# [CS-TR-25-0910] Salesforce Breach and UNC6395 Overview

## Summary

Between March and August 2025, attackers exploited weaknesses in SaaS integrations to execute one of the most significant cloud-native campaigns of the year. The first wave targeted Google, where adversaries linked to UNC6040 and UNC6240 impersonated IT staff during a vishing call and tricked an employee into authorizing a malicious OAuth-connected application in Salesforce. This approval allowed attackers to bypass MFA and conduct bulk queries of customer contact records. The second, and far more extensive, wave was attributed to UNC6395 and confirmed through Mandiant's forensic investigations. This campaign began with the compromise of Salesloft's GitHub repositories, which provided access to Drift's AWS environment. From there, attackers stole OAuth tokens tied to Salesforce and Google Workspace integrations, enabling systematic reconnaissance and exfiltration operations between August 8 and August 18, 2025. More than 700 organizations were impacted globally, including major technology and cybersecurity firms.

The campaign highlights systemic weaknesses in OAuth trust models and SaaS integration governance. By leveraging stolen tokens, adversaries achieved persistence without needing passwords. They used Salesforce Object Query Language (SOQL) queries to extract CRM data, staged secrets such as AWS and Snowflake credentials, and covered their tracks by deleting query jobs. The scope of the breach emphasizes that OAuth tokens and SaaS-connected apps must now be treated with the same criticality as privileged accounts in on-premises infrastructure.

## Key Threat Indicators

The Salesforce and UNC6395 campaigns were defined by several technical markers that defenders can use to scope exposure. The most important temporal marker was the August 8–18, 2025 exfiltration window, during which adversaries systematically abused OAuth tokens stolen from Drift's AWS environment to access Salesforce and Google Workspace data. Investigators confirmed the initial compromise vector was the breach of Salesloft's GitHub repositories, where attackers downloaded content, created new workflows, and pivoted into Drift's infrastructure. From there, they harvested OAuth tokens associated with Salesforce and other SaaS services. These tokens bypassed MFA and conventional login controls, granting adversaries the same privileges as the legitimate apps or users that issued them. Any OAuth tokens created or refreshed between March and August 2025 in environments connected to Drift or Salesloft should be considered at risk.

The credential theft vector extended beyond OAuth abuse. Adversaries actively queried Salesforce objects to identify improperly stored secrets, including AWS access keys, Snowflake tokens, and other API credentials embedded in CRM fields. Patterns such as the AWS AKIA prefix and Snowflake connection strings were specifically targeted, enabling adversaries to escalate the compromise beyond Salesforce itself. These findings underscore that sensitive credentials were both a direct target and a high-value byproduct of the intrusion. The data types exfiltrated included CRM records such as Accounts, Cases, Users, and Opportunities, which were valuable both for reconnaissance and for downstream phishing or extortion campaigns. This blending of business data theft with credential harvesting reveals a dual objective: immediate monetization and preparation for future intrusions.

The scope of affected services was broad. Salesforce environments were the primary target, but OAuth tokens tied to Google Workspace (via Drift Email) and Slack integrations were also exploited, creating cascading risk across the SaaS supply chain. More than 700 organizations worldwide including major technology and cybersecurity companies such as Cloudflare, Palo Alto Networks, and Proofpoint were confirmed to be impacted. Attribution has been assigned to UNC6395 with high confidence, based on forensic evidence of GitHub compromise, Drift AWS intrusion, and token theft. Claims by ShinyHunters, LAPSUS$, and Scattered Spider were judged to be opportunistic and unverified, highlighting the importance of basing response actions on validated attribution.

## Attack Chain and Methodology

The campaign unfolded in multiple stages, each demonstrating the layered way attackers exploited both human weaknesses and technical integrations. The Google-focused breach began with a phone call impersonating IT staff. A Google employee approved a Python-based OAuth application disguised as Salesforce's Data Loader utility. This single authorization event bypassed MFA and provided persistent access until detection.

The broader UNC6395 campaign started with Salesloft's GitHub repositories. Forensic review revealed adversaries downloaded repository content, added guest users, and created malicious workflows. This led to Drift's AWS-hosted environment, where OAuth tokens were stolen. These tokens provided seamless access to Salesforce and Google Workspace, enabling adversaries to query sensitive CRM records. Reconnaissance focused on Accounts, Users, Opportunities, and Cases, followed by the collection of API keys and secrets improperly stored in Salesforce fields. Once operations concluded, adversaries deleted Salesforce query jobs, a deliberate defense evasion tactic.

