ShinyHunters behind Salesforce data theft attacks at Qantas, Allianz Life, and LVMH

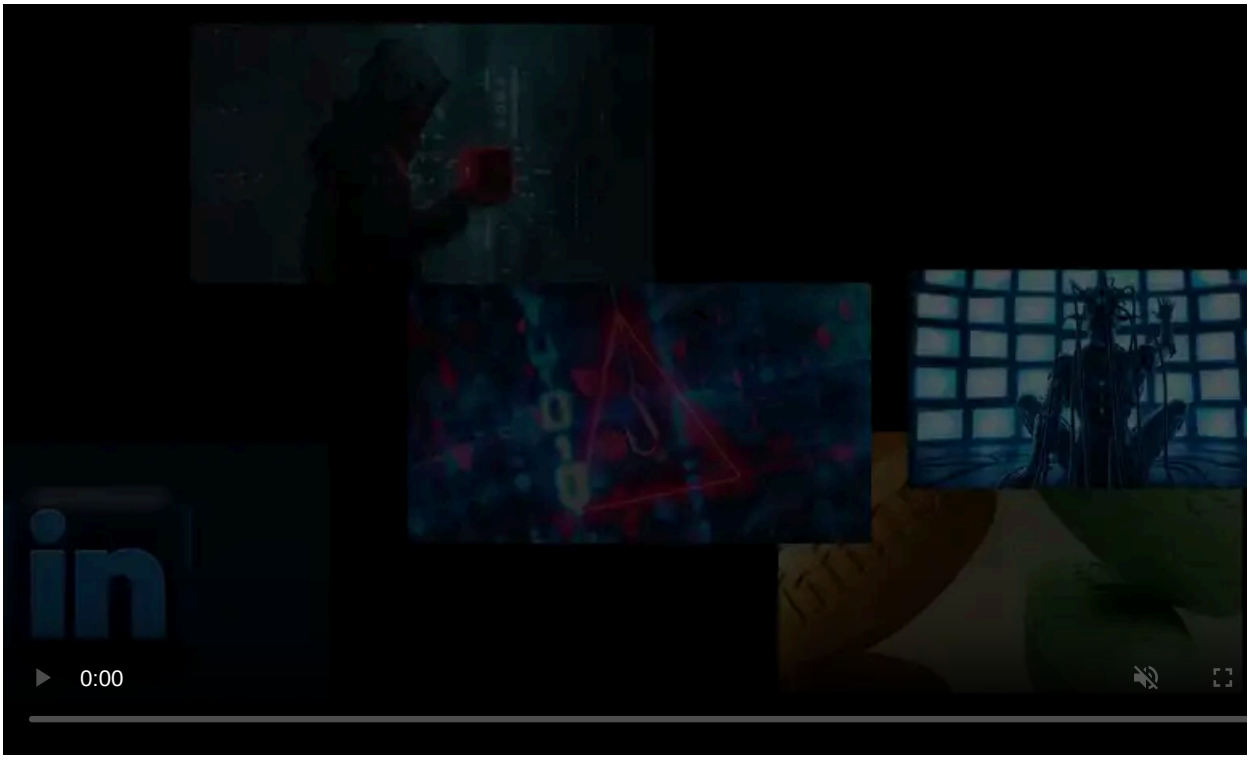
By Lawrence Abrams

Published: 2025-07-30 · Archived: 2026-04-05 17:27:02 UTC

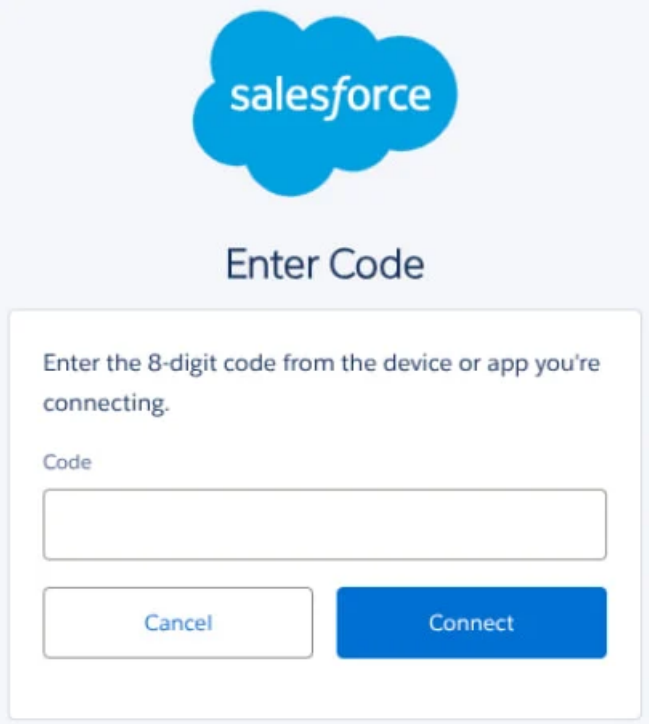
A wave of data breaches impacting companies like Qantas, Allianz Life, LVMH, and Adidas has been linked to the ShinyHunters extortion group, which has been using voice phishing attacks to steal data from Salesforce CRM instances.

In June, Google's Threat Intelligence Group (GTIG) warned that threat actors tracked as UNC6040 were targeting Salesforce customers in social engineering attacks.

In these attacks, the threat actors impersonated IT support staff in phone calls to targeted employees, attempting to persuade them into visiting Salesforce's connected app setup page. On this page, they were told to enter a "connection code", which linked a malicious version of Salesforce's Data Loader OAuth app to the target's Salesforce environment.


0:00

In some cases, the Data Loader component was renamed to "My Ticket Portal," to make it more convincing in the attacks.



Prompt to enter connection code
Source: Google

GTIG says that these attacks were usually conducted through vishing (voice phishing), but credentials and MFA tokens were also stolen through phishing pages that impersonated Okta login pages.

Around the time of this report, multiple companies reported data breaches involving third-party customer service or cloud-based CRM systems.

LVMH subsidiaries Louis Vuitton, Dior, and Tiffany & Co. each disclosed unauthorized access to a customer information database, with Tiffany Korea notifying customers the attackers breached a "vendor platform used for managing customer data."

Adidas, Qantas, and Allianz Life also reported breaches involving third-party systems, with Allianz confirming it was a third-party customer relationship management platform.

