INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-04 13:27 UTC

SaaS-Only Identity Attacks: CORDIAL SPIDER and SNARKY SPIDER Signal a Structural Shift in Extortion Tradecraft

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0267
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	SaaS platforms with SSO/IdP integration, identity providers, enterprises using CrowdStrike Falcon Shield
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 against enterprises using SaaS platforms and federated identity providers. Both actors bypass endpoint detection entirely, operating exclusively within trusted SaaS environments after gaining access through voice phishing and credential interception. Organizations relying on MFA alone for SaaS access are exposed, and the business risk includes data exfiltration, extortion, and reputational damage without any traditional malware footprint to detect.

Technical Analysis

CORDIAL SPIDER and SNARKY SPIDER are distinct threat actors conducting SaaS-centric intrusions observed since October 2025. Neither actor requires endpoint access. Initial access is achieved via vishing (T1566.004) to socially engineer help desk or IT staff into resetting credentials or MFA devices. Adversary-in-the-middle (AiTM) frameworks (T1557) intercept session tokens and cookies (T1539, T1550.001) to bypass MFA. Actors hijack MFA device registrations (T1111, T1621) and modify identity provider authentication mechanisms (T1556.006) to persist in IdP sessions. Post-access activity includes exfiltration to cloud storage (T1567, T1530), internal spearphishing for lateral movement within the SaaS environment (T1534), and disabling or modifying logging and alerting (T1562.001, T1070.003). Cloud account abuse (T1078.004) enables sustained access under the guise of legitimate users. No CVE is associated with this campaign. Relevant weaknesses include CWE-306 (missing authentication for critical function), CWE-308 (use of single-factor authentication), and CWE-287 (improper authentication). Source: CrowdStrike Falcon Shield SaaS Security Risk Review and associated threat research.

Action Checklist

1. Containment: Immediately audit all IdP sessions (Okta, Entra ID, Ping) for anomalous MFA device registrations or recently added authenticators not initiated by the account owner. Suspend suspicious sessions and revoke associated tokens. Review CrowdStrike Falcon Shield SaaS Security Risk Review guidance for platform-specific containment steps.
2. Detection: Query IdP logs for MFA device enrollment events not preceded by a verified user-initiated request. Alert on session tokens used from geographically inconsistent locations within short time windows. Monitor for T1556.006 indicators: unexpected changes to authentication policies or IdP connector configurations. Review SaaS audit logs for bulk data access or export activity (T1530, T1567) from accounts with recent credential or MFA changes.
3. Eradication: Remove unauthorized MFA devices from all IdP-registered accounts. Rotate credentials for any account where vishing or credential interception is suspected. Enforce phishing-resistant MFA (FIDO2/passkeys) across all SaaS and IdP integrations; SMS and push-based MFA are insufficient against AiTM. Review and harden help desk identity verification procedures to eliminate vishing as an access path.
4. Recovery: Validate that all IdP authentication policies reflect intended configurations. Confirm no unauthorized OAuth applications or API tokens remain active. Re-baseline SaaS audit logs to establish normal access patterns. Monitor for recurrence of anomalous session behavior for a minimum of 30 days post-remediation.
5. Post-Incident: Conduct a full SaaS access review to identify over-permissioned accounts and unnecessary SaaS integrations. Implement conditional access policies that evaluate session risk continuously, not only at login. Establish a formal help desk identity verification protocol requiring out-of-band confirmation before any credential or MFA reset. Map control gaps to NIST CSF Protect and Detect functions and prioritize identity governance improvements.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, Legal, and external IR retainer immediately if any evidence of bulk SaaS data export (T1530, T1567) is confirmed, if unauthorized OAuth grants are discovered persisting post-remediation, or if affected accounts have access to PII, PHI, or PCI-scoped data that triggers breach notification obligations under GDPR Article 33, HIPAA §164.412, or applicable US state notification statutes.
Recovery Notes	Post-containment recovery must validate that all IdP authentication policies, OAuth grants, and MFA registrations match a known-good baseline — not just that suspicious items were removed, but that no secondary persistence mechanisms (rogue OAuth apps, shadow admin accounts, or modified federation trusts) were introduced during the attacker's SaaS-only dwell period. Given that CORDIAL SPIDER and SNARKY SPIDER operate without touching endpoints, traditional EDR-based recovery validation is insufficient; recovery must be confirmed entirely through IdP audit logs and SaaS platform audit trails. Maintain elevated monitoring on affected accounts and associated SaaS platforms for a minimum of 30 days, with weekly manual review of MFA enrollment events and OAuth grant lists, as these actors have demonstrated willingness to re-engage targets after initial eviction.

