INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-27 18:50 UTC

ShinyHunters SSO-to-SaaS Campaign Confirms 5.5M ADT Records Exposed, Pattern Points to Systemic Enterprise Risk

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0228
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	ADT (home security platform), Okta (SSO identity provider), Salesforce (CRM/data store)
Published	2026-04-27T10:43:11
Discovery Source	Rss

Executive Summary

On April 20, 2026, threat actor ShinyHunters compromised an ADT employee's Okta SSO account via a vishing attack, then used that session to exfiltrate records on approximately 5.5 million individuals from ADT's Salesforce environment. When ADT declined to pay ransom, ShinyHunters publicly released an 11GB archive; Have I Been Pwned has confirmed the breach scale. The same Okta-to-SaaS attack pattern has hit multiple enterprise targets including McGraw Hill, the European Commission, and Medtronic, meaning any organization running Okta-federated SaaS without phishing-resistant MFA is an active target.

Technical Analysis

No CVE is associated with this breach. The attack relied entirely on social engineering and session abuse, not a software vulnerability. Because no CVE exists, vulnerability scanners will not surface this threat, and detection depends entirely on identity and behavioral controls. Attack chain: (1) ShinyHunters conducted a vishing attack against an ADT employee, harvesting Okta credentials or inducing the target to approve an MFA push (T1566.004, T1598). (2) The actor used the hijacked SSO session to authenticate into ADT's Salesforce instance as a legitimate user (T1078, T1078.004, Valid Accounts: Cloud Accounts). (3) Data on ~5.5 million individuals including PII was exfiltrated from Salesforce (T1530, Data from Cloud Storage; T1213, Data from Information Repositories). (4) Exfiltration occurred via standard SaaS data export mechanisms (T1567, Exfiltration Over Web Service). (5) When ransom was refused, data was publicly leaked (T1657, Financial Extortion). Relevant CWEs: CWE-287 (Improper Authentication), CWE-522 (Insufficiently Protected Credentials), CWE-359 (Exposure of Private Personal Information), CWE-732 (Incorrect Permission

Assignment). No patch exists; mitigation is architectural and procedural.

Action Checklist

1. Containment: Review all Okta SSO sessions active in the last 30 days for anomalous access patterns: off-hours logins, new device fingerprints, impossible travel, or first-time access to Salesforce or other high-value SaaS. Revoke suspicious sessions immediately via Okta Admin Console > Sessions. Temporarily restrict Salesforce API access and bulk data export permissions to named, approved accounts only.
2. Detection: Query Okta System Log for MFA push approval events preceded by failed password attempts or unusual user-agent strings (event types: 'user.authentication.sso', 'policy.evaluate_sign_on', 'user.mfa.okta_verify.deny_push'). In Salesforce, review Setup Audit Trail and Event Monitoring logs for bulk report runs, data export requests, or API calls exporting >10,000 records. Behavioral indicators: SSO login from a new IP followed immediately by a Salesforce data export within the same session.
3. Eradication: Replace SMS and push-based MFA with phishing-resistant authenticators (FIDO2/WebAuthn hardware keys or passkeys) for all Okta users with access to Tier 1 SaaS environments. Enforce number matching and additional context in Okta Verify if hardware tokens are not yet deployed. Remove or restrict Salesforce data export, report download, and bulk API permissions from all non-essential accounts via Salesforce Permission Sets.
4. Recovery: After session revocation and MFA hardening, validate Salesforce Connected Apps to confirm no unauthorized OAuth grants persist (Setup > Connected Apps > OAuth Usage). Re-baseline expected Okta login patterns and set alert thresholds in your SIEM. Confirm that Salesforce Event Monitoring is forwarding to your SIEM and that alert rules for bulk export events are active and tested.
5. Post-Incident: Conduct targeted vishing simulation exercises against employees with Okta access to high-value SaaS. Review your identity security architecture against NIST SP 800-63B AAL2/AAL3 requirements and CISA's Phishing-Resistant MFA guidance (CISA Fact Sheet: Implementing Phishing-Resistant MFA). Map identity provider access paths to SaaS applications and enforce least-privilege access; this attack exposed over-permissioned SSO-to-SaaS trust relationships as a systemic control gap.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if: (1) Okta System Log evidence confirms a successful SSO session was established from a non-baseline IP with Salesforce access in the last 30 days; (2) Salesforce EventLogFile shows any ReportExport or RestApi event with ROWS_PROCESSED exceeding 10,000 from a session not attributed to an authorized service account; or (3) the organization holds PII on residents of states with breach notification statutes (all 50 US states) or EU data subjects under GDPR, as the 5.5M-record scale of the ShinyHunters exfiltration pattern triggers mandatory notification timelines in most jurisdictions.