"On July 16, 2025, a malicious threat actor gained access to a third-party, cloud-based CRM system used by Allianz Life Insurance Company of North America (Allianz Life)," an Allianz Life spokesperson told BleepingComputer.

While BleepingComputer has learned that the Qantas data breach also involved a third-party customer relationship management platform, the company will not confirm it is Salesforce. However, previous reporting from local media claims the data was stolen from Qantas' Salesforce instance.

Furthermore, court documents state that the threat actors targeted "Accounts" and "Contacts" database tables, both of which are Salesforce objects.

While none of these companies have publicly named Salesforce, BleepingComputer has since confirmed that all were targeted in the same campaign detailed by Google.

The attacks have not led to public extortion or data leaks yet, with BleepingComputer learning that the threat actors are attempting to privately extort companies over email, where they name themselves as ShinyHunters.

It is believed that when these extortion attempts fail, the threat actors will release stolen information in a long wave of leaks, similar to ShinyHunter's previous Snowflake attacks.

"We have not identified any data leak sites associated with this activity," Genevieve Stark, Head of Cybercrime, and Information Operations Intelligence Analysis at GTIG, told BleepingComputer.

"It is plausible that the threat actor intends to sell the data instead of sharing it publicly. This approach would align with prior ShinyHunters Group activity."

Google say they are now tracking Salesforce data-theft attacks under multiple threat group designations.

"GTIG attributes multiple incidents impacting Salesforce instances to UNC6040. In at least some cases, the follow-on extortion activity, which we attribute to the distinct threat cluster UNC6240, has used the ShinyHunters brand," Stark told BleepingComputer.

