INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-01 07:10 UTC

SaaS-Native Threat Actors CORDIAL SPIDER and SNARKY SPIDER Bypass Endpoint Defenses Through AiTM Phishing and MFA Hijacking

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0249
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Enterprise SSO/IdP platforms (generic), SaaS applications (generic), organizations using CrowdStrike Falcon Shield environments
Discovery Source	Rss:T1 Threatintel

Executive Summary

Since October 2025, two threat actor groups, CORDIAL SPIDER and SNARKY SPIDER, have conducted data theft and extortion campaigns targeting enterprise SaaS environments by intercepting credentials and hijacking identity sessions without touching endpoints. Both groups exploit SSO trust chains and identity provider flows to move laterally across connected SaaS applications, deliberately avoiding endpoint detection tools. Organizations relying primarily on EDR solutions face a structural detection gap: these attacks leave no host-based evidence, making credential theft and SaaS data exfiltration nearly invisible to traditional security monitoring.

Technical Analysis

CORDIAL SPIDER and SNARKY SPIDER operate as SaaS-native threat actors, active since at least October 2025. Both groups use adversary-in-the-middle (AiTM) phishing frameworks to intercept session tokens and credentials in transit, bypassing MFA by capturing post-authentication session cookies rather than defeating MFA directly. Techniques include voice phishing (vishing) for initial access, manipulation of MFA device registration (T1098.005, T1621) to establish persistent authentication, and abuse of SSO trust relationships to pivot across federated SaaS applications (T1078.004, T1199) without generating endpoint telemetry. Additional observed techniques span internal spearphishing (T1534), email collection via cloud APIs (T1114.003), cookie theft (T1539), application access token abuse (T1550.001), and use of hidden window artifacts (T1564.008). Relevant CWEs: CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Function), CWE-384 (Session Fixation). No CVE is assigned; this campaign exploits architectural trust weaknesses, not a

discrete software vulnerability. There is no patch; mitigation requires identity hygiene and SaaS-layer detection controls.

Action Checklist

1. Step 1: Containment, Audit active SSO sessions and MFA-registered devices across your IdP (Entra ID, Okta, Ping) immediately. Revoke suspicious sessions and unrecognized MFA devices, particularly those registered from unexpected geolocations or outside change-control windows. Prioritize privileged accounts and SaaS admin roles.
2. Step 2: Detection, Query IdP logs for anomalous MFA device registrations, impossible-travel authentication events, and SSO token reuse from new device fingerprints. Review SaaS audit logs (Microsoft 365, Google Workspace, Salesforce) for unexpected OAuth app authorizations, email forwarding rule creation (T1114.003), and bulk data access. Correlate against identity provider sign-in logs; endpoint telemetry will not surface these events.
3. Step 3: Eradication, Remove unauthorized MFA devices and OAuth application grants. Enforce conditional access policies requiring compliant, managed devices for SaaS authentication. Disable legacy authentication protocols that bypass MFA. Review and restrict SSO federation trust scope to limit lateral movement across connected SaaS applications.
4. Step 4: Recovery, Re-validate all privileged account MFA enrollments through out-of-band confirmation. Monitor IdP and SaaS audit logs continuously for 30 days post-remediation for re-registration attempts or new OAuth grants. Confirm no email forwarding rules or inbox delegation remain from the compromise window.
5. Step 5: Post-Incident, This campaign exposes a structural gap in endpoint-centric architectures. Conduct a SaaS and identity attack surface review. Implement SaaS Security Posture Management (SSPM) or equivalent IdP/SaaS-layer detection. Assess whether your current detection stack has visibility into IdP events, MFA registration changes, and OAuth grant activity; if visibility gaps exist, prioritize architectural control investment (SSPM or equivalent SaaS-layer tooling), not configuration-only remediation.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to legal counsel and initiate breach notification assessment immediately if investigation confirms that CORDIAL SPIDER or SNARKY SPIDER accessed mailboxes, cloud storage, or SaaS applications containing PII, PHI, or regulated financial data, as bulk data access via hijacked OAuth tokens and email forwarding rules (T1114.003) is a confirmed exfiltration vector for both groups and likely triggers GDPR 72-hour notification, HIPAA Breach Notification Rule, or SEC Material Cybersecurity Incident reporting depending on data classification and organizational profile.

