مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Widespread Data Theft Campaign Targeting Salesforce via Salesloft Drift Integrations

Tracking #:432317670

Date-03-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers reported a large-scale campaign of data theft targeting Salesforce customer instances via compromised OAuth tokens associated with the Salesloft Drift third-party application.

TECHNICAL DETAILS:

Google Threat Intelligence Group (GTIG) and Mandiant Incident Response have observed a large-scale campaign of data theft targeting Salesforce customer instances via compromised OAuth tokens associated with the Salesloft Drift third-party application.

The threat activity, attributed to the actor UNC6395, took place between August 8–18, 2025 and has since expanded beyond Salesforce, impacting other Salesloft Drift integrations, including Drift Email.

Attackers systematically exported corporate Salesforce data (e.g., Accounts, Opportunities, Users, Cases) and harvested sensitive credentials (e.g., AWS Keys, Snowflake access tokens, and passwords). Investigations confirmed that UNC6395 also used compromised OAuth tokens to access a limited number of Google Workspace email accounts integrated with Drift Email.

While Salesforce's core platform and Google Workspace were not compromised, the abuse of third-party integrations created pathways for widespread data exposure. Immediate action is required by all organizations using Drift integrations.

Key Findings:

- Threat Actor: UNC6395
- Initial Access: Compromised OAuth tokens associated with Salesloft Drift integrations.
- Scope of Impact: Salesforce, Drift Email, and potentially other third-party integrations with Drift.
- Data Targeted:
  - Salesforce data objects (Accounts, Opportunities, Users, Cases).
  - Credentials/Secrets (AWS access keys, Snowflake tokens, API keys, and passwords).
- Operational Tactics:
  - SOQL queries against Salesforce objects.
  - Exfiltration of high-value secrets.
  - Efforts at operational security (deleting queries after execution).
  - Use of Tor exit nodes for anonymity.
- Timeline:
  - Aug 8–18, 2025: Data theft campaign active.
  - Aug 20, 2025: Salesforce & Salesloft revoked all Drift-related tokens, Drift removed from AppExchange.
  - Aug 28, 2025: GTIG confirmed Drift Email OAuth compromises.

Threat Queries Observed

- Enumerating Salesforce object counts:
  - SELECT COUNT() FROM Account;
  - SELECT COUNT() FROM Opportunity;
  - SELECT COUNT() FROM User;

- SELECT COUNT() FROM Case;
- Retrieving sensitive fields from the User object, including:
  - Id, Username, Email, Name, Title, Department, Phone, LastLoginDate
- Exfiltrating Case data at scale:
  - SELECT Id, CaseNumber, ... FROM Case LIMIT 10000

Multiple major cybersecurity vendors—including SpyCloud, Zscaler, Palo Alto Networks, Cloudflare, Pagerduty, Tanium, and Tenable—have publicly confirmed impact from the Salesloft Drift incident, which exploited OAuth tokens to access Salesforce data via third-party integrations

RECOMMENDATIONS:

Organizations with any Salesloft Drift integrations are advised to operate under the assumption that data and secrets have been compromised. Critical steps should be immediately implemented:

1. Investigate for Compromise
- Review all third-party integrations linked to Drift in the Drift Admin console.
- In Salesforce, audit:
  - Event Monitoring logs for anomalous Drift-connected activity.
  - UniqueQuery events logging executed SOQL queries.
  - Authentication events associated with Drift's Connected App.
- Search exfiltrated data for leaks of secrets:
  - AWS keys (AKIA identifiers).
  - Snowflake credentials (snowflakecomputing.com).
  - Keywords: password, secret, key.
  - VPN or SSO login URLs.
- Run secret scanning tools (e.g., Trufflehog) across integrated systems.
- Check for activity originating from Tor exit nodes or suspicious User-Agent strings shared in IOCs.

2. Revoke and Rotate Credentials
- Immediately revoke OAuth tokens, API keys, and access tokens associated with Drift integrations.
- Rotate all discovered sensitive credentials across impacted systems.
- Reset user account passwords, particularly admin or integration accounts.
- For Google Workspace users integrated with Drift Email:
  - Confirm OAuth tokens have been properly revoked.
  - Audit message read/access logs during August 2025.

3. Harden Access Controls
- Restrict Application Scopes: Ensure Drift and third-party apps only get minimum required permissions. Avoid broad full access scopes.
- Enforce IP Restrictions:
  - Set Connected Apps to enforce trusted IP ranges.
  - Configure user profiles to restrict login IPs.
- Limit API Exposure: Remove "API Enabled" permissions from unnecessary profiles. Assign only via dedicated Permission Sets.
- Configure strict session timeout values for Salesforce to reduce token lifetime in case of compromise.

4. Monitor & Engage

- Notify security teams and leadership of potential data exposure.
- Engage with Salesforce, Salesloft, and Mandiant for investigative support.
- Follow advisories via Salesloft's Trust Center and the Salesforce advisory portal for ongoing updates.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift