Google suffers data breach in ongoing Salesforce data theft attacks

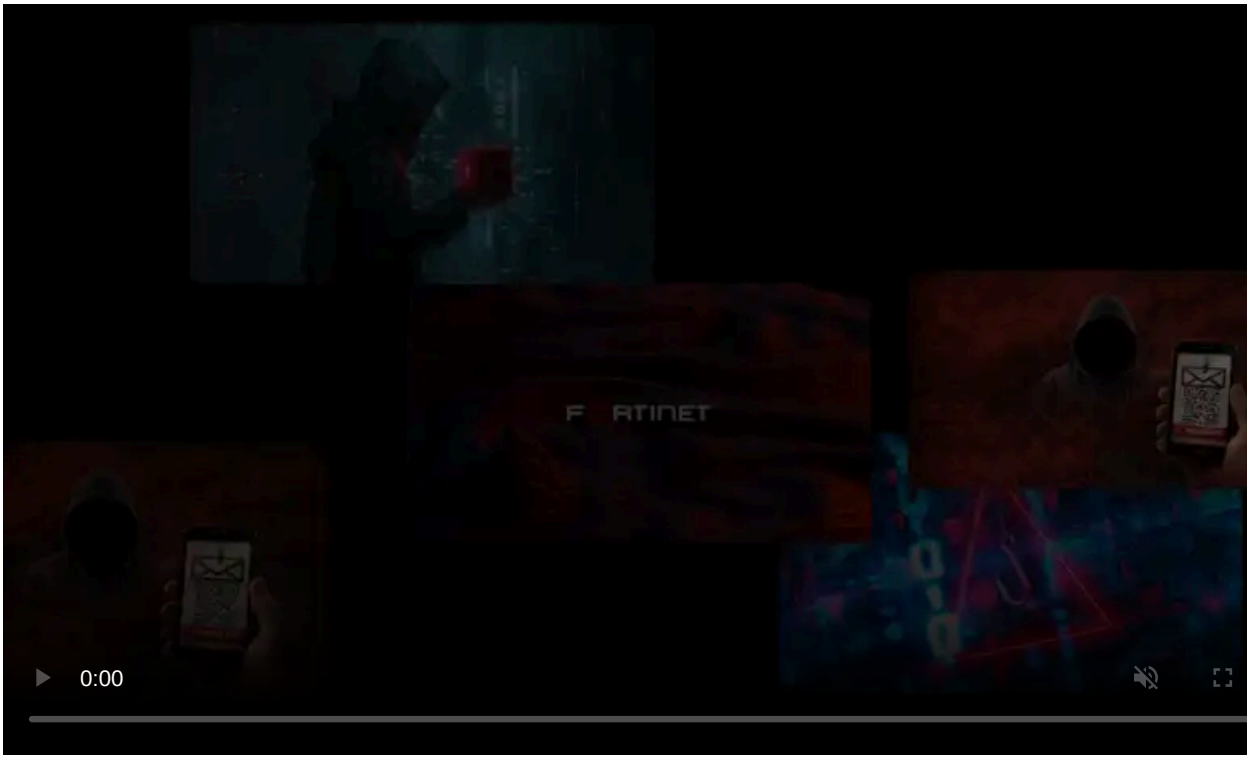
By Lawrence Abrams

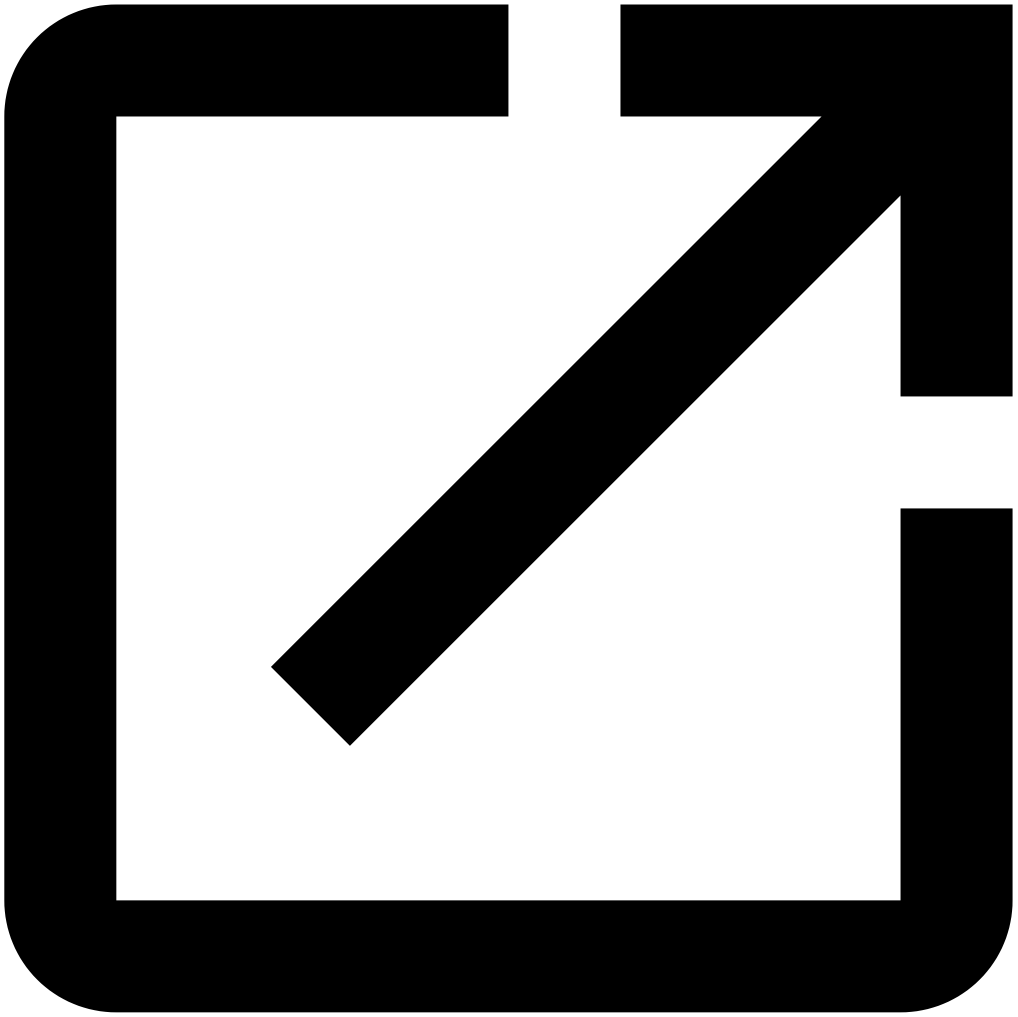
Published: 2025-08-06 · Archived: 2026-04-05 21:05:56 UTC

Google is the latest company to suffer a data breach in an ongoing wave of Salesforce CRM data theft attacks conducted by the ShinyHunters extortion group.

In June, Google warned that a threat actor they classify as 'UNC6040' is targeting companies' employees in voice phishing (vishing) social engineering attacks to breach Salesforce instances and download customer data. This data is then used to extort companies into paying a ransom to prevent the data from being leaked.

In a brief update to the article last night, Google said that it too fell victim to the same attack in June after one of its Salesforce CRM instances was breached and customer data was stolen.


F RTINET
0:00



"In June, one of Google's corporate Salesforce instances was impacted by similar UNC6040 activity described in this post. Google responded to the activity, performed an impact analysis and began mitigations," reads Google's update.

"The instance was used to store contact information and related notes for small and medium businesses. Analysis revealed that data was retrieved by the threat actor during a small window of time before the access was cut off."

"The data retrieved by the threat actor was confined to basic and largely publicly available business information, such as business names and contact details."

Google is classifying the threat actors behind these attacks as 'UNC6040' or 'UNC6240.' However, BleepingComputer, which has been tracking these attacks, has learned that a notorious threat actor known as ShinyHunters is behind the attacks.

ShinyHunters has been around for years, responsible for a wide range of breaches, including those at PowerSchool, Oracle Cloud, the Snowflake data-theft attacks, AT&T, NitroPDF, Wattpad, MathWay, and many more.

In a conversation with BleepingComputer yesterday, ShinyHunters claimed to have breached many Salesforce instances, with attacks still ongoing.

The threat actor claimed yesterday to BleepingComputer that they breached a trillion-dollar company, and were considering just leaking the data rather than attempting to extort them. It is unclear if this company is Google.

As for the other companies impacted in these attacks, the threat actor is extorting them through email, demanding they pay a ransom to prevent the data from being publicly leaked.

Once the threat actor has finished privately extorting companies, they plan to publicly leak or sell data on a hacking forum.

BleepingComputer has learned of one company that has already paid 4 Bitcoins, or approximately $400,000, to prevent the leak of their data.

Other companies impacted in these attacks include Adidas, Qantas, Allianz Life, Cisco, and the LVMH subsidiaries Louis Vuitton, Dior, and Tiffany & Co.

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.
