Widespread Data Theft Targets Salesforce Instances via Salesloft Drift

By Google Threat Intelligence Group, Mandiant

Published: 2025-08-26 · Archived: 2026-04-05 13:28:34 UTC

Written by: Austin Larsen, Matt Lin, Tyler McLellan, Omar ElAhdan

---

Update (August 28)

Based on new information identified by GTIG, the scope of this compromise is not exclusive to the Salesforce integration with Salesloft Drift and impacts other integrations. We now advise all Salesloft Drift customers to **treat any and all authentication tokens stored in or connected to the Drift platform as potentially compromised**.

On August 28, 2025, our investigation confirmed that the actor also compromised OAuth tokens for the "Drift Email" integration. On August 9, 2025, a threat actor used these tokens to access email from a very small number of Google Workspace accounts. The only accounts that were potentially accessed were those that had been specifically configured to integrate with Salesloft Drift; the actor would not have been able to access any other accounts on a customer's Workspace domain.

In response to these findings and to protect our customers, Google identified the impacted users, revoked the specific OAuth tokens granted to the Drift Email application, and disabled the integration functionality between Google Workspace and Salesloft Drift pending further investigation. We are notifying all impacted Google Workspace administrators.

To be clear, there has been no compromise of Google Workspace or Alphabet itself. Google has not been a Salesloft Drift customer, and therefore is not impacted. Any inquiries regarding potential breach impact should be directed to Salesloft or its customers.

We recommend organizations take immediate action to review all third-party integrations connected to their Drift instance, revoke and rotate credentials for those applications, and investigate all connected systems for signs of unauthorized access.

Salesloft has now engaged Mandiant to assist in their investigation. See Salesloft's updated advisory for more details.

Introduction

Google Threat Intelligence Group (GTIG) is issuing an advisory to alert organizations about a widespread data theft campaign, carried out by the actor tracked as UNC6395. Beginning as early as Aug. 8, 2025 through at least

Aug. 18, 2025, the actor targeted Salesforce customer instances through compromised OAuth tokens associated with the Salesloft Drift third-party application.

The actor systematically exported large volumes of data from numerous corporate Salesforce instances. GTIG assesses the primary intent of the threat actor is to harvest credentials. After the data was exfiltrated, the actor searched through the data to look for secrets that could be potentially used to compromise victim environments. GTIG observed UNC6395 targeting sensitive credentials such as Amazon Web Services (AWS) access keys (AKIA), passwords, and Snowflake-related access tokens. UNC6395 demonstrated operational security awareness by deleting query jobs, however logs were not impacted and organizations should still review relevant logs for evidence of data exposure.

Based on data available at the time, Salesloft indicated that customers that do not integrate with Salesforce are not impacted by this campaign.

On Aug. 20, 2025 Salesloft, in collaboration with Salesforce, revoked all active access and refresh tokens with the Drift application. In addition, Salesforce removed the Drift application from the Salesforce AppExchange until further notice pending further investigation. This issue does not stem from a vulnerability within the core Salesforce platform.

GTIG, Salesforce, and Salesloft have notified impacted organizations.

Threat Detail

The threat actor executed queries to retrieve information associated with Salesforce objects such as Cases, Accounts, Users, and Opportunities. For example, the threat actor ran the following sequence of queries to get a unique count from each of the associated Salesforce objects.

```
 SELECT COUNT() FROM Account;

SELECT COUNT() FROM Opportunity;

SELECT COUNT() FROM User;

SELECT COUNT() FROM Case;
```

Query to Retrieve User Data

```
 SELECT Id, Username, Email, FirstName, LastName, Name, Title, CompanyName,
Department, Division, Phone, MobilePhone, IsActive, LastLoginDate,
CreatedDate, LastModifiedDate, TimeZoneSidKey, LocaleSidKey,
LanguageLocaleKey, EmailEncodingKey
FROM User
WHERE IsActive = true
```

```
ORDER BY LastLoginDate DESC NULLS LAST
LIMIT 20
```

Query to Retrieve Case Data

```
 SELECT Id, IsDeleted, MasterRecordId, CaseNumber <snip>
FROM Case
LIMIT 10000
```

Recommendations

Given GTIG's observations of data exfiltration associated with the campaign, organizations using Salesloft Drift to integrate with third-party platforms (including but not limited to Salesforce) should consider their data compromised and are urged to take immediate remediation steps.