Recovery Notes	After session revocation, MFA hardening, and OAuth grant cleanup, maintain elevated monitoring of Okta SSO and Salesforce Event Monitoring logs for a minimum of 90 days — ShinyHunters has demonstrated persistence across multiple enterprise targets and may re-attempt via a secondary compromised credential or a rogue OAuth application registered during the initial session. Validate weekly that no new Salesforce Connected Apps have been added and that FIDO2 enrollment rates for Tier 1 SaaS users are at 100% before reducing monitoring frequency. Confirm that the 11GB archive released publicly by ShinyHunters does not contain credentials or session tokens that could enable secondary compromise of related third-party integrations (cross-reference exposed email domains against your Okta user directory and force password resets for any matches).
Forensic Artifacts	Okta System Log (JSON export via GET /api/v1/logs) — preserves the vishing-assisted MFA push approval sequence, including 'user.mfa.okta_verify.deny_push' events immediately preceding the successful 'user.authentication.auth_via_mfa' event, with originating IP, raw user-agent, device fingerprint, and external session ID that chains to the Salesforce exfiltration session. | Salesforce EventLogFile records for event types 'Login', 'ReportExport', 'RestApi', and 'DataExport' — documents the specific REPORT_IDs accessed, ROWS_PROCESSED counts, and SESSION_KEY values that map the Okta-issued SAML assertion to the bulk data exfiltration of 5.5M records from ADT's Salesforce CRM objects. | Salesforce Setup Audit Trail (Setup > Audit Trail > Download, 180-day retention) — captures any administrative changes made during the compromised session, including Permission Set modifications, Connected App registrations, or Profile changes that ShinyHunters may have made to establish persistence or expand access beyond the initial compromised account. | Okta Connected App OAuth grant list (GET /api/v1/apps/{salesforce-app-id}/grants) — identifies whether the compromised session was used to authorize a rogue OAuth application for persistent access to Salesforce data after the primary session was terminated or the password was reset. | Network perimeter or proxy logs filtered on Salesforce API endpoints (*.salesforce.com/services/data/ and *.salesforce.com/services/async/) during the breach window — captures the volume, timing, and destination IPs of the data exfiltration egress traffic, which for an 11GB archive will produce anomalous outbound throughput spikes attributable to a single source IP not matching ADT's corporate egress ranges.

Per-Action IR Details

Containment — Audit all Okta SSO sessions active in the last 30 days for anomalous access patterns: off-hours logins, new device fingerprints, impossible travel, or first-time access to Salesforce or other high-value SaaS. Revoke suspicious sessions immediately via Okta Admin Console > Sessions. Temporarily restrict Salesforce API access and bulk data export permissions to named, approved accounts only.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST SI-4 (System Monitoring), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without a SIEM, run the Okta System Log API directly via curl or PowerShell to pull session records for the last 30 days filtered by 'user.session.start' events: `Invoke-RestMethod -Uri 'https:///api/v1/logs?filter=eventType+eq+"user.session.start"&since=' -Headers @{Authorization='SSWS '}`. Pipe output to a CSV and sort by client.geographicalContext.country and client.device to surface new geos or device types. For Salesforce, use the free Salesforce CLI (sf) to query the EventLogFile object: `sf data query --query "SELECT LogDate, LogFile FROM EventLogFile WHERE EventType='Login' AND LogDate = LAST_N_DAYS:30" --target-org ` and download for manual review. Restrict Salesforce bulk API by editing Permission Sets via Setup > Permission Sets > [set name] > System Permissions — uncheck 'API Enabled' and 'Export Reports' for all non-essential accounts.

