INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-03 18:28 UTC

SaaS-First Adversaries: How CORDIAL SPIDER and SNARKY SPIDER Are Rewriting the Social Engineering Playbook

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0264
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	SSO/IdP platforms (generic), SaaS applications (generic), CrowdStrike Falcon Shield (defensive context)
Discovery Source	Rss:T1 Threatintel

Executive Summary

Since October 2025, two financially motivated threat actors, CORDIAL SPIDER and SNARKY SPIDER, have conducted targeted data theft and extortion campaigns by hijacking employee SSO credentials and session tokens through adversary-in-the-middle phishing and voice-based deception. Once inside, attackers move freely across cloud and SaaS environments without ever touching a managed endpoint, bypassing endpoint detection tools entirely. Organizations relying solely on EDR and traditional MFA face significant exposure; the business risk includes data exfiltration, extortion, and potential disruption to any SaaS-dependent business process.

Technical Analysis

CORDIAL SPIDER and SNARKY SPIDER conduct AiTM phishing campaigns, typically vishing-assisted, to intercept SSO credentials and session cookies in real time, defeating standard TOTP and push-based MFA. Post-authentication, actors register attacker-controlled devices to the victim's MFA profile (T1556.006), effectively locking out legitimate recovery paths. Lateral movement occurs entirely within the SaaS layer (T1078, T1078.004, T1550.001, T1550.004) using harvested application access tokens and stolen session cookies (T1539), without requiring endpoint footholds. Inbox rule manipulation (T1114.003) suppresses security alert delivery and hides follow-on phishing lures. The Genymobile Android emulator is abused to simulate mobile device registration, supporting persistence and complicating forensic timelines (T1564, T1564.008). No CVE identifiers are associated with this campaign; exploitation targets authentication design weaknesses: CWE-1390 (Weak Authentication), CWE-308 (Single-Factor Authentication reliance), CWE-384 (Session Fixation), and

CWE-287 (Improper Authentication). Attribution and defensive guidance are sourced from CrowdStrike threat intelligence.

Action Checklist

1. Containment, Immediately audit all SSO/IdP registered MFA devices for unrecognized entries; revoke suspicious device registrations and force re-authentication for affected accounts.
2. Containment, Review active SaaS sessions across Microsoft 365, Google Workspace, Okta, and similar platforms for anomalous token usage.
3. Detection, Query identity provider logs for MFA device registration events from unexpected IP addresses or outside business hours. Search email logs for inbox rules created by users that forward, delete, or suppress messages containing keywords like 'alert', 'security', 'phishing', or vendor notification subjects. Review SSO authentication logs for session tokens used from multiple geographic locations within short windows (T1539, T1550.001).
4. Eradication, Remove all unrecognized MFA devices from affected accounts. Invalidate all active sessions and tokens for confirmed or suspected compromised accounts. Audit and delete unauthorized inbox rules across the mail environment (T1114.003). Review and remove any unrecognized Android device registrations in mobile device management or IdP console.
5. Recovery, Re-enroll affected users in MFA using phishing-resistant methods (FIDO2/hardware keys where possible). Validate that all inbox rules match expected user configurations. Monitor identity logs for 30 days post-remediation for re-registration attempts or anomalous token activity. Confirm no persistent OAuth application grants or delegated access remain from attacker-controlled apps.
6. Post-Incident, Assess current detection coverage for identity-layer and SaaS-layer activity; EDR alone does not detect this attack pattern. Implement Conditional Access policies enforcing device compliance and geographic/network restrictions for SSO. Establish a detection rule baseline for MFA device registration events and inbox rule creation. Review CrowdStrike's Falcon Shield SaaS Security Risk Review guidance for control benchmarking.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to legal counsel and executive leadership immediately if IdP audit logs confirm attacker session tokens were used to access SaaS applications containing PII, PHI, or financial records, as this triggers breach notification obligations under GDPR Article 33 (72-hour window), HIPAA Breach Notification Rule, or applicable state statutes; escalate to your cloud service provider's abuse team if attacker-controlled OAuth apps or delegated mailbox access cannot be fully revoked through standard admin controls.