## Indicators of Compromise (IOCs)

Narratively, the breach aligns with multiple ATT&CK techniques. The initial compromise fits supply chain compromise (T1195.002) and valid accounts via OAuth tokens (T1078.004). Credential access was achieved by locating secrets within Salesforce data (T1552.001), while reconnaissance leveraged account and system discovery techniques (T1087.001, T1082). Automated queries (T1119) and potential staging (T1074.001) were used for collection. Exfiltration was accomplished over standard APIs (T1041), with deletion of jobs (T1070.004) masking activity.

| Phase | Technique (ID) | Description |
|---|---|---|
| Initial Access | T1195.002 – Supply Chain Compromise | Compromise of Salesloft GitHub repositories |
| Initial Access | T1078.004 – Valid Accounts: Cloud | OAuth token theft enabled Salesforce/GWS access |
| Credential Access | T1552.001 – Unsecured Credentials in Files | Secrets (AWS keys, Snowflake tokens) in Salesforce data |
| Discovery | T1087.001 – Account Discovery | Enumeration of Salesforce user roles via SOQL |
| Discovery | T1082 – System Information Discovery | Salesforce metadata queries to map org structure |
| Collection | T1119 – Automated Collection | Automated SOQL queries via Drift OAuth sessions |
| Exfiltration | T1041 – Exfiltration Over C2 Channel | Data exfiltration through Salesforce APIs |
| Defense Evasion | T1070.004 – File Deletion | Deletion of Salesforce query jobs |
| Defense Evasion | T1550.001 – Alternate Auth Material | Reuse of OAuth tokens for persistence |

## Data Sources for Investigation

Organizations investigating possible impact need to correlate across SaaS audit logs, IdP telemetry, and network data. Salesforce Event Monitoring logs reveal SOQL activity and job deletions, while identity provider logs (Okta, Azure AD, Google Workspace) show OAuth token usage. GitHub audit logs are essential to confirm repository exposure, and Google Workspace logs highlight "Drift Email" OAuth access. The table below lists the most relevant sources.

| Source | Relevance |
|---|---|
| Salesforce Event Monitoring | Identify SOQL queries, bulk exports, job deletions |
| IdP logs (Okta, Azure AD, GWS) | Track OAuth grants, refreshes, reuses |
| Proxy/DNS logs | Spot Salesforce and Drift domain activity |
| GitHub audit logs | Verify repository exposure in Salesloft compromise |
| Google Workspace audit logs | Monitor Drift OAuth activity |

## Lessons Learned

These incidents emphasize that OAuth tokens are now equivalent to privileged credentials. Their theft or misuse can grant persistence even in environments protected by MFA and strong passwords. Another critical lesson is that supply chain compromise now extends into SaaS integrations: the breach of Salesloft's GitHub repositories cascaded downstream into Drift, Salesforce, and Google Workspace. Furthermore, improper storage of secrets within Salesforce objects magnified the impact, as attackers could easily query for credential patterns. Finally, adversaries demonstrated comfort in using SaaS-native functions such as query job deletions to evade detection, showing that traditional endpoint-based defenses are insufficient in cloud-native breaches.

## What Organizations Should Watch Out For

Defenders should be alert to OAuth tokens granted or reused unexpectedly, especially those linked to Drift apps between March and August 2025. Salesforce logs showing high-volume queries against Accounts, Cases, or Users are indicative of reconnaissance. Follow-on job deletions should be considered a critical evasion tactic. Any Salesforce field values containing strings resembling AWS keys, Snowflake domains, or tokens should be investigated for credential exposure. Finally, organizations should monitor for OAuth apps masquerading as legitimate but requesting broad permissions, and for traffic routed through Tor or VPNs during SaaS access sessions.

## How Organizations Can Protect Themselves

Mitigation requires both immediate containment and long-term governance improvements. Organizations must revoke all OAuth tokens associated with Drift, rotate exposed secrets, and disable legacy or overprivileged integrations. Salesforce Event Monitoring and IdP logs should be configured to alert on unusual SOQL queries and token activity. Governance should include mandatory reviews before approving new OAuth apps and continuous auditing of existing apps. Employees must be trained to recognize vishing and validate IT requests through secondary channels before granting application access. At a strategic level, organizations should adopt zero-trust for SaaS, treating all connected apps as untrusted until validated, and continuously monitoring token and API activity as part of normal security operations.

## Detection Rules & Hunting Queries

For specific hunting queries, please see publication TR-2025-09-10 in CORR

## Disclaimer

Please note that the information presented in this report reflects the most current intelligence available at the time of compilation and may be subject to change in the future.

---

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence

research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.