Google discovered a new scam—and also fell victim to it

Google said that its Salesforce instance was among those that were compromised. The breach occurred in June, but Google only disclosed it on Tuesday, presumably because the company only learned of it recently.

“Analysis revealed that data was retrieved by the threat actor during a small window of time before the access was cut off,” the company said.

Data retrieved by the attackers was limited to business information such as business names and contact details, which Google said was “largely public” already.

Google initially attributed the attacks to a group traced as UNC6040. The company went on to say that a second group, UNC6042, has engaged in extortion activities, “sometimes several months after” the UNC6040 intrusions. This group brands itself under the name ShinyHunters.

“In addition, we believe threat actors using the ‘ShinyHunters’ brand may be preparing to escalate their extortion tactics by launching a data leak site (DLS),” Google said. “These new tactics are likely intended to increase pressure on victims, including those associated with the recent UNC6040 Salesforce-related data breaches.”

With so many companies falling to this scam—including Google, which only disclosed the breach two months after it happened—the chances are good that there are many more we

don’t know about. All Salesforce customers should carefully audit their instances to see what external sources have access to it. They should also implement multifactor authentication and train staff how to detect scams before they succeed.

https://arstechnica.com/information-technology/2025/08/google-sales-data-breached-in-the-same-scam-it-discovered/