Palo Alto Networks Breach Tied to Salesloft Drift OAuth Token Abuse

TL;DR

Palo Alto Networks confirmed that attackers accessed its Salesforce environment using stolen OAuth tokens from the Salesloft Drift breach. Customer contact data, sales records, and support case text were exfiltrated, though no products, firewalls, or core security services were impacted.

Threat actors scanned for secrets like AWS keys, VPN logins, and passwords, likely to continue attacks against other platforms.

Overview

This week, Palo Alto Networks confirmed it was affected by the Salesloft Drift supply chain attack. The Salesloft Drift tool links the Drift AI chat platform with Salesforce, allowing organizations to push conversations, leads, and support cases directly into their CRM.

Using stolen OAuth tokens, attackers gained access to the company's Salesforce CRM and stole customer contact details, internal sales records, and support case data. Once inside Salesforce, the attackers stole data from accounts, contacts, and cases. They scanned this information for credentials and cloud access keys (including AWS, Snowflake, and VPN/SSO logins) using automated Python-based tools to speed up the theft. Logs and queries were deleted to obscure activity.

Credentials were found within support case comments, which could allow attackers to pivot into other connected cloud environments. Palo Alto has since revoked the compromised tokens, but the attack is part of a broader campaign that has hit hundreds of organizations, including other major cloud and security vendors (Cloudflare, Zscaler, etc.). Google tracks the threat actors behind this activity as UNC6395.

Although Palo Alto stated that its products, network defenses, and customer-deployed systems were not impacted; the incident is a reminder that even trusted vendors within cybersecurity can be collateral damage in supply chain attack campaigns.

Aspire Protects

- Salesloft recommends following their re-authentication guidance:
    - In order to re-authenticate Salesforce in Drift:
        - Go to Settings > Integrations > Salesforce;
        - Click Disconnect;
        - Click Connect Account;
        - Log in with your Salesforce credentials and authorize the connection.
            - **Note**: You may need to give the app a minute or so to process before refreshing the page, at which point you should see a successful connection.
            - Please note that the above referenced issue does not impact any Drift customers who **do not integrate with Salesforce**.
- Review Salesforce, IdP, and network logs for unusual authentication or API activity.
- Revoke and rotate all Salesforce API keys, connected app credentials, and any secrets may have been exposed.
- Apply Zero Trust access principles to restrict lateral movement if credentials are compromised.

TTPs to Watch

Defense Evasion

- Indicator Removal on Host [T1070] – The attackers deleted Salesforce queries and logs to conceal their activity, making forensic analysis more difficult.

Privilege Escalation

- Access Token Manipulation [T1134] – Compromised OAuth tokens were abused to gain authenticated access to Salesforce without needing user credentials.

Command and Control

- Proxy [T1090] – Traffic was routed through Tor exit nodes to hide the true origin of the connections and complicate attribution.

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

Targeted Industries

This supply chain attack isn't limited to one sector. The industries most likely to be affected include:

- Energy
- Education
- Finance
- Healthcare
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **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 cyber attacks.
- **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.

Supporting Documentation

Threat Brief: Salesloft Drift Integration Used To Compromise Salesforce Instances

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

Widespread Data Theft Targets Salesforce Instances via Salesloft Drift. - LevelBlue - Open Threat Exchange

Salesloft Trust Portal