Forensic Artifacts	Okta System Log entries for 'user.mfa.factor.activate' events — specifically enrollments where the actor IP geolocation does not match the account owner's historical login pattern, or where the enrollment occurred within minutes of a help desk ticket closure, indicating CORDIAL SPIDER or SNARKY SPIDER vishing-assisted enrollment | Entra ID Sign-in Logs and Audit Logs showing session tokens authenticated successfully from an AiTM proxy IP (look for sign-ins with MFA claim satisfied but originating from hosting provider ASNs inconsistent with the user's normal location, a hallmark of the AiTM credential interception technique used by both actors) | SaaS platform audit logs (Microsoft 365 Unified Audit Log 'FileDownloaded'/'FileSyncDownloadedFull', Salesforce Event Monitoring 'ReportExport', Google Workspace Drive audit 'download') from the compromised account session window — these capture T1530 and T1567 data theft activity that occurs entirely within the SaaS layer with no endpoint footprint | IdP connector and federation configuration change logs (Okta System Log event type 'system.idp.lifecycle.update', Entra ID Audit Log 'Update federation settings on domain') indicating T1556.006 manipulation of authentication policies by the threat actor to establish persistence or weaken authentication requirements | OAuth application grant records from all integrated SaaS platforms (Entra ID Audit Log 'Add OAuth2PermissionGrant', Okta /api/v1/apps endpoint snapshot) capturing any third-party application granted delegated permissions during or after the attacker's session — these grants survive credential rotation and represent a persistence mechanism specific to the SaaS-only attack model employed by CORDIAL SPIDER and SNARKY SPIDER

Per-Action IR Details

Containment — Immediately audit all IdP sessions (Okta, Entra ID, Ping) for anomalous MFA device registrations or recently added authenticators not initiated by the account owner. Suspend suspicious sessions and revoke associated tokens. Review CrowdStrike Falcon Shield SaaS Security Risk Review guidance for platform-specific containment steps.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), 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 built-in System Log (Admin > Reports > System Log) filtered on event type 'user.mfa.factor.activate' and 'user.session.start' — export to CSV and sort by 'actor.alternateId' to surface accounts with MFA changes in the last 72 hours. For Entra ID, run: Get-MgAuditLogSignIn -Filter "createdDateTime ge 2025-10-01" | Where-Object {$_.conditionalAccessStatus -eq 'failure'} combined with Get-MgUserAuthenticationMethod -UserId to enumerate registered authenticators per account. Revoke sessions via Okta Admin Console > User > More Actions > Clear User Sessions, or Entra ID: Revoke-MgUserSignInSession -UserId .

Evidence: Before revoking sessions, export and preserve: (1) Okta System Log entries for 'user.mfa.factor.activate', 'user.authentication.sso', and 'user.session.impersonation' events with full actor IP, user-agent, and geolocation metadata; (2) Entra ID Sign-in Logs (Azure Portal > Entra ID > Monitoring > Sign-in logs) filtered on the targeted accounts, capturing IP address, location, device compliance state, and MFA method used; (3) Entra ID Audit Logs for 'Update user' and 'Add registered owners to application' events; (4) any Okta ThreatInsight or Entra ID Identity Protection risk event records flagged against the affected accounts at time of compromise — these are overwritten on session revocation in some tenant configurations.

Detection — Query IdP logs for MFA device enrollment events not preceded by a verified user-initiated request. Alert on session tokens used from geographically inconsistent locations within short time windows. Monitor for T1556.006 indicators: unexpected changes to authentication policies or IdP connector configurations. Review SaaS audit logs for bulk data access or export activity (T1530, T1567) from accounts with recent credential or MFA changes.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Use the free Sigma rule 'okta_mfa_fatigue_attack.yml' (SigmaHQ/sigma repository) adapted to flag 'user.mfa.factor.activate' events not preceded by a 'user.mfa.factor.activate.request' within a 5-minute window. For Entra ID, run this PowerShell query against exported sign-in logs: Import-Csv signins.csv | Group-Object UserPrincipalName | Where-Object { ($_.Group | Select-Object -ExpandProperty IPAddress | Sort-Object -Unique).Count -gt 2 } to surface accounts authenticating from multiple countries within a single day — a key AiTM (Adversary-in-the-Middle) indicator used by both CORDIAL SPIDER and SNARKY SPIDER. For SaaS bulk export detection without a SIEM, query Salesforce Event Monitoring (free tier: Login History), Google Workspace Admin > Reports > Drive, or Microsoft 365 Unified Audit Log (Search-UnifiedAuditLog -Operations 'FileDownloaded','FileSyncDownloadedFull' -StartDate (Get-Date).AddDays(-7)) filtering on accounts with recent MFA changes.