Evidence: Before revoking sessions, export the full Okta System Log for the last 30 days in JSON format via the Okta API (GET /api/v1/logs) and preserve locally — this is your authoritative record of ShinyHunters' vishing-compromised session activity, including the originating IP, user-agent, device token, and MFA push approval timestamp for the compromised ADT employee account. From Salesforce, capture the Setup Audit Trail (Setup > Audit Trail > Download) and the EventLogFile records for 'Login', 'ReportExport', 'DataExport', and 'RestApi' event types covering the breach window, as these will document the session used to stage and exfiltrate the 5.5M records. Preserve all evidence in write-protected, timestamped storage before session revocation destroys live session metadata.

Detection — Query Okta System Log for MFA push approval events preceded by failed password attempts or unusual user-agent strings (event types: 'user.authentication.sso', 'policy.evaluate_sign_on', 'user.mfa.okta_verify.deny_push'). In Salesforce, review Setup Audit Trail and Event Monitoring logs for bulk report runs, data export requests, or API calls exporting >10,000 records. Behavioral indicators: SSO login from a new IP followed immediately by a Salesforce data export within the same session.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use the free Sigma rule converter (sigmac or pySigma) to translate Okta-specific Sigma rules against exported Okta logs in JSON format — search GitHub for 'SigmaHQ okta vishing' or 'okta mfa fatigue' rules targeting 'user.mfa.okta_verify.deny_push' followed within 60 seconds by 'user.authentication.sso'. For Salesforce event correlation, download EventLogFile CSVs for the 'RestApi' and 'ReportExport' types and run a Python or PowerShell join on Session_Key to correlate the Okta login timestamp with Salesforce export timestamps in the same session — any session showing >10,000 rows_processed in RestApi logs within 10 minutes of an Okta SSO event from a new IP is a confirmed indicator. Free Splunk (500MB/day free tier) can ingest both log sets for correlation if available.

Evidence: The primary forensic artifact for ShinyHunters' Okta vishing technique is the sequence of Okta event types in the System Log: look for 'user.mfa.okta_verify.deny_push' (victim rejected push) followed by a second or third 'user.mfa.okta_verify.deny_push' within minutes, then a successful 'user.authentication.auth_via_mfa' — this is the MFA fatigue or vishing-assisted push approval signature. In Salesforce EventLogFile, the exfiltration of 5.5M records will appear as RestApi events with high ROWS_PROCESSED values or multiple ReportExport events with REPORT_ID values pointing to customer data objects (Contact, Lead, Account), all sharing a single SESSION_KEY that maps back to the Okta-issued SAML session. Capture the Okta 'actor.id', 'client.ipAddress', 'client.userAgent.rawUserAgent', and 'authenticationContext.externalSessionId' fields from the suspicious authentication event — these link the vishing call's SSO session to the Salesforce exfiltration chain.

Eradication — Replace SMS and push-based MFA with phishing-resistant authenticators (FIDO2/WebAuthn hardware keys or passkeys) for all Okta users with access to Tier 1 SaaS environments. Enforce number matching and additional context in Okta Verify if hardware tokens are not yet deployed. Remove or restrict Salesforce data export, report download, and bulk API permissions from all non-essential accounts via Salesforce Permission Sets.