Recovery Notes	Re-enrollment of affected users must use FIDO2 or certificate-based authentication exclusively — TOTP and push-based MFA remain vulnerable to the AiTM proxy technique used by both CORDIAL SPIDER and SNARKY SPIDER, and re-enrolling affected accounts in the same MFA method that was bypassed provides no additional protection. Monitor Okta System Log, Entra ID Sign-In Logs, and Google Workspace Admin Audit for the 30-day window post-remediation specifically for `user.mfa.factor.activate` events from mobile ASNs or residential ISPs, which are characteristic of attacker re-registration attempts after initial eviction. Before declaring recovery complete, verify that no OAuth application with `Mail.Read`, `Mail.ReadWrite`, `Calendars.ReadWrite`, or `Files.ReadWrite.All` delegated permissions exists in the tenant beyond explicitly approved, IT-managed applications.
Forensic Artifacts	Okta System Log (JSON export via /api/v1/logs): events `user.mfa.factor.activate`, `user.session.start`, `policy.evaluate_sign_on` — the AiTM relay used by CORDIAL SPIDER and SNARKY SPIDER produces sequential authentication events from two distinct IPs (victim IP, then attacker relay IP) against the same session within seconds, which is the definitive forensic signature of T1550.001 token theft via adversary-in-the-middle | Microsoft Entra ID AADNonInteractiveUserSignInLogs table (Log Analytics or CSV export): captures OAuth token refresh events that persist after the initial phishing session ends — attacker-reused tokens appear as non-interactive sign-ins from IP addresses inconsistent with the user's normal authentication pattern, often from cloud-hosted VPS or residential proxy ASNs | Exchange Online or Google Workspace inbox rule audit log: records rule creation timestamp, creator IP, and full rule predicate — rules created by CORDIAL SPIDER and SNARKY SPIDER during the compromise window systematically suppress forwarded copies of security alerts, MFA enrollment notifications, and vendor advisory emails to prevent victim detection of T1114.003 activity | SaaS application access logs for Microsoft 365 (Unified Audit Log, `FileAccessed` and `SearchQueryInitiated` operations), Google Drive audit events, and Salesforce event monitoring logs for the compromised account's session window — these logs establish the data access scope and are the primary evidence source for exfiltration assessment, since these actors operate exclusively at the SaaS layer without touching managed endpoints | MDM or IdP device enrollment console export (Intune `Get-MgDeviceManagementManagedDevice` or Okta device API): Android device registrations created during the attacker's access window — SNARKY SPIDER specifically registers rogue authenticator-enrolled Android devices as a persistence mechanism to survive password resets, making this artifact the key indicator distinguishing a fully eradicated compromise from one with remaining attacker foothold

Per-Action IR Details

Containment — Immediately audit all SSO/IdP registered MFA devices for unrecognized entries; revoke suspicious device registrations and force re-authentication for affected accounts. Review active SaaS sessions across Microsoft 365, Google Workspace, Okta, and similar platforms for anomalous token usage.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without a SIEM: use Okta's System Log API with a free-tier export — run `curl -H 'Authorization: SSWS ' 'https://.okta.com/api/v1/logs?filter=eventType+eq+%22user.mfa.factor.activate%22&since='` to pull all MFA enrollment events in the last 30 days. For Entra ID (Azure AD), run `Get-MgAuditLogSignIn -Filter "createdDateTime ge " | Where-Object {$_.RiskState -ne 'none'} | Export-Csv signins.csv` using the free Microsoft Graph PowerShell SDK. For Google Workspace, use the free Admin SDK Reports API to pull `admin` activity events filtered on `ADD_RECOVERY_INFO` or `ENROLL_SECOND_FACTOR`.

