TIR-20250910 The Aftermath - Salesloft Drift Supply Chain Campaign & UNC6395

9/10/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

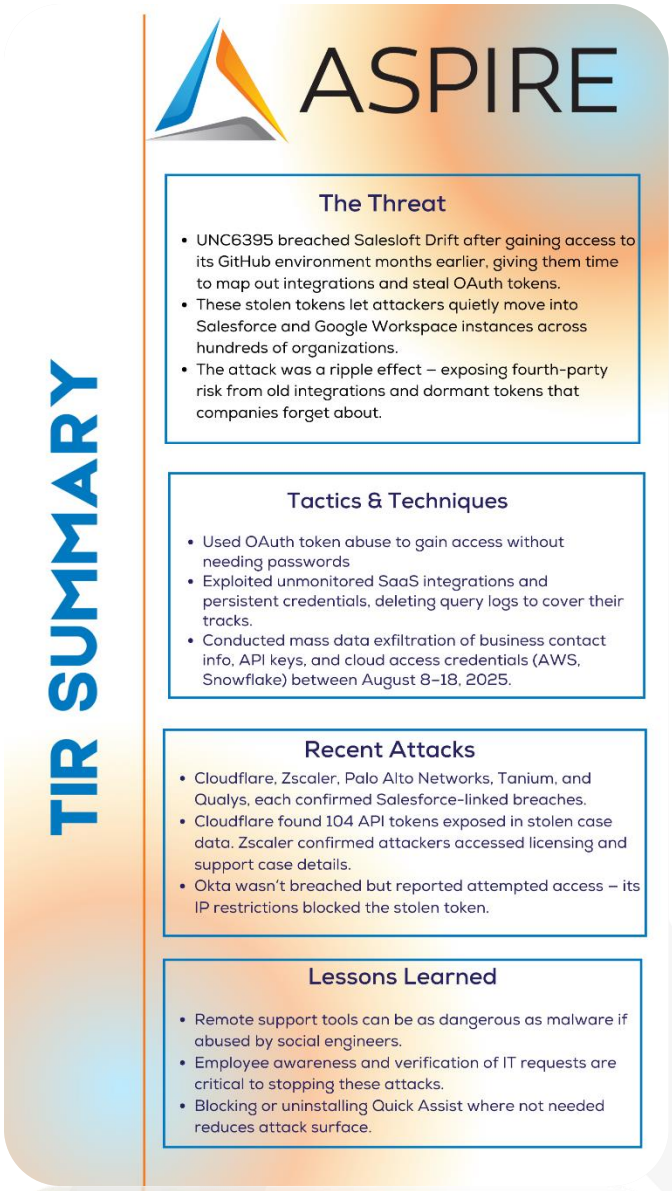
Executive Summary 3
What is Salesloft Drift and How Does it Work? 4
Salesloft Drift Attack Campaign 5
UNC6395 7
Known TTPs of UNC6395 8
Fourth Party Risk 8
Key Fourth-Party Risks 9
Conclusion 9
Aspire Recommendations 9
MITRE MAP 11
Aspire Protects 11
Indicators of Compromise (IoCs) 12
Supporting Documentation 13
Appendix II: Disclaimer 14

EXECUTIVE SUMMARY

In August 2025, a widespread campaign of data theft and supply chain compromise was uncovered, attributed to the threat actor UNC6395. The campaign exploited OAuth tokens tied to Salesloft's Drift platform, an AI-driven chatbot and sales engagement tool, which had been acquired by Salesloft in 2024. Using these tokens, attackers exfiltrated Salesforce data from hundreds of organizations and extended their reach into other platforms, including Google Workspace.

This attack is one of the most significant SaaS compromises of the year due to its scale and the prominence of its victims. Impacted organizations included Cloudflare, Palo Alto Networks, Zscaler, Qualys, Tenable, Tanium, SpyCloud, PagerDuty, and even Google. The attackers leveraged trusted integrations to bypass direct defenses, accessing Salesforce instances as though they were legitimate users.

