Hackers target Workday in social engineering attack

By David Jones

Published: 2025-08-19 · Archived: 2026-04-29 02:11:20 UTC

An article from CYBERSECURITY DIVE

Researchers cite increasing evidence of collaboration between Scattered Spider and the cybercrime group ShinyHunters in the campaign.

Published Aug. 19, 2025

An aerial view of Workday headquarters on Feb. 6, 2025 in Pleasanton, California. The company was targeted in a social engineering campaign that snagged a CRM vendor. Justin Sullivan via Getty Images

Workday has confirmed that it fell victim to a wide-ranging social engineering campaign that allowed hackers to access information at one of its third-party vendors.

The hackers work by impersonating IT and human-resources personnel in order to trick employees into sharing their personal information and account credentials, Workday said in a blog post published Friday.

Breaching the customer-support system gave the hackers access to support tickets that included Workday customers' names, email addresses and phone numbers, which the hackers could use to conduct further social-engineering attacks. But Workday said there was no sign that the intruders had accessed data stored on its own servers.

"All signs show that our customer Workday data remains secure," a spokesperson told Cybersecurity Dive via email.

Workday is a major AI-based platform for managing human resources and payments. More than 11,000 organizations around the world use its services, including more than 60% of the Fortune 500.

The attack follows a string of social-engineering intrusions linked to ShinyHunters, a hacker group associated with an underground cybercrime collective known as The Com. The Com also has ties to the notorious hacker team Scattered Spider, which has targeted companies in multiple industries over the past several months, including retail, insurance and aviation.

ShinyHunters has launched numerous attacks in recent months targeting Salesforce instances, according to researchers at Google. The group targeted one of Google's own Salesforce instances earlier this month.

Reliaquest recently published evidence of possible collaboration between ShinyHunters and Scattered Spider, including ticket-themed phishing domains and Salesforce credential-harvesting pages.

Workday said it has informed customers and partners about the incident with its vendor and has taken additional security measures to prevent a similar incident from happening again.

The company emphasized that it never contacts anyone by phone to request passwords or other personal information.
