New Data Theft Campaign Targets Salesforce via Salesloft App - Against In

Data: 2025-08-29 03:32:51

Autor: Inteligência Against Invaders

Salesforce customers have again been targeted in a “widespread data theft campaign,” this time via

compromised OAuth tokens associated with thethird-party Salesloft Drift application.

Salesloft Drift integrates with Salesforce to help sales and marketing teams collaborate on projects. Salesloft issued a security alert on August 20 revealing it had detected a security issue and “proactively revoked connections between Drift and Salesforce.”

However, the firm had little more to say on the matter until Google Threat Intelligence Group (GTIG) lifted the lid on Tuesday August 26.

It said a threat actor tracked as UNC6395 had targeted “numerous” Salesforce customer instances between August 8 and August 18, systematically exfiltrating large volumes of data. Some experts have suggested that “hundreds”of customers may have been impacted.

“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,” Google explained.

“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.”

Read more on Salesforce attacks: Allianz Life Data Breach Exposes Personal Data of 1.1 Million Customers

Google warned any Salesforce customers using Drift to assume their Salesforce data is now compromised and to take immediate steps to remediate.

“Impacted organizations should search for sensitive information and secrets contained within Salesforce objects 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,” it added.

Because Salesloft revoked all active access and refresh tokens for the Drift app, admins will need to reauthenticate their Salesforce connection, Salesloft clarifiedin an update yesterday. The firm has hired an incident response specialist to carry out an investigation.

Salesforce has removed the Drift app from its Salesforce AppExchange while an investigation is underway.

The news comes as more victim names emerge from a parallel data extortion campaign targeting Salesforce instances via vishing attacks. Reports suggest the latest company to fall victim to the ShinyHunters group is US insurer Farmers Insurance, whose website was offline at the time of writing.

Experts Suspect State Actor

Cory Michal, CSO of AppOmni, argued that the Salesloft attacks could be the work of a nation state, given the scale of the compromise and the coordinated nature of the campaign.

“What’s most noteworthy about the UNC6395 attacks is both the scale and the discipline. This wasn’t a one-off compromise; hundreds of Salesforce tenants of specific organizations of interest were targeted using stolen OAuth tokens, and the attacker methodically queried and exported data across many environments,” he explained.

“They demonstrated a high level of operational discipline, running structured queries, searching specifically for credentialsand even attempting to cover their tracks by deleting jobs. The combination of scale, focusand tradecraft makes this campaign stand out.”

Jonathan Sander, field CTO at Astrix Security, added that the campaign highlights the challenge of protecting non-human identities (NHIs).

“The Salesloft Drift token breach is a classic NHI attack. Steal things humans won’t notice because humans don’t use them, and operate in the shadows for as long as you can. And then they use that to steal even more NHI assets to do it again and again,” Sander argued.

“Sadly, most of the time what we see is that people don’t know what they don’t know about their NHIs. They haven’t even built a basic inventory of what these bad guys are going after.”