Last week, Aspire's Cyber Threat Intelligence unit issued an Emergency Flash Notice addressing Palo Alto Networks' breach. That advisory explained how Palo Alto's Salesforce environment was compromised through the Salesloft Drift incident. While Palo Alto confirmed that its products and services remained secure, the breach still exposed business contact details and case data. This showed how even



advanced cybersecurity companies can be caught in downstream supply chain incidents when trust relationships are abused.

The UNC6395 campaign clearly shows the risks businesses face from indirect vendor relationships and inherited integrations. Businesses should understand that threats no longer stop at third parties. They now extend into “fourth parties” — acquisitions, integrations, and legacy connections that are invisible until exploited.

What is Salesloft Drift and How Does it Work?

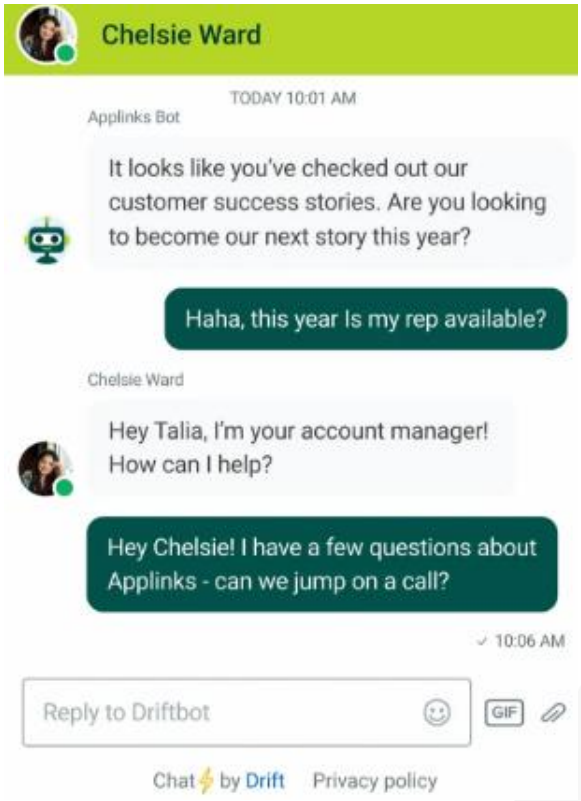
Salesloft Drift is a sales engagement and AI chatbot tool originally built by Drift and later acquired by Salesloft in 2024. It allows businesses to interact with website visitors in real time, qualify leads, and automatically push those details into customer relationship management platforms like Salesforce. Sales representatives rely on Drift daily to capture customer data and open Salesforce cases.

The system functions through OAuth integrations, which establish secure connections between Drift and third-party platforms. Once permissions are granted, the tokens allow Drift to continuously sync data without requiring repeated logins. This automation is important for modern sales teams but creates long-lived trust relationships that can be abused if compromised.

Businesses widely adopted Drift due to its efficiency. Large enterprises and mid-market firms integrate it not only with Salesforce but also with Google Workspace, Slack, and other SaaS tools. This widespread use means the application sits at the center of sensitive workflows. For many organizations, Drift is the gateway between customer interactions and core systems.

On a daily basis, a typical support team might receive a customer’s request through a Drift chatbot. That information flows directly into Salesforce, where it can include contact details, logs, passwords, or access tokens. Under normal conditions this streamlines business processes. In the context of a breach, it provides attackers with secrets that can be weaponized.

Image 1: Salesloft Chat Bot



Salesloft.com

Because Drift relies on OAuth tokens that persist until explicitly revoked, integrations can remain active even through acquisitions or platform changes. This persistence, combined with the visibility gaps that often accompany mergers, made Drift an attractive and powerful target for UNC6395.