Recovery Notes	Re-validate the integrity of SSO federation trusts and OAuth application grant tables weekly for the first 30 days post-remediation, as both CORDIAL SPIDER and SNARKY SPIDER have demonstrated persistence through re-registration of adversary-controlled MFA devices and re-authorization of malicious OAuth apps following initial remediation. Confirm that Entra ID or Okta diagnostic log streaming is fully operational and that retention covers at least 90 days before closing the incident, since the October 2025 campaign start date indicates these actors operate with long dwell times that exceed default 30-day IdP log retention windows. Verify that all SaaS application admin consoles (Microsoft 365, Google Workspace, Salesforce) have been audited for backdoor admin account creation or delegated access grants independent of the primary IdP, as SaaS-native admin access can survive IdP-level remediation.
Forensic Artifacts	Entra ID Sign-In Logs (Graph API 'auditLogs/signIns'): preserve the 'deviceDetail.deviceId', 'deviceDetail.browser', 'tokenIssuerType', and 'mfaDetail.authMethod' fields — AiTM proxy sessions used by CORDIAL SPIDER and SNARKY SPIDER produce sign-in records where a valid MFA claim is present but the device ID is unrecognized and the IP is a residential proxy or VPN exit node, creating a detectable fingerprint against the legitimate user's historical device baseline. | Okta System Log (API '/api/v1/logs'): events of type 'user.mfa.factor.activate', 'user.session.start', and 'policy.evaluate_sign_on' timestamped from October 2025 onward — specifically, MFA factor activations where the enrolling IP differs from the user's established authentication geography, indicating adversary-controlled device registration during a hijacked session. | Microsoft 365 Unified Audit Log — 'New-InboxRule' and 'Set-InboxRule' operations: CORDIAL SPIDER and SNARKY SPIDER create inbox forwarding rules (MITRE T1114.003) as a persistence and exfiltration mechanism post-SSO compromise; preserve the full rule definition including ForwardTo, RedirectTo, and MarkAsRead parameters, which reveal the external collection address and confirm whether the actor intended silent exfiltration. | OAuth Application Grant Records (Entra 'Get-MgOauth2PermissionGrant' and 'Get-MgServicePrincipalAppRoleAssignment'): snapshot the full grant table including appId, consentType, scope, and principalId at time of discovery — both groups authorize malicious or over-privileged OAuth apps during the compromised session to maintain SaaS access independently of the IdP session, and the grant table is the primary artifact establishing cross-SaaS lateral movement scope. | SaaS Audit Logs — Salesforce Event Log Files and Google Workspace Token Audit Log: Salesforce '/services/data/vXX.0/sobjects/EventLogFile' entries for 'Report', 'ReportExport', and 'API' event types reveal bulk data access consistent with the exfiltration phase of SNARKY SPIDER and CORDIAL SPIDER campaigns; Google Workspace token audit events with 'token_revoke' actions absent despite active forwarding rules indicate the OAuth grant persisted through the compromise window and must be correlated with Drive access logs for exfiltration scope assessment.

Per-Action IR Details

Step 1: Containment — Audit active SSO sessions and MFA-registered devices across your IdP (Entra ID, Okta, Ping) immediately. Revoke suspicious sessions and unrecognized MFA devices, particularly those registered from unexpected geolocations or outside change-control windows. Prioritize privileged accounts and SaaS admin roles.