Evidence: Capture before any account modification: (1) Okta System Log entries for 'policy.evaluate_sign_on', 'user.mfa.factor.activate', and 'application.provision.user' events showing the session token, IP, and user-agent string at time of AiTM credential interception — the intercepted session token will show a source IP inconsistent with the victim's normal geopattern; (2) Entra ID Conditional Access policy change audit log entries for T1556.006 — look for 'Update conditional access policy' events with actor not matching a known admin account; (3) SaaS application audit logs (SharePoint, Salesforce, Workday) for bulk 'FileDownloaded' or 'ReportExported' operations within the session window of the compromised account — CORDIAL SPIDER and SNARKY SPIDER specifically target high-value SaaS repositories post-access; (4) IdP connector configuration change logs (Okta Admin > Reports > System Log, event type 'system.idp.lifecycle.update') for unauthorized federation trust modifications.

Eradication — Remove unauthorized MFA devices from all IdP-registered accounts. Rotate credentials for any account where vishing or credential interception is suspected. Enforce phishing-resistant MFA (FIDO2/passkeys) across all SaaS and IdP integrations; SMS and push-based MFA are insufficient against AiTM. Review and harden help desk identity verification procedures to eliminate vishing as an access path.

NIST Phase: Eradication

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

Controls: NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without an IdP automation platform, use Okta's bulk user update via API: GET /api/v1/users/{userId}/factors to enumerate all registered factors, then DELETE /api/v1/users/{userId}/factors/{factorId} for each unauthorized TOTP or push factor — script this in Python using the okta-sdk-python library targeting accounts flagged in the detection phase. For Entra ID, remove unauthorized authenticators via: Get-MgUserAuthenticationMethod -UserId followed by Remove-MgUserAuthenticationMethod -UserId -AuthenticationMethodId . To enforce FIDO2 in Entra ID without Azure AD Premium P2, use the free Authentication Methods Policy (Update-MgPolicyAuthenticationMethodPolicy) to disable SMS and voice OTP at the tenant level. Document each removed factor with timestamp and factor ID before deletion for chain-of-custody purposes.

Evidence: Before removing unauthorized MFA devices, export and preserve: (1) Full authenticator enrollment records from Okta (Admin > Reports > System Log, event 'user.mfa.factor.activate') capturing enrollment IP, timestamp, device fingerprint, and whether enrollment was self-service or admin-initiated — CORDIAL SPIDER and SNARKY SPIDER use vishing to social-engineer help desk staff into enrolling attacker-controlled authenticators, so admin-initiated enrollments on accounts not in active onboarding are high-fidelity IOCs; (2) Entra ID Audit Log entries for 'User registered security info' and 'User deleted security info' events for all accounts in scope; (3) Help desk ticketing system records (ServiceNow, Jira Service Management, or email) for any password or MFA reset requests received in the 30 days prior to detection — vishing attempts by these actors frequently precede unauthorized MFA enrollment by 24–72 hours.

Recovery — Validate that all IdP authentication policies reflect intended configurations. Confirm no unauthorized OAuth applications or API tokens remain active. Re-baseline SaaS audit logs to establish

normal access patterns. Monitor for recurrence of anomalous session behavior for a minimum of 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CM-6 (Configuration Settings), NIST AU-11 (Audit Record Retention), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Export a current snapshot of all Okta authentication policies via: curl -H 'Authorization: SSWS ' https://.okta.com/api/v1/policies?type=OKTA_SIGN_ON and diff against a known-good configuration snapshot saved before the incident — store both in version control (git) for audit trail. For Entra ID, export Conditional Access policies via: Get-MgIdentityConditionalAccessPolicy | ConvertTo-Json -Depth 10 > ca_policy_baseline_$(Get-Date -Format yyyyMMdd).json. To enumerate active OAuth app grants without a CASB, use: Get-MgServicePrincipalOauth2PermissionGrant (Entra ID) or query Okta's /api/v1/authorizationServers/{authServerId}/clients endpoint and flag any application not in the pre-incident approved application inventory. Set a 30-day recurring calendar task to re-run the MFA enrollment audit query and OAuth grant review as a manual recurrence check.

Evidence: Before declaring recovery complete, capture and retain: (1) A timestamped export of all active Okta and Entra ID session tokens and their associated device/IP metadata immediately post-remediation, as a recovery baseline; (2) OAuth application grant lists from affected SaaS platforms (Microsoft 365 via Search-UnifiedAuditLog -Operations 'Add OAuth2PermissionGrant', Salesforce Connected Apps audit, Google Workspace > Security > API Controls) — CORDIAL SPIDER and SNARKY SPIDER have been observed establishing persistent OAuth grants to maintain access after initial credential revocation; (3) SaaS platform-specific audit log exports (Workday, ServiceNow, Salesforce) covering the full incident window, retained for a minimum of 12 months per NIST AU-11 (Audit Record Retention) to support post-incident analysis and potential regulatory inquiry.