Evidence: Capture BEFORE revoking any sessions — export full IdP session and device registration audit logs timestamped from 90 days prior to discovery: (1) Okta System Log entries for `user.mfa.factor.activate`, `user.session.start`, and `user.account.update_password`; (2) Entra ID Sign-In Logs and Audit Logs — specifically `Add registered users` and `Update device` operations in the `DirectoryAudit` table via Microsoft Sentinel or Log Analytics; (3) Google Workspace Admin Audit log for `ENROLL_SECOND_FACTOR` and `SUSPICIOUS_LOGIN`; (4) Active session token metadata including IP addresses, user-agent strings, and ASN/geolocation for all concurrent or rapid-succession sessions, which are the primary AiTM artifact left by CORDIAL SPIDER and SNARKY SPIDER tooling (T1550.001).

Detection — Query identity provider logs for MFA device registration events from unexpected IP addresses or outside business hours. Search email logs for inbox rules created by users that forward, delete, or suppress messages containing keywords like 'alert', 'security', 'phishing', or vendor notification subjects. Review SSO authentication logs for session tokens used from multiple geographic locations within short windows (T1539, T1550.001).

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-2 (Event Logging), 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 three targeted queries: (1) Inbox rule detection — connect to Exchange Online via PowerShell: `Get-Mailbox -ResultSize Unlimited | ForEach-Object { Get-InboxRule -Mailbox $_.UserPrincipalName } | Where-Object { $_.ForwardTo -or $_.DeleteMessage -or $_.SubjectContainsWords -match 'alert|security|phishing' } | Export-Csv inbox_rules_audit.csv`; (2) Impossible travel detection — export Okta or Entra sign-in logs to CSV and use a simple Python script with `geopy` or the free MaxMind GeoLite2 database to flag session pairs where the same token authenticates from IPs more than 500km apart within 60 minutes; (3) For Google Workspace environments, use the free GAM CLI tool (`gam all users show forwardingaddresses` and `gam all users show filters`) to enumerate forwarding rules and filters across all mailboxes in a single pass.

Evidence: Before closing any sessions, preserve: (1) Raw Okta System Log JSON for the 72-hour window preceding discovery, specifically events `policy.evaluate_sign_on`, `user.mfa.factor.activate`, and `user.session.start` — the AiTM proxy used by these actors produces a distinctive user-agent pattern and IP sequence where the legitimate user IP and the attacker relay IP appear in rapid succession on the same account; (2) Exchange Online or Google Workspace message trace logs showing the exact creation timestamp, rule conditions, and originating IP of any inbox rules touching keywords related to security notifications — CORDIAL SPIDER and SNARKY SPIDER both suppress vendor security alerts post-compromise to extend dwell time; (3) Microsoft Entra ID `AADNonInteractiveUserSignInLogs` table entries, which capture OAuth token refresh activity that persists after the initial AiTM session and is the primary indicator of T1550.001 token reuse.

Eradication — Remove all unrecognized MFA devices from affected accounts. Invalidate all active sessions and tokens for confirmed or suspected compromised accounts. Audit and delete unauthorized inbox rules across the mail environment (T1114.003). Review and remove any unrecognized Android device registrations in mobile device management or IdP console.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST CM-2 (Baseline Configuration), NIST SI-2 (Flaw Remediation), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For complete token invalidation in Entra ID without a PAM tool: `Revoke-MgUserSignInSession -UserId ` via Microsoft Graph PowerShell (free) — run against all confirmed and suspected accounts in a loop from a CSV list. For Okta: use the Sessions API `DELETE /api/v1/users/{userId}/sessions` to clear all sessions programmatically. For inbox rule removal across Exchange Online: `Get-Mailbox -ResultSize Unlimited | ForEach-Object { Get-InboxRule -Mailbox $_.UserPrincipalName | Where-Object { $_.ForwardTo -or $_.DeleteMessage } | Remove-InboxRule -Confirm:$false }`. For Android MDM device audit: if Intune is in use, run

`Get-MgDeviceManagementManagedDevice -Filter "operatingSystem eq 'Android'" | Where-Object { $_.EnrolledDateTime -gt '' }` to identify devices enrolled during the attacker's access window.

