ZEROFOX INTELLIGENCE

Flash

Exploitation of Salesforce Systems Likely to Continue

F-2025-09-04a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Threat Actor, Data Breach, Deep Web

September 4, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on September 4, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Exploitation of Salesforce Systems Likely to Continue

| Key Findings

- Beginning around August 8, 2025, and continuing until approximately August 18, 2025, a sophisticated supply chain breach targeting the Drift-Salesforce integration AI chatbot was reportedly carried out by a threat actor leveraging OAuth credentials to exfiltrate Salesforce instance data from multiple companies.
- Notably, customers who integrate online services with Salesloft's Drift platform (such as Slack, Google Workspace, Amazon S3, Microsoft Azure, and OpenAI) can potentially be impacted by threat actors using the stolen OAuth tokens.
- ZeroFox assesses that more companies that have utilized the compromised Salesforce integration with Salesloft Drift are likely to be publicly disclosed as victims in the coming weeks.

© 2025 ZeroFox, Inc. All rights reserved.

Details

Beginning around August 8, 2025, and continuing until approximately August 18, 2025, a sophisticated supply chain breach targeting the Drift-Salesforce integration, which connects the two platforms to automate lead capture and sales outreach workflows, was reportedly carried out by a threat actor leveraging OAuth credentials to exfiltrate Salesforce instance data from multiple companies.[1]

- This has enabled attackers to exfiltrate sensitive credentials such as AWS keys, Snowflake tokens, and internal passwords across hundreds of organizations—including Cloudflare, Palo Alto Networks, and PagerDuty.[2]
- Multiple organizations, including Cisco, Cloudflare (104 API tokens stolen), Zscaler, Palo Alto Networks, SpyCloud, PagerDuty, and Tanium, have since confirmed exposure and initiated remediation efforts.
- The attackers reportedly demonstrated strong operational security, deleting query jobs post-exfiltration, and the breadth of affected integrations expanded beyond Salesforce to platforms such as Google, Slack, and Amazon.[3]

Investigations later revealed that the breach also affected a small subset of Google Workspace accounts through the "Drift Email" integration. Notably, security researchers have reported that customers who integrate online services such as Slack, Google Workspace, Amazon S3, Microsoft Azure, and OpenAI with Salesloft may be potentially impacted by threat actors leveraging the stolen OAuth tokens.[4]

Threat group “ShinyHunters” (also tracked as UNC6040) has reportedly been linked to the Drift-Salesforce campaign; the tactics, techniques, and procedures (TTPs) observed are also similar to those used by another threat group, “Scattered Spider”. As detailed in a recent ZeroFox Flash report, ShinyHunters and Scattered Spider were among the threat actors potentially involved in an August 2025 Workday breach also linked to a Salesforce vulnerability.

[1] hXXps://trust.salesloft[.]com/?uid=Drift%2FSalesforce+Security+Update
[2] hXXps://blog.cloudflare[.]com/response-to-salesloft-drift-incident/
[3] hXXps://krebsonsecurity[.]com/2025/09/the-ongoing-fallout-from-a-breach-at-ai-chatbot-maker-salesloft/
[4] *Ibid.*

© 2025 ZeroFox, Inc. All rights reserved.

- ShinyHunters, active since 2020 with at least 91 known victims, primarily seeks financial gain via network intrusion, data breach, and (recently) social engineering.
- The group has previously sold large stolen datasets, including 73 million AT&T customer records, and typically exploits vulnerabilities in cloud applications and website databases.
- A Telegram channel has claimed that "UNC6395", a threat actor suspected to be linked to this chain of attacks, has been arrested. The Telegram channel operator claims to be a former employee of cryptocurrency company ChangeNOW, who was allegedly fired following a ScatteredSpider hacking incident.[5] ChangeNOW has denied being the victim of a cyberattack. ZeroFox cannot independently verify the claim UNC6395 has been arrested.

ZeroFox assesses that more companies that have utilized the compromised Salesforce integration with Salesloft Drift are likely to be publicly disclosed as victims in the coming weeks. This ongoing supply chain compromise is also likely to affect downstream entities of already-impacted companies.

- Threat actors will likely use phishing, business email compromise (BEC), and social engineering attacks to target the downstream entities.
- There will very likely be additional risks, such as threat actors leveraging impersonation techniques and reusing stolen OAuth/API tokens to regain access or move laterally within connected Software as a Service (SaaS) environments.
- The stolen customer relationship management (CRM) datasets are likely to be resold on underground forums, which could broaden exposure across multiple industries.

As of writing, Salesforce has disabled its integration with the Drift application. ZeroFox recommends that companies exercise caution and disable the connection between Salesforce and the Drift application in their networks, rotate any exposed OAuth tokens or API keys, and apply the principle of least privilege to connected apps.

[5] hXXps://x[.]com/IntCyberDigest/status/1963308828713418869

© 2025 ZeroFox, Inc. All rights reserved.