Salesloft Drift Attack Campaign

UNC6395's campaign was not sudden. It was a carefully staged operation. The earliest signs date back to March 2025, when attackers gained unauthorized access to Salesloft's GitHub account. They downloaded code repositories, added a guest user,

and set up workflows, maintaining access undetected for several months. This time gave the group valuable reconnaissance and insight into Drift's environment.

By June 2025, the attackers pivoted into Drift's AWS environment, where they obtained OAuth tokens associated with Drift's customer integrations. These tokens acted as master keys, granting access to Salesforce and other connected systems. Salesloft did not detect this theft until the August breaches began to surface, raising serious concerns about its security posture and monitoring capabilities.

Between August 8 and August 18, UNC6395 exfiltrated Salesforce data across hundreds of organizations. They executed queries against Salesforce objects such as Cases, Accounts, Users, and Opportunities. They also scanned exported data for credentials including AWS access keys and Snowflake tokens. To cover their tracks, they deleted query jobs, though logs remained intact for later forensic review.

The attack timeline is as follows:

- **March–June 2025** – UNC6395 accesses Salesloft GitHub repositories and establishes persistence.
- **June 2025** – Attackers obtain OAuth tokens from Drift's AWS environment.
- **August 8–9, 2025** – Limited Google Workspace accounts integrated with Drift Email are accessed.
- **August 8–18, 2025** – Mass exfiltration of Salesforce data across hundreds of companies.
- **August 20, 2025** – Salesloft and Salesforce revoke all active Drift tokens.
- **August 26, 2025** – Google and Mandiant attribute the campaign to UNC6395.
- **September 2025** – Victims including Cloudflare, Zscaler, Palo Alto Networks, Qualys, Tenable, SpyCloud, and Tanium confirm breaches.

The attack chain followed a clear pattern. Initial compromise of GitHub provided knowledge of internal systems. Access to Drift's AWS environment yielded OAuth tokens. These tokens were then replayed against Salesforce and Google Workspace integrations, allowing direct data theft. For visualization, this chain looks like this: GitHub compromise → AWS environment access → OAuth token theft → Salesforce and Workspace exfiltration.

Salesloft's delayed recognition of the GitHub breach could mean insufficient monitoring of source code repositories and user activity. Dormant OAuth tokens played a major role in widening the breach. It's a clear example of how neglected SaaS integrations can create opportunities for large-scale compromise.

The victims included some of the most well-defended technology companies in the world. Cloudflare, Zscaler, and Palo Alto Networks each confirmed breaches, though they emphasized that their products and infrastructure were not impacted. Instead, attackers focused on business contact information, support cases, and credentials embedded in customer interactions. Google also confirmed that several Workspace accounts tied to Drift Email were accessed.

The campaign makes it clear how invisible trust relationships can be weaponized. Companies thought they were securing their own systems, but they were compromised through a vendor's acquisition and an overlooked integration. This was not a simple breach of a single company but a supply chain incident that impacted various industries.

UNC6395

UNC6395 is the activity cluster attributed to this campaign by Google and Mandiant. While public information on the group prior to this incident is limited, their behavior shows patience and an understanding of SaaS ecosystems. What made this attack so damaging is that OAuth tokens from past integrations were still valid. That's the kind of overlooked access point that can quietly put dozens of companies at risk. Their country of origin has not been publicly confirmed. However, analysts assess UNC6395 as financially motivated, that could be based out of China. It is not clear whether or not the group could be state sponsored. The choice of targets (cybersecurity vendors, SaaS-heavy enterprises, and cloud providers) points to a desire to harvest credentials that can unlock additional revenue or downstream opportunities.

UNC6395 first entered the spotlight in August 2025 when Google publicly connected them to the Salesloft Drift campaign. Forensic evidence shows their presence in Salesloft's GitHub as early as March 2025. The group is deliberate, planning intrusions months in advance, and comfortable with maintaining persistence across environments.