Post-Incident — Conduct a full SaaS access review to identify over-permissioned accounts and unnecessary SaaS integrations. Implement conditional access policies that evaluate session risk continuously, not only at login. Establish a formal help desk identity verification protocol requiring out-of-band confirmation before any credential or MFA reset. Map control gaps to NIST CSF Protect and Detect functions and prioritize identity governance improvements.

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 AC-2 (Account Management), NIST IA-11 (Re-authentication), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For continuous session risk evaluation without a CASB or Entra ID P2, implement Okta's free ThreatInsight (Admin > Security > General > ThreatInsight) set to 'Log and Enforce Mode' — this applies behavioral risk signals to active sessions, not only at login, at no additional cost. For the help desk out-of-band verification protocol, implement a simple callback procedure using a pre-registered phone number from the HR system (not a number supplied by the caller) — document this as a mandatory step in the ticketing system template for all MFA/credential reset requests, requiring a supervisor override with documented justification for any exception. For the SaaS access review, use the free tier of Entra ID's Access Reviews (available to all tenants) or manually query Get-MgUserAppRoleAssignment for all users and cross-reference against HR active employee list to flag orphaned or over-permissioned accounts targeted by these actors.

Evidence: For the post-incident lessons-learned record (NIST 800-61r3 §4), preserve and document: (1) The complete vishing call timeline reconstructed from help desk ticket logs, phone system CDRs (if available), and the sequence of MFA enrollment events in the IdP — this reconstruction is essential to close the social engineering vector that both CORDIAL SPIDER and SNARKY SPIDER exploit as their primary access path; (2) A before/after comparison of IdP conditional access policies and MFA enrollment records showing the attacker-introduced changes versus restored configurations; (3) The full list of SaaS applications accessed during the attacker's session window, extracted from the

Unified Audit Log or Okta System Log, to scope potential data exposure for breach notification assessment; (4) Annotated timeline mapping attacker activity to MITRE ATT&CK techniques T1556.006 (Modify Authentication Process: Multi-Factor Authentication), T1530 (Data from Cloud Storage), and T1567 (Exfiltration Over Web Service) — this mapping directly supports control gap analysis against NIST CSF Protect and Detect functions.

Detection Guidance

Focus detection on the identity and SaaS layers. No endpoint telemetry will surface these attacks. Key detection signals: (1) IdP logs showing MFA device registration events (Okta: system.mfa.factor.activate; Entra ID: 'Update user' or 'Add authentication method' audit events) not correlated with a user-initiated request ticket. (2) Session token reuse from multiple IP addresses or geolocations within a single session lifecycle, indicating token theft (T1550.001, T1539). (3) AiTM indicators: authentication success events where the source IP is a known proxy, VPN exit node, or does not match the user's historical access pattern. (4) Bulk data access or export from SharePoint, OneDrive, Google Drive, or equivalent SaaS storage (T1530) by accounts with recently changed credentials. (5) Internal SaaS messaging activity (T1534) showing mass message sends or unusual DM patterns from a compromised account. (6) Alerting and logging configuration changes (T1562.001) in SaaS admin consoles. Behavioral indicators include: help desk tickets for MFA resets followed immediately by off-hours login activity, and new OAuth app authorizations from accounts that do not typically authorize third-party apps.

Framework Mappings

MITRE-ATTACK

- **T1070.003** — Clear Command History
- **T1567** — Exfiltration Over Web Service
- **T1566.004** — Spearphishing Voice
- **T1111** — Multi-Factor Authentication Interception
- **T1621** — Multi-Factor Authentication Request Generation
- **T1556.006** — Multi-Factor Authentication
- **T1078.004** — Cloud Accounts
- **T1550.001** — Application Access Token
- **T1539** — Steal Web Session Cookie
- **T1534** — Internal Spearphishing
- **T1557** — Adversary-in-the-Middle
- **T1530** — Data from Cloud Storage
- **T1562.001** — Disable or Modify Tools

OWASP-TOP10-2021

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

NIST-800-53R5

- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)

- **AT-2** — Literacy Training and Awareness
- **SI-4** — System Monitoring

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
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

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

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
T1070.003	Clear Command History	Defense-Evasion
T1567	Exfiltration Over Web Service	Exfiltration
T1566.004	Spearphishing Voice	Initial-Access
T1111	Multi-Factor Authentication Interception	Credential-Access
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1556.006	Multi-Factor Authentication	Credential-Access
T1078.004	Cloud Accounts	Defense-Evasion
T1550.001	Application Access Token	Defense-Evasion

Technique ID	Technique Name	Tactic
T1539	Steal Web Session Cookie	Credential-Access
T1534	Internal Spearphishing	Lateral-Movement
T1557	Adversary-in-the-Middle	Credential-Access
T1530	Data from Cloud Storage	Collection
T1562.001	Disable or Modify Tools	Defense-Evasion

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

Generated 2026-05-04 13:27 UTC by TJS Security Command Center