"The extortion activity is attributed to UNC6240 instead of UNC6040 due to a significant time gap between the initial data theft activity and the subsequent extortion activity. We have not confirmed the nature of the relationship between these intrusions and the prior use of this handle on underground forums."

Who is ShinyHunters

The breaches have caused confusion among the cybersecurity community and the media, including BleepingComputer, with the attacks attributed to Scattered Spider (tracked by Mandiant as UNC3944), as those threat actors were also targeting the aviation, retail, and insurance sectors around the same time and demonstrated similar tactics.

However, threat actors associated with Scattered Spider tend to perform full-blown network breaches, culminating with data theft and, sometimes, ransomware. ShinyHunters, tracked as UNC6040, on the other hand, tends to focus more on data-theft extortion attacks targeting a particular cloud platform or web application.

It is BleepingComputer's and some security researchers' belief that both UNC6040/UNC6240 and UNC3944 consist of overlapping members that communicate within the same online communities. The threat group is also believed to overlap with "The Com," a network of experienced English-speaking cybercriminals.

"According to Recorded Future intelligence, the overlapping TTPs between known Scattered Spider and ShinyHunters attacks indicate likely some crossover between the two groups," Allan Liska, an Intelligence Analyst for Recorded Future, told BleepingComputer.

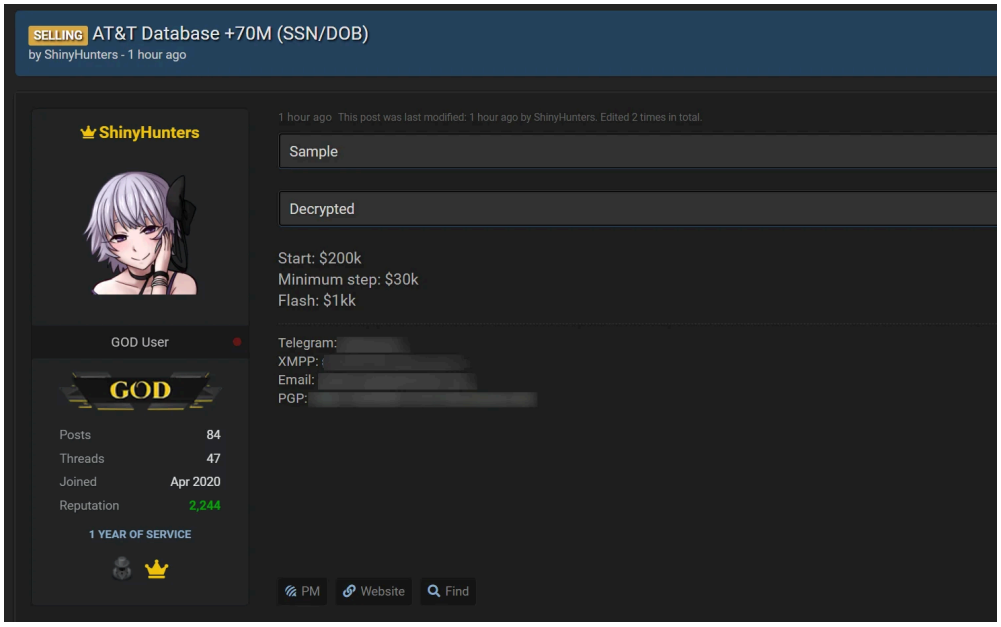
Other researchers have told BleepingComputer that ShinyHunters and Scattered Spider appear to be operating in lockstep, targeting the same industries at the same time, making it harder to attribute attacks.

Some also believe that both groups have ties to threat actors from the now-defunct Lapsus$ hacking group, with reports indicating that one of the recently arrested Scattered Spider hackers was also in Lapsus$.

Another theory is that ShinyHunters is acting as an extortion-as-a-service, where they extort companies on behalf of other threat actors in exchange for a revenue share, similar to how ransomware-as-a-service gangs operate.

This theory is supported by previous conversations BleepingComputer has had with ShinyHunters, where they claimed not to be behind a breach, but just acting as the seller of the stolen data.