UNCE6395 was discovered abusing Drift through abnormal Salesforce queries. Google Threat Intelligence observed suspicious bulk API jobs and OAuth activity, which led to deeper investigation. Mandiant's parallel review of Salesloft confirmed the presence of malicious workflows, guest accounts, and AWS access tied to OAuth token theft.

Known TTPs of UNC6395

- Initial Access, GitHub Compromise [T1078] – Unauthorized access to Salesloft's GitHub repositories, adding guest users and establishing workflows.
- Credential Access, Cloud Infrastructure [T1552**]** – Theft of secrets and tokens from Drift's AWS environment.
- Persistence, Valid Accounts [T1078.004] – Use of stolen OAuth tokens for long-term access.
- Collection, Salesforce API Queries [T1530] – Export of Cases, Accounts, Opportunities, and User records via Salesforce APIs.
- Defense Evasion, Indicator Removal [T1070] – Deletion of query jobs to obscure evidence.
- Exfiltration, Cloud Storage [T1537] – Systematic export of sensitive business data.

FOURTH PARTY RISK

The Salesloft Drift campaign brought the concept of fourth-party risk into sharp focus. Businesses were not compromised directly through their vendors, or even their vendors' vendors, but through an acquired company's dormant integrations. These connections extended the attack surface far beyond what most organizations can see or assess.

Fourth-party risk happens whenever vendors acquire other companies. Legacy OAuth tokens, API connections, and integrations often persist across acquisitions. Unless carefully inventoried and revoked, these tokens remain valid indefinitely, creating silent exposures that can be exploited years later.

Traditional vendor risk assessments rarely ask about acquisitions or inherited integrations. Security teams may review SOC 2 reports or access control policies, but they seldom ask whether a vendor recently acquired another company and whether old OAuth tokens were still active. This creates blind spots that adversaries like UNC6395 exploit.

The Salesloft Drift breach shows what happens when a business's attack surface extends into chains of trust that are often invisible. Every acquisition introduces unknown risks that organizations downstream inherit whether they know it or not.

Key Fourth-Party Risks

- Inherited OAuth tokens that persist across acquisitions.
- Legacy integrations tied to SaaS tools no longer actively used.
- Dormant permissions that grant excessive access to sensitive data.
- Vendor consolidations that expand the attack surface without proper auditing.

Organizations must shift from point-in-time questionnaires to continuous monitoring of actual data flows. Zero-trust principles should be extended to vendors and their acquisitions, with every OAuth token treated as a potential attack vector.

Conclusion

What happened with Salesloft Drift changes the conversation around SaaS security and vendor oversight. By targeting a single vendor integration, UNC6395 compromised hundreds of organizations across multiple industries. The breadth of victims shows how no business is immune from the ripple effects of supply chain compromises.

For business leaders, the lesson is that supply chain risks now extend to fourth parties and beyond. Acquisitions, dormant tokens, and inherited integrations can all become attack paths. Without continuous monitoring, companies cannot see or control the exposures buried in their vendor ecosystems.

Understanding this breach is not just about learning how UNC6395 operated. It is about recognizing how trust, once granted, can be abused indefinitely. Companies should demand transparency from vendors, so they can be better positioned to withstand the next supply chain attack.

Aspire Recommendations

Organizations should take immediate, specific steps to protect against the risks associated with this campaign.

- Revoke and rotate all OAuth tokens tied to Salesloft Drift and any integrations connected to it.
- Audit all SaaS integrations, focusing on dormant or overscoped permissions.
- Monitor Salesforce Event Monitoring logs for unusual queries or API calls tied to Drift.
- Search exported Salesforce data for embedded credentials such as AWS keys and Snowflake tokens, and rotate them immediately.
- Enforce IP restrictions and session timeouts on Salesforce Connected Apps.
- Implement proof-of-possession controls (such as DPoP) to constrain token use to specific clients.
- Require vendors to disclose acquisitions and inherited integrations during risk assessments.
- Deploy continuous monitoring of OAuth activity across SaaS environments to detect abnormal behavior.