Evidence: Capture before eradication: (1) Full export of all MFA authenticator app registrations, hardware tokens, and phone numbers registered to each affected account — include registration timestamp, registering IP, and device fingerprint; SNARKY SPIDER specifically registers rogue Android authenticator devices to maintain persistent MFA access after initial credential theft; (2) Complete inbox rule export for all affected accounts including rule ID, creation time, creator IP, and full rule conditions — this is forensic proof of T1114.003 and may be required for regulatory notification; (3) OAuth application consent grants for all affected accounts via Entra ID `Get-MgUserOauth2PermissionGrant -UserId ` — both actor groups have been observed granting persistent delegated access to attacker-controlled OAuth apps as a secondary persistence mechanism beyond session tokens.

Recovery — Re-enroll affected users in MFA using phishing-resistant methods (FIDO2/hardware keys where possible). Validate that all inbox rules match expected user configurations. Monitor identity logs for 30 days post-remediation for re-registration attempts or anomalous token activity. Confirm no persistent OAuth application grants or delegated access remain from attacker-controlled apps.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST IA-3 (Device Identification and Authentication), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For FIDO2 key deployment on limited budget: YubiKey 5 NFC (~$50/unit) or Google Titan keys are the minimum viable phishing-resistant authenticator — prioritize accounts with access to financial systems, HR data, or cloud admin consoles first. For ongoing 30-day monitoring without a SIEM: schedule a daily cron job or Windows Task Scheduler entry to run the Okta or Entra audit log export script and pipe output through `grep` or PowerShell `Select-String` filtering on `mfa.factor.activate`, `device.enroll`, and `oauth2.token.grant` events, emailing results to the IR team. For OAuth grant auditing: run `Get-MgUserOauth2PermissionGrant` weekly across all previously affected accounts and diff against a known-good baseline saved at re-enrollment time.

Evidence: Before closing the recovery phase, document: (1) Baseline snapshot of all MFA devices registered post-re-enrollment per account, including FIDO2 key serial numbers or authenticator app device IDs — this is the clean-state reference for future anomaly detection; (2) Verified list of all approved inbox rules per affected user signed off by the user and their manager — required to distinguish legitimate rules from any re-established attacker rules during the 30-day monitoring window; (3) Full OAuth application consent inventory (`Get-MgOauth2PermissionGrant` at the tenant level) as of recovery completion — CORDIAL SPIDER and SNARKY SPIDER have re-established access by re-phishing users after initial remediation when OAuth app grants were not fully removed.

Post-Incident — Assess current detection coverage for identity-layer and SaaS-layer activity; EDR alone does not detect this attack pattern. Implement Conditional Access policies enforcing device compliance and geographic/network restrictions for SSO. Establish a detection rule baseline for MFA device registration events and inbox rule creation. Review CrowdStrike's Falcon Shield SaaS Security Risk Review guidance for control benchmarking.

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 SI-4 (System Monitoring), NIST CA-7 (Continuous Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For detection rule deployment without a commercial SIEM: publish Sigma rules targeting `user.mfa.factor.activate` (Okta) and `Add registered users` (Entra ID) to a free ELK Stack or Wazuh instance — the Sigma project (github.com/SigmaHQ/sigma) contains community rules for AiTM phishing and inbox rule creation that map directly to T1539 and T1114.003. For Conditional Access without Entra ID P2: Entra ID P1 (included in Microsoft 365 Business Premium) supports named location-based CA policies — create a named location policy blocking authentication from Tor exit nodes and high-risk ASNs using the free `ipinfo.io` bulk ASN dataset. For CrowdStrike

Falcon Shield benchmarking without a Falcon subscription: use the free CIS CSAT (Controls Self Assessment Tool) mapped to CIS Controls v8.1 IG2 safeguards as a proxy control benchmark for SaaS identity security posture.