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: In Entra ID: run 'Get-MgUserAuthenticationMethod -UserId ' via Microsoft Graph PowerShell to enumerate all registered MFA methods per account; export with 'Get-MgAuditLogSignIn' filtered on 'riskState eq atRisk'

or 'isRisky eq true'. In Okta: use the Okta System Log API endpoint '/api/v1/logs?filter=eventType+eq+"user.mfa.factor.activate"' scoped to the incident window, then cross-reference against your change-control calendar manually. Session revocation in Entra: 'Revoke-MgUserSignInSession -UserId '; in Okta: POST to '/api/v1/users/{userId}/sessions?oauthTokens=true' with DELETE method. A 2-person team should divide: one works privileged/admin accounts, the other SaaS-connected service accounts.

Evidence: Preserve BEFORE revoking sessions: full Entra ID sign-in log export for the last 90 days (Microsoft Graph 'auditLogs/signIns', retention limit is 30 days for non-P2 tenants — export immediately to Azure Storage or CSV); Okta System Log export covering all 'user.authentication.sso', 'user.mfa.factor.activate', and 'policy.evaluate_sign_on' events; screenshot or API export of all currently active sessions including device ID, IP, user-agent string, and geolocation for every privileged account. Capture MFA device registration timestamps — CORDIAL SPIDER and SNARKY SPIDER register adversary-controlled MFA devices during the AiTM session hijack window, so registration events timestamped during the identified phishing campaign period (October 2025 onward) are primary forensic anchors.

Step 2: Detection — Query IdP logs for anomalous MFA device registrations, impossible-travel authentication events, and SSO token reuse from new device fingerprints. Review SaaS audit logs (Microsoft 365, Google Workspace, Salesforce) for unexpected OAuth app authorizations, email forwarding rule creation (T1114.003), and bulk data access. Correlate against identity provider sign-in logs — endpoint telemetry will not surface these events.

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: Microsoft 365 — use the Unified Audit Log via 'Search-UnifiedAuditLog -RecordType ExchangeAdmin -Operations "New-InboxRule","Set-InboxRule"' to surface T1114.003 email forwarding rules; also query '-RecordType AzureActiveDirectory -Operations "Add service principal credentials","Consent to application"' for OAuth grants. Google Workspace — pull Admin SDK Reports API for 'login' and 'token' event types filtering on 'is_suspicious:true'. For impossible-travel detection without SIEM: export Entra sign-in logs to CSV and use a PowerShell script calculating time-delta and geolocation-distance between consecutive authentications per UPN — flag any delta under 2 hours with distance over 500 miles. Apply the public Sigma rule 'azure_ad_mfa_device_registration_from_new_country.yml' (available in SigmaHQ repository) against exported logs using 'sigma convert' with a grep/jq backend. MITRE ATT&CK T1114.003 (Email Forwarding Rule), T1550.001 (Application Access Token), T1606.002 (SAML Token forgery) should frame hunting queries.

Evidence: Capture before analysis is complete: raw Entra ID sign-in JSON exports (preserve 'deviceDetail.deviceId', 'deviceDetail.browser', 'location.countryOrRegion', 'conditionalAccessStatus', 'mfaDetail.authMethod' fields — these fingerprint AiTM proxy sessions where the intercepted token is replayed from a new device ID); Microsoft 365 Unified Audit Log entries for 'MailboxLogin', 'New-InboxRule', and 'ModifyFolderPermissions' operations correlated to accounts flagged in Step 1; Salesforce event log files ('/services/data/vXX.0/sobjects/EventLogFile') for 'Login', 'URI', and 'API' event types showing bulk object access or report exports; OAuth application grant records from Entra 'servicePrincipalSignIns' and Google Workspace token audit log showing app name, scope, and grant timestamp.