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-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams that cannot immediately procure FIDO2 hardware keys, enforce Okta FastPass with number matching and user additional context enabled immediately (Okta Admin Console > Security > Authenticators > Okta Verify > Edit — enable 'Number Challenge' and 'Show Push Notification Context'). Document hardware key procurement as a tracked remediation item with a 30-day deadline. For Salesforce permission cleanup without a paid DLP tool, use the free Salesforce Permission Set Analyzer or run a SOQL query via the Developer Console: `SELECT Id, Name, PermissionsExportReport, PermissionsBulkApiHardDelete FROM PermissionSet WHERE

PermissionsExportReport = true` to enumerate all permission sets with export rights, then revoke them from non-essential users via Setup > Permission Set Assignments. Generate a before/after permission matrix as evidence of remediation.

Evidence: Before modifying Okta authenticator policies, export the current Okta policy configuration via the Okta Policy API (GET /api/v1/policies?type=MFA_ENROLL) and preserve as a baseline — this documents the weakened push-based MFA posture that ShinyHunters exploited via vishing. From Salesforce, export the full Permission Set assignment list before revoking export rights (SOQL: `SELECT AssigneeId, Assignee.Name, PermissionSetId, PermissionSet.Name FROM PermissionSetAssignment WHERE PermissionSet.PermissionsExportReport = true`) to establish a forensic record of over-permissioned accounts that had bulk export access during the breach window. These two artifacts demonstrate the systemic over-trust in SSO-to-SaaS access paths that enabled the 5.5M record exfiltration.

Recovery — After session revocation and MFA hardening, validate Salesforce Connected Apps to confirm no unauthorized OAuth grants persist (Setup > Connected Apps > OAuth Usage). Re-baseline expected Okta login patterns and set alert thresholds in your SIEM. Confirm that Salesforce Event Monitoring is forwarding to your SIEM and that alert rules for bulk export events are active and tested.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: Without an enterprise SIEM, configure free Grafana + Loki or the ELK stack (free tier) to ingest Okta System Log via the Okta Log Streaming feature (Okta Admin Console > Reports > Log Streaming) — this provides a persistent, queryable log store without a commercial license. For Salesforce Connected Apps, enumerate OAuth grants via SOQL: `SELECT AppName, UserId, User.Name, LastUsedDate, InstalledLocation FROM ConnectedApplication` and flag any AppName not in your authorized app inventory. Create a manual alert by scheduling a daily PowerShell or Python script that queries the Okta API for 'user.authentication.sso' events where client.geographicalContext differs from the user's baseline country, and emails results to the security team — this replicates impossible-travel detection without a SIEM.

Evidence: Before closing the recovery phase, capture a final snapshot of Okta Connected App OAuth token grants via the Okta API (GET /api/v1/apps/{appId}/grants) for all Salesforce-connected applications — ShinyHunters or a persistence mechanism could have registered a rogue OAuth app during the compromised session to maintain access after password reset. Pull the Salesforce Setup Audit Trail one final time post-remediation and compare against the breach-window version to confirm no additional administrative changes (profile edits, connected app additions, permission set changes) were made by the compromised session that were not yet reverted. Retain both the pre- and post-remediation Okta policy exports and Salesforce permission matrices for regulatory breach notification documentation.

Post-Incident — Conduct targeted vishing simulation exercises against employees with Okta access to high-value SaaS. Review your identity security architecture against NIST SP 800-63B AAL2/AAL3 requirements and CISA's Phishing-Resistant MFA guidance (CISA Fact Sheet: Implementing Phishing-Resistant MFA). Map identity provider access paths to SaaS applications and enforce least-privilege access; this attack exposed over-permissioned SSO-to-SaaS trust relationships as a systemic control gap.