While technical defenses are important, employee behavior also plays a role in preventing attackers from turning a vendor's compromise into your breach. Here's where employee awareness and IT request verification comes in for downstream victims (the customers of Drift):

- **Support cases often include secrets** — Employees sometimes drop API keys, logs, or credentials into Salesforce tickets, trusting that the vendor will use them securely. Training staff not to share sensitive information this way (or verifying requests before sending anything) would have limited the value of what attackers found.
- **Credential rotation and unusual IT requests** — If employees are aware that OAuth tokens, API keys, or integration requests can be abused, they'll be more likely to escalate unusual vendor requests (like "reconnect your integration" or "re-enter this API key"). Attackers often replay stolen tokens or send fake integration prompts to trick users into reauthorizing access.
- **Stopping lateral damage** — Even though the initial compromise was on Salesloft's side, UNC6395's ability to harvest secrets and reuse them depends on employees and IT staff not questioning where those requests come from. A simple verification step — "Did Salesloft really ask me to send this API key?" — can stop the bleed into your environment.

MITRE MAP

UNC6395

Initial Access	T1078 – Valid Accounts
Credential Access	T1552 – Unsecured Credentials
Persistence	T1078.004 – Valid Accounts: Cloud Accounts
Collection	T1530 – Data from Cloud Storage
Defense Evasion	T1070 – Indicator Removal on Host
Exfiltration	T1537 – Exfiltration to Cloud Storage

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers

around-the-clock protection across cloud, network, and endpoints in one integrated solution.

- Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

IPv4

- 154[.]41[.]95[.]2
- 176[.]65[.]149[.]100
- 179[.]43[.]159[.]198
- 185[.]130[.]47[.]58
- 185[.]207[.]107[.]130
- 185[.]220[.]101[.]133
- 185[.]220[.]101[.]143
- 185[.]220[.]101[.]164
- 185[.]220[.]101[.]167
- 185[.]220[.]101[.]169
- 185[.]220[.]101[.]180
- 185[.]220[.]101[.]185

- 185[.]220[.]101[.]33
- 192[.]42[.]116[.]179
- 192[.]42[.]116[.]20
- 194[.]15[.]36[.]117
- 195[.]47[.]238[.]178
- 195[.]47[.]238[.]83
- 208[.]68[.]36[.]90
- 44[.]215[.]108[.]109

User-Agent Strings

- Salesforce-Multi-Org-Fetcher/1.0
- Salesforce-CLI/1.0
- python-requests/2.32.4
- Python/3.11 aiohttp/3.12.15
- sf-export/1.0.0

Application ID

- 1084253493764-ipb2ntp4jb4rmqc76jp7habdrhfdus3q.apps.googleusercontent.com

SUPPORTING DOCUMENTATION

Widespread Data Theft Targets Salesforce Instances via Salesloft Drift | Google Cloud Blog

Cloudflare, Zscaler among companies impacted by Salesloft Drift incident | The Record from Recorded Future News

Palo Alto Networks disclosed a data breach linked to Salesloft Drift incident

5 Cybersecurity Vendors Impacted In Salesloft Drift Breach

Salesloft Drift hackers had access to company GitHub account for months before attacks | IT Pro

Security Firms Hit by Salesforce–Salesloft Drift Breach - SecurityWeek

The Salesloft incident: A wake-up call for SaaS security and IPSIE adoption

Google Warns Salesloft Drift Breach Impacts All Drift Integrations Beyond Salesforce

Widespread Salesforce Data Theft via Compromised Salesloft Drift OAuth Tokens - Arctic Wolf

Widespread Data Theft Targets Salesforce Instances via Salesloft Drift | Google Cloud Blog

BREAKING: UNC6395 – The Biggest SaaS Breach of 2025

Salesloft Trust Portal

What the Salesloft Drift breaches reveal about 4th-party risk | CSO Online

Qualys, Tenable Latest Victims of Salesloft Drift Hack - Infosecurity Magazine

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.