Step 3: Eradication — Remove unauthorized MFA devices and OAuth application grants. Enforce conditional access policies requiring compliant, managed devices for SaaS authentication. Disable legacy authentication protocols that bypass MFA. Review and restrict SSO federation trust scope to limit lateral movement across connected SaaS applications.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: MFA device removal in Entra: 'Remove-MgUserAuthenticationMethod -UserId -AuthenticationMethodId ' for each unauthorized FIDO2 key, authenticator app registration, or phone number added

outside the change window. OAuth grant revocation: 'Remove-MgServicePrincipalAppRoleAssignment' and 'Revoke-MgOauth2PermissionGrant' for all non-approved app grants identified in Step 2. Legacy auth blocking without Entra P1: create an Entra Conditional Access policy (available in free tier for blocking legacy auth) targeting 'Exchange ActiveSync Clients' and 'Other Clients' with block grant control. SSO federation scope restriction: in Entra, audit app registrations via 'Get-MgServicePrincipal -All | Where-Object {$_.ReplyUrls -ne $null}' and remove redirect URIs for unrecognized external tenants. Document every removed artifact with timestamp for chain-of-custody.

Evidence: Before executing eradication, preserve: a full export of the OAuth application grant table from Entra ('Get-MgOauth2PermissionGrant -All' to CSV) and Okta application assignments API response — these establish the post-compromise application trust state that CORDIAL SPIDER and SNARKY SPIDER leverage for cross-SaaS lateral movement; Entra Conditional Access policy evaluation logs (sign-in log field 'appliedConditionalAccessPolicies') showing which policies were in place and which were bypassed during the attack window; Okta System Log entries for 'application.lifecycle.update' and 'user.session.access_admin_app' events showing SaaS application access chains used for lateral movement.

Step 4: Recovery — Re-validate all privileged account MFA enrollments through out-of-band confirmation. Monitor IdP and SaaS audit logs continuously for 30 days post-remediation for re-registration attempts or new OAuth grants. Confirm no email forwarding rules or inbox delegation remain from the compromise window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 6.5 (Require MFA for Administrative Access), CIS 6.1 (Establish an Access Granting Process)

Compensating: Out-of-band MFA re-enrollment: generate a Temporary Access Pass (TAP) in Entra ID for each privileged account ('New-MgUserAuthenticationTemporaryAccessPass') and walk each account owner through re-enrollment on a confirmed managed device via in-person or video-verified session — do not use email for this communication as inbox access may still be compromised. For 30-day continuous monitoring without SIEM: configure Entra ID diagnostic settings to stream sign-in and audit logs to an Azure Storage Account (free tier sufficient for log storage); run a daily scheduled PowerShell task querying 'Get-MgAuditLogSignIn' for 'user.mfa.factor.activate' and 'appId' values not in your approved OAuth app allowlist, outputting alerts to a shared mailbox. For email rule verification: 'Get-InboxRule -Mailbox | Select-Object Name,ForwardTo,RedirectTo,DeleteMessage,Enabled' across all affected mailboxes; repeat weekly for 30 days.

Evidence: Capture as recovery baseline: a clean-state export of all MFA registrations post-re-enrollment ('Get-MgUserAuthenticationMethod -UserId ' for all privileged accounts) to serve as the verified baseline for future comparison; Microsoft 365 'Get-InboxRule' output for all affected accounts confirming zero forwarding rules, to be retained as the remediation-complete artifact; Entra audit log entry for each TAP issuance and subsequent MFA re-registration event, establishing the verified re-enrollment chain of custody required under NIST IR-5 (Incident Monitoring).

Step 5: Post-Incident — This campaign exposes a structural gap in endpoint-centric architectures. Conduct a SaaS and identity attack surface review. Implement SaaS Security Posture Management (SSPM) or equivalent IdP/SaaS-layer detection. Evaluate whether your current detection stack has visibility into IdP events, MFA registration changes, and OAuth grant activity — if not, that gap requires a control investment, not a configuration change.

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 RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: For teams who cannot procure a commercial SSPM tool: implement free detection coverage using (1) Microsoft Sentinel free ingestion tier for Entra ID and Microsoft 365 logs with the community Sigma-to-KQL ruleset from the 'Azure-Sentinel' GitHub repository, specifically rules targeting 'AiTM phishing' and 'OAuth consent grant' patterns;

(2) Okta's free System Log with a lightweight Python polling script using the Okta SDK to alert on 'user.mfa.factor.activate' outside business hours or from new countries; (3) a quarterly manual SaaS application grant audit using 'Get-MgOauth2PermissionGrant' cross-referenced against an approved-app allowlist maintained in a shared spreadsheet. Lessons-learned session should specifically address the CORDIAL SPIDER and SNARKY SPIDER TTPs of AiTM credential interception and SSO trust chain abuse — document detection gaps that allowed initial access to persist undetected and assign control owners for each gap.

