containing 'MFA reset', 'account locked', or 'password recovery' from your ticketing system (Jira, ServiceNow, or email) and cross-reference with Okta/Entra MFA factor enrollment events within a 2-hour window of each ticket.

Evidence: Preserve before analysis: (1) Okta System Log entries for eventType user.mfa.factor.deactivate and user.mfa.factor.activate within the same 24-hour window per user — the SNARKY/CORDIAL pattern is deactivate legitimate factor, activate attacker-controlled factor. (2) Microsoft 365 Unified Audit Log entries for MailItemsAccessed (operation) with ClientInfoString values showing non-interactive/OAuth access — bulk MailItemsAccessed from a single session token is the T1114.003 exfiltration artifact. (3) Salesforce Event Monitoring logs (LoginHistory and API usage logs) for anomalous API client IDs and bulk record export operations. (4) Inbound call center / helpdesk phone records or VoIP system logs (Teams call records, Zoom call logs, or your PABX CDR) for calls from numbers not matching employee directory — CORDIAL SPIDER uses spoofed internal numbers for vishing. (5) Google Workspace Admin > Reports > Audit > Drive for bulk file download events (download of >50 files in a session by a single user is a high-confidence T1530 indicator).

Eradication — Enforce phishing-resistant MFA (FIDO2/passkeys) across all SSO-connected SaaS applications; remove SMS and voice-based MFA options where feasible. Implement conditional access policies requiring device compliance verification before SaaS session establishment. Revoke all active sessions and tokens for any account confirmed or suspected in scope. Require re-authentication from a managed, compliant device.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST IA-2 (Identification and Authentication — Organizational Users), NIST SI-2 (Flaw Remediation), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: FIDO2 enforcement without enterprise MDM: In Okta, navigate to Security > Authenticators, set FIDO2 WebAuthn to 'Required' and set SMS/Voice factor enrollment policy to 'Disabled' for all groups — this is included in Okta's free tier for up to 100 users. In Entra ID (free tier), create a Conditional Access policy (requires Entra

ID P1) targeting All Cloud Apps, set Grant control to 'Require authentication strength: Phishing-resistant MFA'; if P1 is unavailable, use Per-user MFA enforcement at aka.ms/mfasetup and manually disable OATH-TOTP and phone options per user via: Update-MgUserAuthenticationPhoneMethod -UserId -PhoneType mobile -PhoneNumber '' (removes phone factor). Session revocation for all in-scope accounts: In Okta run: POST /api/v1/users/{userId}/sessions/me/lifecycle/expire for each identified account. In Entra ID run: Revoke-MgUserSignInSession -UserId for each account. OAuth grant revocation: In Entra ID run: Get-MgUserOauth2PermissionGrant -UserId | Remove-MgOauth2PermissionGrant for each grant issued to unrecognized applications.

Evidence: Before eradicating, preserve: (1) Complete list of OAuth permission grants (scopes, client IDs, grant dates) for all in-scope accounts exported from Entra ID via: Get-MgOauth2PermissionGrant | ConvertTo-Json — these represent the persistent access T1550.001 leaves behind even after password reset. (2) Snapshot of all registered authentication methods per affected user: GET /api/v1/users/{id}/factors (Okta) or Get-MgUserAuthenticationMethod -UserId (Entra) — attacker-registered FIDO2 or TOTP authenticators will appear here and must be documented before removal. (3) Conditional access policy audit log showing policy state at time of compromise — establishes whether device compliance gaps existed that enabled the AiTM session token theft.

Recovery — Validate that re-registered MFA devices belong to confirmed employees via out-of-band identity verification (not helpdesk calls alone). Monitor affected accounts for 30 days post-remediation for re-compromise indicators: new device registrations, anomalous SaaS API calls, or resumption of bulk data access patterns. Confirm no persistent OAuth applications or delegated mail rules remain from the intrusion period.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-11 (Re-Authentication), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 5.3 (Disable Dormant Accounts), CIS 6.1 (Establish an Access Granting Process)

Compensating: Out-of-band MFA device re-enrollment verification: Create a Google Form or internal survey with a unique per-employee token (generated from your HR system), require employees to submit the form from their corporate email on a known-good device, and cross-reference submissions against IdP re-enrollment events before approving. Delegated mail rule detection in M365 (no SIEM required): Run Search-UnifiedAuditLog -Operations 'New-InboxRule','Set-InboxRule' -StartDate -EndDate | Where-Object {$_.AuditData -match 'ForwardTo|RedirectTo|DeleteMessage'} — CORDIAL SPIDER commonly establishes forwarding rules to maintain email visibility post-eradication. Google Workspace equivalent: Use Admin SDK Reports API, pull rules.create events from Gmail audit log. For Salesforce, review Setup > Security > Connected Apps OAuth Usage and revoke any app with last-used date during the intrusion window.

Evidence: Preserve before closing recovery phase: (1) Exchange Online mailbox audit log export (MailboxAuditLog) for all in-scope accounts covering the full intrusion window — specifically MessageBind and SendAs operations that indicate data staging or exfiltration via email (T1114.003 artifact). (2) Full export of inbox rules for all in-scope M365 mailboxes via: Get-InboxRule -Mailbox | Select Name,Description,ForwardTo,DeleteMessage,RedirectTo — persistence mechanism specific to this campaign's post-compromise email access pattern. (3) Salesforce login history export (LoginHistory SOQL query) and Connected App Usage report for the intrusion period — documents the scope of SaaS data access achievable via the stolen OAuth tokens.