These breaches include PowerSchool, Oracle Cloud, the Snowflake data-theft attacks, AT&T, NitroPDF, Wattpad, MathWay, and many more.



ShinyHunters leaking attempting to sell AT&T data breach
Source: BleepingComputer

To muddy the waters further, there have been numerous arrests of people linked to the name "ShinyHunters," including those who have been arrested for the Snowflake data-theft attacks, breaches at PowerSchool, and the operation of the Breached v2 hacking forum.

Yet even after these arrests, new attacks occur with companies receiving extortion emails stating, "We are ShinyHunters," referring to themselves as a "collective."

Protecting Salesforce instances from attacks

In a statement to BleepingComputer, Salesforce emphasized that the platform itself was not compromised, but rather, customers' accounts are being breached via social engineering.

"Salesforce has not been compromised, and the issues described are not due to any known vulnerability in our platform. While Salesforce builds enterprise-grade security into everything we do, customers also play a critical role in keeping their data safe — especially amid a rise in sophisticated phishing and social engineering attacks," Salesforce told BleepingComputer.

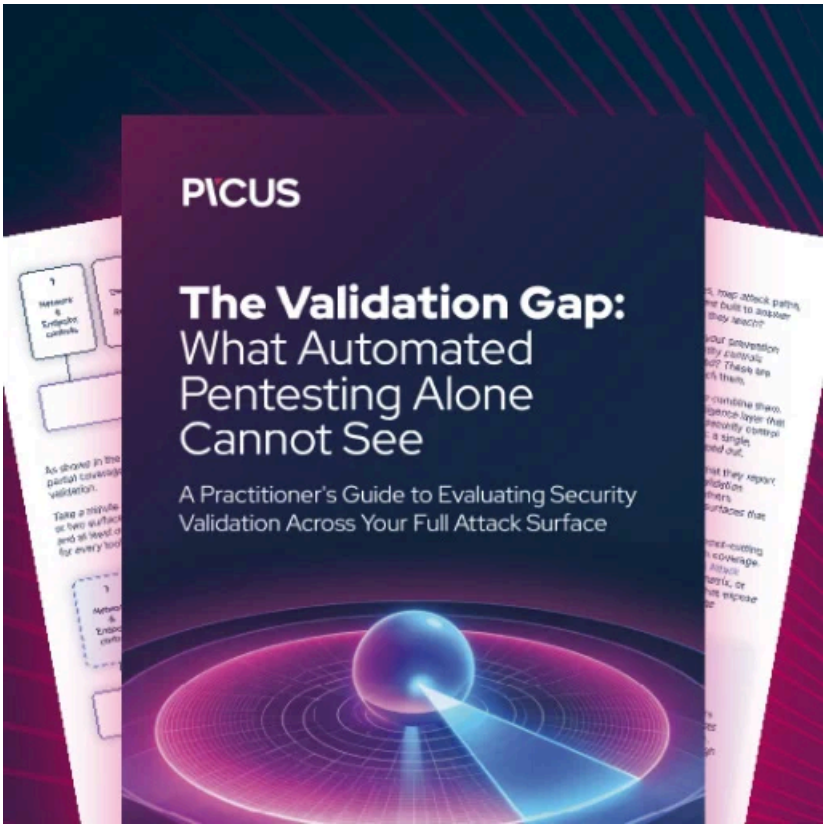
"We continue to encourage all customers to follow security best practices, including enabling multi-factor authentication (MFA), enforcing the principle of least privilege, and carefully managing connected applications. For more information, please visit: https://www.salesforce.com/blog/protect-against-social-engineering/."

Salesforce is urging customers to strengthen their security posture by:

- Enforcing trusted IP ranges for logins
- Following the principle of least privilege for app permissions
- Enabling multi-factor authentication (MFA)
- Restricting use of connected apps and managing access policies
- Using Salesforce Shield for advanced threat detection, event monitoring, and transaction policies
- Adding a designated Security Contact for incident communication

Further details on these mitigations can be found in Salesforce's guidance linked above.

Update 8/1/25: Added information from GTIG.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/