Impacted organizations should search for sensitive information and secrets contained within the integrated platforms and take appropriate action, such as revoking API keys, rotating credentials, and performing further investigation to determine if the secrets were abused by the threat actor.

Investigate for Compromise and Scan for Exposed Secrets

- Review all third-party integrations associated with an organization's Drift instance (accessible within the Drift Admin settings page).
- Within each integrated third-party application, search for the IP addresses and User-Agent strings provided in the IOCs section below. While this list includes IPs from the Tor network that have been observed to date, Mandiant recommends a broader search for any activity originating from Tor exit nodes.
- Review Salesforce Event Monitoring logs for unusual activity associated with the Drift connection user.
- Review authentication activity from the Drift Connected App.
- Review UniqueQuery events that log executed SOQL queries.
- Open a Salesforce support case to obtain specific queries used by the threat actor.
- Search Salesforce objects for potential secrets, such as:
    - `AKIA` for long-term AWS access key identifiers
    - `Snowflake` or `snowflakecomputing.com` for Snowflake credentials
    - `password`, `secret,key` to find potential references to credential material
    - Strings related to organization-specific login URLs, such as VPN or SSO login pages
- Run tools like Trufflehog to find secrets and hardcoded credentials.

Revoke and Rotate Credentials

- Within each integrated third-party application, revoke and rotate API keys, credentials. and authentication tokens associated with third-party application integrations with a Drift instance.
- Immediately revoke and rotate any discovered keys or secrets.
- Reset passwords for associated user accounts.
- For Salesforce integrations, configure session timeout values in Session Settings to limit the lifespan of a compromised session.

Harden Access Controls

- Review and Restrict Connected App Scopes: Ensure that applications have the minimum necessary permissions and avoid overly permissive scopes like `full` access.
- Enforce IP Restrictions on the Connected App: In the app's settings, set the "IP Relaxation" policy to "Enforce IP restrictions."
- Define Login IP Ranges: On user profiles, define IP ranges to only allow access from trusted networks.
- Remove the "API Enabled" Permission: Remove the "API Enabled" permission from profiles and grant it only to authorized users via a Permission Set.

Additional instructions and updates are available on the Salesloft Trust Center and Salesforce advisory.

Acknowledgments

We would like to thank Salesforce, Salesloft, and other trusted partners for their collaboration and assistance in responding to this threat.

IOCs

The following indicators of compromise are available in a Google Threat Intelligence (GTI) collection for registered users.

Indicator Value	Description
Salesforce-Multi-Org-Fetcher/1.0	Malicious User-Agent string
Salesforce-CLI/1.0	Malicious User-Agent string

python-requests/2.32.4	User-Agent string
Python/3.11 aiohttp/3.12.15	User-Agent string
208.68.36.90	DigitalOcean
44.215.108.109	Amazon Web Services
154.41.95.2	Tor exit node
176.65.149.100	Tor exit node
179.43.159.198	Tor exit node
185.130.47.58	Tor exit node
185.207.107.130	Tor exit node
185.220.101.133	Tor exit node
185.220.101.143	Tor exit node
185.220.101.164	Tor exit node
185.220.101.167	Tor exit node
185.220.101.169	Tor exit node
185.220.101.180	Tor exit node

185.220.101.185	Tor exit node
185.220.101.33	Tor exit node
192.42.116.179	Tor exit node
192.42.116.20	Tor exit node
194.15.36.117	Tor exit node
195.47.238.178	Tor exit node
195.47.238.83	Tor exit node

Posted in

- Threat Intelligence