Evidence: Post-incident documentation artifacts required: a timeline reconstruction of the full attack chain from initial AiTM phishing lure through SSO session hijack, MFA device registration, OAuth grant, and SaaS lateral movement — sourced from IdP log exports preserved in Steps 1-4; a control gap analysis document mapping where CORDIAL SPIDER and SNARKY SPIDER TTPs (T1114.003, T1550.001, T1606.002) were not covered by existing detection controls; Entra ID and Okta log retention confirmation showing whether pre-incident logs were available for the October 2025 campaign start date — log retention gaps are a finding requiring remediation under NIST AU-11 (Audit Record Retention).

Detection Guidance

Detection for these campaigns requires IdP and SaaS-layer telemetry; endpoint logs will not surface activity. Key detection signals: (1) MFA device registrations outside approved change windows or from unexpected IP ranges, query Entra ID/Okta system logs for 'device enrollment' or 'authenticator registered' events; (2) SSO token use from a device fingerprint or IP that differs from the authentication session origin, indicating possible session cookie hijacking (CWE-384); (3) OAuth application grants added to user accounts, especially those with mail read or file access scopes; (4) Email forwarding rules created via EWS, Graph API, or admin console (T1114.003), query Exchange Online or Google Workspace admin audit logs; (5) Impossible-travel events in IdP sign-in logs within the same session; (6) Vishing precursors: help desk tickets requesting MFA resets or device re-enrollment, particularly for privileged accounts. MITRE techniques to map detection rules against: T1621 (MFA Request Generation), T1098.005 (Device Registration), T1539 (Cookie Theft), T1114.003 (Email Forwarding), T1078.004 (Cloud Accounts).

Framework Mappings

MITRE-ATTACK

- **T1534** — Internal Spearphishing
- **T1566** — Phishing
- **T1098.005** — Device Registration
- **T1621** — Multi-Factor Authentication Request Generation
- **T1556.006** — Multi-Factor Authentication
- **T1566.004** — Spearphishing Voice
- **T1557** — Adversary-in-the-Middle
- **T1539** — Steal Web Session Cookie
- **T1078** — Valid Accounts
- **T1078.004** — Cloud Accounts
- **T1114.003** — Email Forwarding Rule
- **T1550.001** — Application Access Token
- **T1199** — Trusted Relationship

- **T1564.008** — Email Hiding Rules

NIST-800-53R5

- **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
- **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)

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
- **CC9.2** — Manages risks associated with vendors and business partners

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.5.21** — Managing information security in the ICT supply chain
- **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
T1566	Phishing	Initial-Access
T1098.005	Device Registration	Persistence
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1556.006	Multi-Factor Authentication	Credential-Access
T1566.004	Spearphishing Voice	Initial-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1078.004	Cloud Accounts	Defense-Evasion
T1114.003	Email Forwarding Rule	Collection
T1550.001	Application Access Token	Defense-Evasion
T1199	Trusted Relationship	Initial-Access
T1564.008	Email Hiding Rules	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/falcon-intelligence-recon-an...	T3
	https://www.crowdstrike.com/en-us/blog/pit-stop-vs-pit-wall-teamwor...	T3
SaaS Security Risk Review - CrowdStrike	https://www.crowdstrike.com/en-us/platform/falcon-shield/saas-secur...	T3
Lightboard Lab: Preventing SaaS Breaches with Falcon Shield	https://www.youtube.com/watch?v=Z1a-MffPK-c	T3

Generated 2026-05-01 07:10 UTC by TJS Security Command Center