Post-Incident — Conduct a gap assessment against MITRE ATT&CK techniques T1078, T1556.006, T1557, and T1621. Evaluate whether your current detection stack has SaaS-layer visibility independent of endpoint telemetry. Update incident response playbooks to include identity-only intrusion scenarios. Implement a strict helpdesk verification protocol (manager callback, HR cross-check) before any MFA reset or account recovery action.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: ATT&CK gap assessment without a commercial tool: Download the MITRE ATT&CK Navigator (free, browser-based at https://mitre-attack.github.io/attack-navigator/) and create a layer mapping your current log sources against T1078 (Valid Accounts), T1556.006 (Modify Authentication Process — Multi-Factor Authentication), T1557 (Adversary-in-the-Middle), and T1621 (MFA Request Generation) — color cells red where you have no detection coverage. For SaaS-layer visibility gap assessment: document which of your monitored log sources are IdP/SaaS-native vs. endpoint-derived; if all your alerts require an endpoint agent (CrowdStrike, Defender, Sysmon), you have a blind spot for this campaign since CORDIAL and SNARKY operate exclusively through SSO-integrated SaaS with no endpoint footprint. Free Sigma rules for these techniques are available in the SigmaHQ repository (github.com/SigmaHQ/sigma) — search for tags attack.t1621 and attack.t1556.006 to get detection rules convertable to Splunk, Elastic, or raw grep queries against exported logs.

Evidence: Preserve for post-incident review: (1) Complete timeline reconstruction from IdP audit logs correlating the vishing call timestamp (from helpdesk records or call logs) → MFA reset event (Okta/Entra audit) → first anomalous session → first SaaS data access event — this chain documents the full CORDIAL/SNARKY kill chain for playbook development. (2) Any CrowdStrike Falcon Shield detection alerts or Identity Protection events generated during the incident — even if no endpoint was compromised, Falcon Identity Threat Protection may have flagged the SSO anomaly and its alert fidelity should be evaluated for future tuning. (3) Helpdesk ticket records, call recordings (if available), and email correspondence associated with the vishing attempt — these are the primary social engineering artifacts unique to this campaign and are essential for staff awareness training.

Detection Guidance

Detection must occur at the identity and SaaS layer; these actors produce no endpoint telemetry. Key log sources: IdP audit logs (Okta System Log, Microsoft Entra Sign-in Logs, Google Workspace Admin Audit), SaaS application audit logs, and telephony/call center records. Behavioral indicators: (1) MFA fatigue sequences - multiple failed push notifications within a short window followed by a successful authentication (T1621); (2) new authenticator or device registration events outside standard provisioning hours or without an associated helpdesk ticket (T1556.006); (3) SaaS OAuth grants issued to new or unrecognized third-party applications (T1550.001); (4) AiTM indicators - authentication events where the IP or ASN does not match the user's historical access pattern, particularly reverse-proxy hosting providers; (5) bulk mailbox access or large-volume file downloads from SaaS storage shortly after a new session is established (T1114.003, T1530); (6) token and session cookie reuse from anomalous network locations (T1539); (7) email hiding rules or forwarding rules configured outside normal user behavior windows (T1564.008); (8) helpdesk call volume spikes with employees reporting MFA requests they did not initiate. CrowdStrike Falcon Shield is referenced by the vendor as a control providing SaaS session visibility for this threat class. MITRE ATT&CK techniques T1078, T1557, T1556.006, T1621, T1550.001, and T1539 are the highest-priority hunting targets.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1557** — Adversary-in-the-Middle
- **T1556.006** — Multi-Factor Authentication
- **T1539** — Steal Web Session Cookie

- **T1564.008** — Email Hiding Rules
- **T1111** — Multi-Factor Authentication Interception
- **T1530** — Data from Cloud Storage
- **T1566** — Phishing
- **T1621** — Multi-Factor Authentication Request Generation
- **T1598.004** — Spearphishing Voice
- **T1550.001** — Application Access Token
- **T1114.003** — Email Forwarding Rule
- **T1550.004** — Web Session Cookie
- **T1598** — Phishing for Information

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
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)

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
- **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)(i)** — Security Awareness and Training

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
T1078	Valid Accounts	Defense-Evasion
T1557	Adversary-in-the-Middle	Credential-Access
T1556.006	Multi-Factor Authentication	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1564.008	Email Hiding Rules	Defense-Evasion
T1111	Multi-Factor Authentication Interception	Credential-Access
T1530	Data from Cloud Storage	Collection
T1566	Phishing	Initial-Access
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1598.004	Spearphishing Voice	Reconnaissance
T1550.001	Application Access Token	Defense-Evasion
T1114.003	Email Forwarding Rule	Collection
T1550.004	Web Session Cookie	Defense-Evasion
T1598	Phishing for Information	Reconnaissance

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/defending-against-cordial-sp...	T3
	https://www.crowdstrike.com/en-us/blog/announcing-threat-ai-industr...	T3
	https://www.crowdstrike.com/en-us/blog/scattered-spider-attempts-to...	T3
	https://www.crowdstrike.com/en-us/blog/announcing-falcon-intelligen...	T3

Source	URL	Tier
SaaS Security Risk Review - CrowdStrike	https://www.crowdstrike.com/en-us/platform/falcon-shield/saas-secur...	**T3**

Generated 2026-05-03 06:18 UTC by TJS Security Command Center