NIST Phase: Post Incident

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

Controls: NIST IR-2 (Incident Response Training), NIST IR-3 (Incident Response Testing), NIST IR-8 (Incident Response Plan), NIST IA-2 (Identification and Authentication — Organizational Users), NIST RA-3 (Risk Assessment), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Conduct a tabletop vishing simulation using GoPhish (free, open source) configured for voice/callback pretexting scenarios — script the scenario around an attacker impersonating IT helpdesk requesting Okta push approval, which mirrors the ShinyHunters vishing technique used against ADT. Use free Okta Expression Language

policies (in Okta Admin Console > Security > Sign-On Policies) to enforce FIDO2-only authentication for users whose SCIM profile maps to Salesforce high-data-volume Permission Sets, implementing a manual version of risk-based access control. For identity path mapping, build a free spreadsheet-based SSO-to-SaaS dependency matrix: enumerate all Okta application assignments (GET /api/v1/apps?limit=200) and cross-reference against Salesforce Profile and Permission Set assignments to identify all accounts with both SSO federation and bulk export rights — this is the systemic over-permission map that this attack exploited.

Evidence: The post-incident lessons-learned package for this ShinyHunters campaign should include: (1) the Okta System Log excerpt documenting the vishing-assisted MFA push approval sequence as a training artifact for future social engineering detection; (2) the before-remediation Salesforce permission matrix showing which accounts held bulk export rights, quantifying the blast radius of a single compromised Okta identity; (3) the timeline correlation between the compromised SSO session and the Salesforce data export events, demonstrating the seconds-to-exfiltration window that makes SSO-to-SaaS attacks uniquely high-velocity. These three artifacts directly support the post-incident report, regulatory breach notification (state PII notification laws triggered by 5.5M records), and the architectural remediation case for FIDO2 investment.

Detection Guidance

Primary detection surface is Okta System Log and Salesforce Event Monitoring forwarded to your SIEM. Key Okta query targets: 'user.authentication.sso' events with new device or new IP context; 'user.mfa.okta_verify.approve' events following a failed password attempt; 'policy.evaluate_sign_on' events that resolve to allow from an unusual geolocation. Key Salesforce detection targets: Event Monitoring 'ReportExport' and 'ListViewExport' event types with record counts exceeding normal baseline; 'ApiTotalUsage' spikes on accounts not typically using the API; Setup Audit Trail entries for permission changes made during the suspicious session window. Behavioral IOC pattern: Okta SSO authentication from a previously unseen IP or device fingerprint, followed within minutes by a Salesforce bulk report export or API data pull, this sequence is the core attack signature. No public IOCs (IPs, domains, hashes) have been confirmed and attributed to this specific campaign at this time; do not treat absence of IOCs as clearance.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs publicly attributed to this campaign at time of writing`	ShinyHunters has not had specific IPs, domains, or file hashes publicly attributed to this ADT campaign in available sources. Do not treat absence as clearance.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078.004** — Cloud Accounts
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage
- **T1657** — Financial Theft
- **T1567** — Exfiltration Over Web Service

- **T1213** — Data from Information Repositories
- **T1539** — Steal Web Session Cookie
- **T1566.004** — Spearphishing Voice
- **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
- **AC-3** — Access Enforcement
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design

CIS-V8

- **3.3** — Configure Data Access Control Lists
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.2** — Use Unique Passwords
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

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)(ii)(D)** — Password Management
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078.004	Cloud Accounts	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1657	Financial Theft	Impact
T1567	Exfiltration Over Web Service	Exfiltration
T1213	Data from Information Repositories	Collection
T1539	Steal Web Session Cookie	Credential-Access
T1566.004	Spearphishing Voice	Initial-Access
T1598	Phishing for Information	Reconnaissance

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/home-security-giant-...	T3
	https://www.bleepingcomputer.com/news/security/home-security-giant-...	T3
	https://www.bleepingcomputer.com/news/security/data-breach-at-edtec...	T3
	https://www.bleepingcomputer.com/news/security/cloudflare-hacked-us...	T3
ShinyHunters Vishing-to-Salesforce Chain Hits ADT: SSO Compr	https://techjacksolutions.com/scc-intel/shinyhunters-vishing-to-sal...	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 2026-04-27 18:50 UTC by TJS Security Command Center