ZEROFOX INTELLIGENCE

Flash

Workday Breach Linked to Social Engineering Attack

F-2025-08-20a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Social Engineering, Data Breach, Threat Actor

August 20, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 6:30 AM (EDT) on August 20, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Workday Breach Linked to Social Engineering Attack

| Key Findings

- On August 15, 2025, human resource (HR) management organization Workday announced that threat actors were able to access personally identifiable information (PII) from its unnamed third-party customer relationship management (CRM) platform via a social engineering campaign.
- Although Workday has not yet confirmed this, the attack reportedly resembles the tactics, techniques, and procedures (TTPs) seen in the recent Salesforce attacks first reported in June 2025.
- There is a roughly even chance that threat actors accessed a Workday-related database containing records of Salesforce CRM users, leading to the targeted campaign.
- Although the data exposed in this breach may not lend itself directly to extortion—given much of it is publicly accessible—it still presents significant downstream risks.

Details

On August 15, 2025, HR management organization Workday announced that threat actors were able to access PII from its unnamed third-party CRM platform via a social engineering campaign.[1] Workday is a U.S. cloud-based software platform that provides human capital management (HCM)—including HR, payroll, and talent management—and financial management solutions for businesses. Workday has more than 11,000 customers globally, representing more than 70 million users.[2]

- Workday reportedly disclosed in a separate notification to potentially affected customers that the breach was identified on August 6, nearly two weeks prior.[3]

In its August 15 blog post, Workday stated that there was no evidence that the attackers had accessed any Workday customer tenants (the isolated environments where customers' HR or financial data is stored). However, the attackers reportedly accessed PII such as names, email addresses, and phone numbers; Workday did not clarify whether the PII was associated with customers or employees.

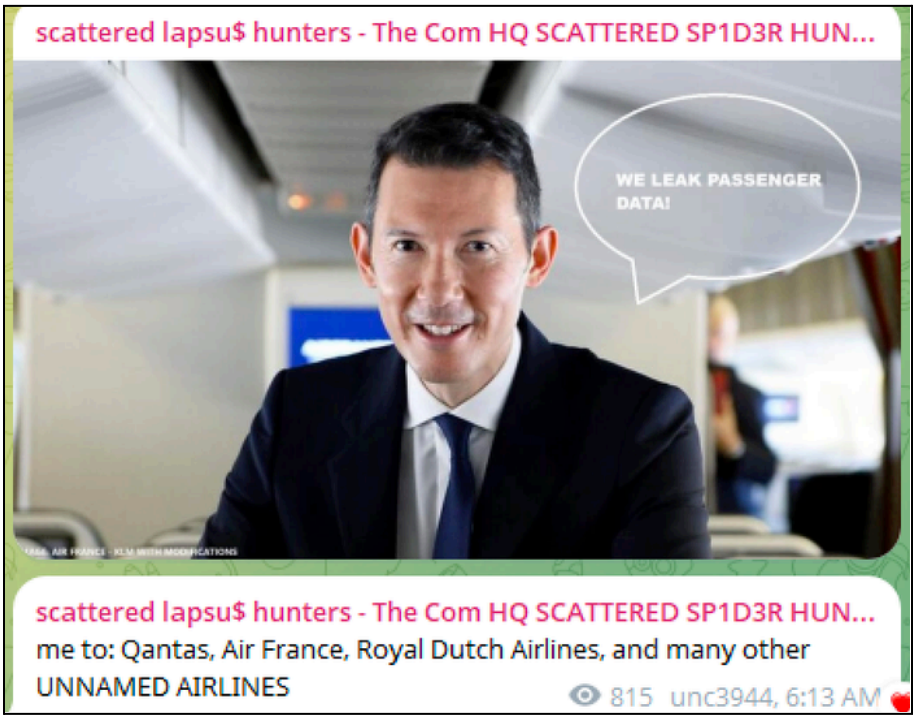
- Threat actors reportedly socially engineered either Workday or the third-party CRM employees by text or phone pretending to be from an unspecified HR or IT team, likely aiming to gain account access or PII.[4]

Although Workday has not yet confirmed this, the attack resembles the TTPs of the recent Salesforce attacks first reported in June 2025.[5] These attacks have targeted major companies across industries, including Cisco, LVMH, Chanel, Google, Pandora, and Qantas. While threat group ShinyHunters has been attributed to the alleged Salesforce

[1] hXXps://blog.workday[.]com/en-us/protecting-you-from-social-engineering-campaigns-update-from-workday.html
[2] hXXps://newsroom.workday[.]com/company-overview-customer-facts
[3] hXXps://www.bleepingcomputer[.]com/news/security/hr-giant-workday-discloses-data-breach-amid-salesforce-attacks/
[4] *Ibid.*
[5] hXXps://www.bleepingcomputer[.]com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/

campaign, TTPs similar to those used in the Workday breach have also been observed in Scattered Spider campaigns.[6]

- On August 8, 2025, a new account named "scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS" surfaced on instant messaging platform Telegram. The channel was launched by individuals claiming to be part of the prominent cybercrime collectives Scattered Spider, Lapsus$, and ShinyHunters. On August 12, 2025, this channel was banned, and another was launched in its place.
- A PGP-signed message was posted on the new Telegram channel, purportedly authored by the actor known as "Shiny" (alleged leader of the ShinyHunters group).
- Although the majority of the claims observed on both Telegram channels remain unverified, there is a roughly even chance that the launch of these Telegram channels signals an intent by Scattered Spider, ShinyHunters, and Lapsus$ to collaborate in future cybercrime operations.



Post on the new Telegram channel

Source: hXXps://t[.]me/scatteredlapsusp1d3rhunters

[6] *Ibid.*

The recent wave of Salesforce CRM-linked attacks suggests that more organizations are likely to be disclosed as victims in the coming weeks. While it is not immediately clear why threat actors are targeting Salesforce instances, the Workday campaign is likely due to the initial success of the TTPs used to target Salesforce customers.

- There is a roughly even chance that threat actors accessed a Workday-related database containing records of Salesforce CRM users, leading to the targeted campaign. The database could have been accessed either through open-source resources used for sales and market analysis or through an initial data breach at Salesforce.
- Salesforce has stated that it has not been compromised and that the ongoing attacks are not due to any known vulnerability in its technology.[7]
- Threat actors reportedly wait one month after gaining initial access to launch an extortion bid, likely indicating that more victim organizations will be publicly announced.[8]

Although the data exposed in this Workday breach may not lend itself directly to extortion—given much of it is publicly accessible—it still presents significant downstream risks. If customer or partner data has been compromised, threat actors could exploit this information to launch targeted social engineering campaigns against Workday's 11,000+ corporate clients, potentially affecting millions of end users.

- The exposed data would likely aid in credential theft of employee records, job applicant data, and internal communication.
- This access could likely facilitate further compromise, including business email compromise (BEC), wherein attackers impersonate trusted employees or vendors to manipulate financial transactions or extract additional data.

[7] hXXps://www.techradar[.]com/pro/security/hackers-breach-hr-firm-workday-is-it-the-latest-salesforce-crm-attack-victim
[8] hXXps://www.securityweek[.]com/google-discloses-salesforce-hack/

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multifactor authentication (MFA) and secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

Appendix B: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix C: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%