ShinyHunters Target Salesforce CRM Platforms in Ongoing Data Extortion Campaign

TL;DR

ShinyHunters is behind a coordinated campaign breaching Salesforce environments through vishing and malicious OAuth apps. No Salesforce vulnerability is involved; attackers trick employees into authorizing fake connected apps that siphon CRM data.

Victims include Qantas, Allianz Life, and LVMH. The group is quietly extorting companies without public leaks.

Organizations using Salesforce should immediately audit connected apps, lock down OAuth permissions, and train staff to spot vishing tactics.

Overview

ShinyHunters, the data extortion group previously linked to high-profile cloud breaches, has been named as the threat actor behind a string of attacks targeting Salesforce CRM environments across multiple industries. Recent victims include Qantas Airways, Allianz Life, and luxury giant LVMH, each reporting unauthorized access to customer data tied to third-party platforms. Although the companies have not named Salesforce, evidence and victim overlap confirm the attacks stem from the same campaign flagged by Google's Threat Intelligence Group in June 2025.

Affected Organizations

- Qantas – 5.7 million customer records reportedly accessed via Salesforce
- Allianz Life – Breach of cloud CRM platform confirmed (believed to be Salesforce)
- LVMH (Louis Vuitton, Dior, Tiffany & Co.) – Vendor platform compromised, confirmed to be part of same campaign
- Adidas – Confirmed data breach involving a third-party CRM

The campaign does not involve a vulnerability in Salesforce itself but exploits human behavior. Attackers initiate vishing calls to convince employees to connect malicious OAuth apps to their Salesforce instance. MFA tokens and login credentials have also been harvested via spoofed Okta pages in some cases.

Once access is obtained, attackers extract customer databases, particularly “Accounts” and “Contacts” tables common to Salesforce’s CRM architecture. The fact that the breaches are still unfolding suggests that many organizations remain unaware their platforms have already been compromised. As of now, the attacks have not resulted in data leaks. Stay vigilant and see Aspire’s recommendations below.

Aspire Protects

- ShinyHunters is exploiting human trust via social engineering. Here is a quick recap of how they are doing it:
    - They call employees pretending to be IT support (vishing).
    - They direct them to the connected app setup page in Salesforce.
    - The victim is asked to enter a malicious connection code.
    - That code authorizes a rogue app, giving attackers persistent access without needing to hack Salesforce itself.
- To stay safe, Aspire recommends the following:
    - Train users to verify any IT requests received over the phone. No IT team should ever ask for app authorization codes.
    - Mandate phishing-resistant MFA, such as hardware security keys (FIDO2/U2F) or platform authenticators.
        - Avoid relying solely on push-based MFA or SMS codes, which can be phished or socially engineered.
    - Audit all connected apps in Salesforce immediately and remove unrecognized or suspicious entries.
    - Enforce IP restrictions on Salesforce login and app connections.
    - Enable Salesforce Shield for anomaly detection, data loss prevention, and audit trail logging.

TTPs to Watch

Initial Access

- Phishing [T1566.001] – Spoofed Okta login pages used to capture credentials.

- Vishing [T1598.004] – Threat actors call employees pretending to be internal IT, instructing them to authorize malicious OAuth apps.

Persistence

- Abuse of OAuth Tokens [T1528] – Linked apps maintain access beyond password resets.

Collection

- Data from Information Repositories [T1213] – Exfiltration of Salesforce "Accounts" and "Contacts" data tables.

Command and Control

- Web Service [T1102] – Data transfer likely occurs via compromised app infrastructure.

IoCs

There are no known IoCs associated with ShinyHunters at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

ShinyHunters is stealing customer data from Salesforce environments across industries like:

- Aviation
- Insurance
- Retail
- Technology

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

The Cost of a Call: From Voice Phishing to Data Extortion | Google Cloud Blog

Hackers abuse malicious version of Salesforce tool for data theft, extortion | Cybersecurity Dive