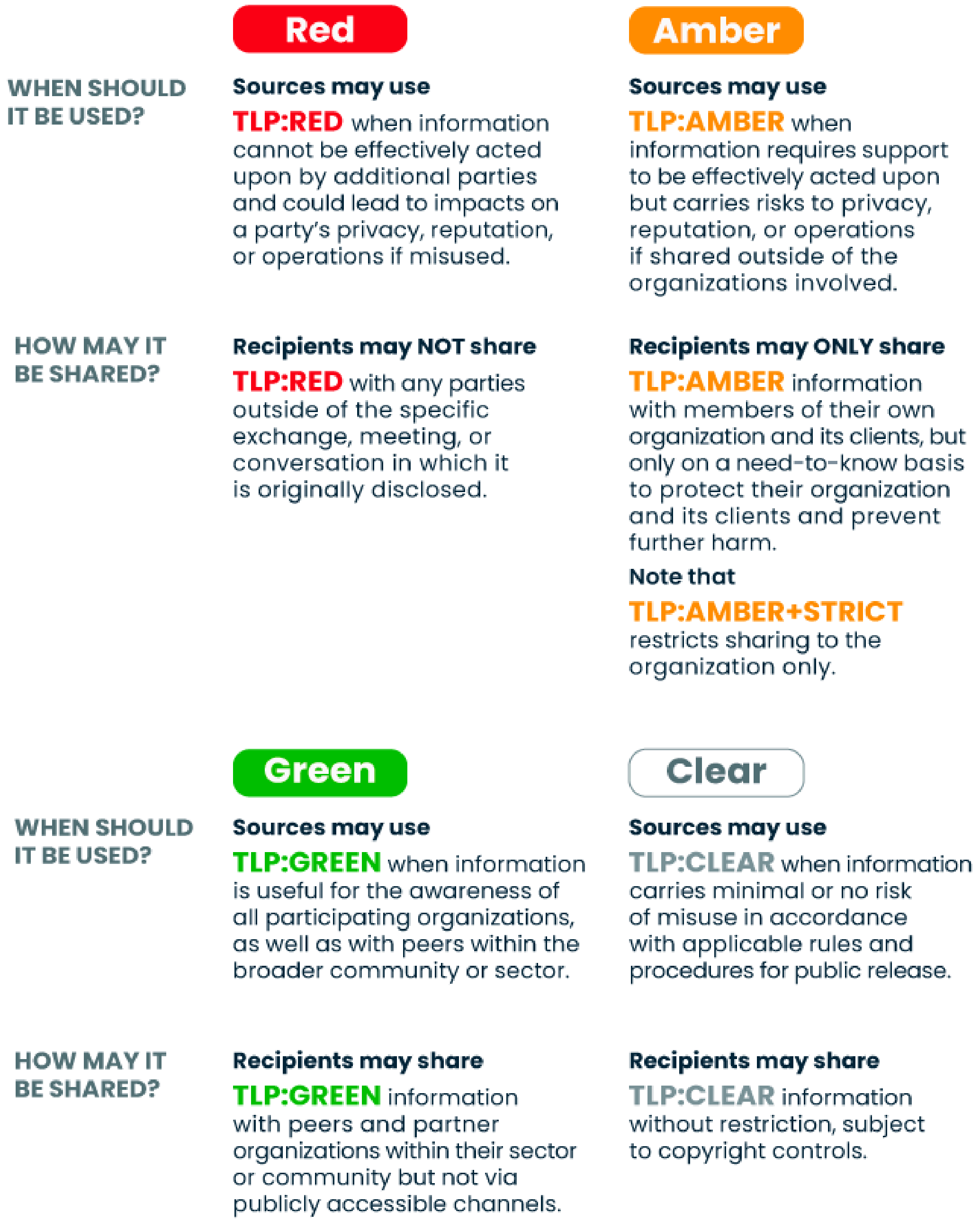
Recommendations

- In response to the recent incident, Salesloft has published the following guidance:[6]
    - All Drift customers who manage their own Drift connections to third-party applications via API key should proactively revoke the existing key and reconnect using a new API key for these applications. This only relates to API key-based Drift integrations. OAuth applications are being handled directly by Salesloft.
    - These actions will need to be taken directly within the third-party provider's application. You can see a list of your current connected integrations within the Drift Admin settings. In order to see your integrations, follow these steps:
        - Settings > Integrations > [Your connected Drift integrations will appear here.]
        - Take action directly in each third-party provider's application.
        - When ready, update your API key in each connected Drift integration.
- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multifactor authentication, secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

[6] hXXps://trust.salesloft[.]com/?uid=Drift%2FSalesforce+Security+Update

© 2025 ZeroFox, Inc. All rights reserved.

Appendix A: Traffic Light Protocol for Information Dissemination



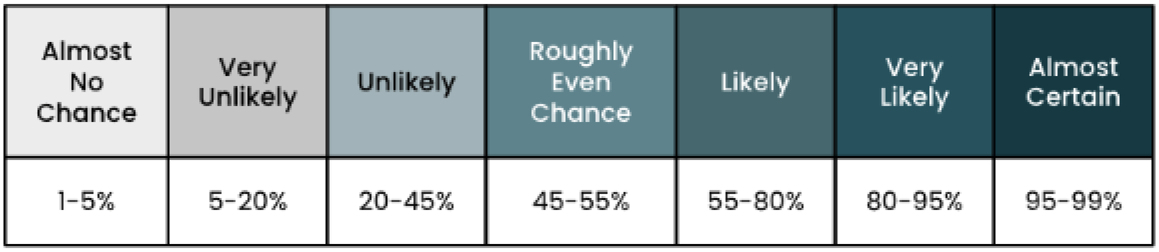
	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

© 2025 ZeroFox, Inc. All rights reserved.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

© 2025 ZeroFox, Inc. All rights reserved.