Evidence: Preserve for lessons-learned and regulatory documentation: (1) Complete timeline reconstruction from IdP logs showing the full attack chain — initial AiTM phishing event (T1557), session token harvest (T1539), first attacker authentication (T1550.001), inbox rule creation (T1114.003), and any data access events in connected SaaS applications — this timeline is required for breach notification assessments under GDPR Article 33 or state data breach laws if PII was accessed; (2) Detection gap analysis documenting which EDR, SIEM, or email security controls generated zero alerts during the intrusion — this is the primary deliverable for improving detection coverage against future CORDIAL SPIDER and SNARKY SPIDER campaigns; (3) Final count and classification of SaaS applications accessed via the compromised session tokens, with data sensitivity classification per application — required to assess exfiltration scope and regulatory notification obligations.

Detection Guidance

Primary detection surface is the identity and SaaS layer, not endpoints. Key signals: (1) MFA device registration events from IP addresses not previously associated with the user, query IdP audit logs (Okta System Log event type 'system.mfa.factor.activate', Azure AD 'Add registered security info', Google Workspace 'enrollment' events). (2) Inbox rules created via API or mail client that redirect, delete, or suppress messages, query Exchange/M365 audit logs for 'New-InboxRule' or 'Set-InboxRule' operations, particularly those targeting security-related keywords. (3) Session token reuse from geographically or ASN-inconsistent source IPs within the same session window, review Conditional Access sign-in logs and SIEM correlation rules for 'impossible travel' on token-based authentication. (4) Application access token grants to unrecognized OAuth applications, audit OAuth consent logs in Azure AD, Google Workspace Admin, and Okta. (5) Android device registrations from emulator signatures (Genymobile/Genymotion emulator fingerprints in device management or IdP user agent strings). Behavioral indicators include: login followed immediately by MFA device change, inbox rule creation within 10 minutes of first login, and bulk data access or download events in SaaS applications shortly after authentication.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1078.004** — Cloud Accounts
- **T1598** — Phishing for Information
- **T1556.006** — Multi-Factor Authentication
- **T1539** — Steal Web Session Cookie
- **T1566** — Phishing
- **T1550.001** — Application Access Token
- **T1564.008** — Email Hiding Rules
- **T1114.003** — Email Forwarding Rule
- **T1550.004** — Web Session Cookie
- **T1621** — Multi-Factor Authentication Request Generation
- **T1557** — Adversary-in-the-Middle

- **T1098.005** — Device Registration
- **T1111** — Multi-Factor Authentication Interception
- **T1564** — Hide Artifacts
- **T1534** — Internal Spearphishing
- **T1566.004** — Spearphishing Voice

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
T1078.004	Cloud Accounts	Defense-Evasion
T1598	Phishing for Information	Reconnaissance
T1556.006	Multi-Factor Authentication	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1566	Phishing	Initial-Access
T1550.001	Application Access Token	Defense-Evasion
T1564.008	Email Hiding Rules	Defense-Evasion
T1114.003	Email Forwarding Rule	Collection
T1550.004	Web Session Cookie	Defense-Evasion
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1098.005	Device Registration	Persistence
T1111	Multi-Factor Authentication Interception	Credential-Access
T1564	Hide Artifacts	Defense-Evasion
T1534	Internal Spearphishing	Lateral-Movement
T1566.004	Spearphishing Voice	Initial-Access

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/meet-crowdstrikes-adversary-...	T3
SaaS Security Risk Review - CrowdStrike	https://www.crowdstrike.com/en-us/platform/falcon-shield/saas-secur...	T3

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 2026-05-03 18:28 UTC by TJS Security Command Center