

Weekly Intelligence Summary

Report Date: 18.07.2025

Intelligence Cut-off Date: 18.07.2025

Weekly Focus: Confirmed third Louis Vuitton data breach reportedly linked to the same incident.

After the breaches of Louis Vuitton in Korea and in Turkey, Louis Vuitton UK confirms a third breach, which is believed to stem from the same incident.

On 2 July 2025, threat actors compromised the systems of Louis Vuitton UK and stole customer information such as names, contact details and purchase history. No bank details or other financial information were reportedly accessed.

Louis Vuitton Korea and Turkey previously confirmed similar incidents involving the theft of customer information. A breach notification was sent to customers of Louis Vuitton Korea, Turkey and the UK. It was also reportedly sent to customers in Italy and Sweden, indicating the campaign may have a wider geographic impact than initially disclosed.

These incidents are believed to be connected and attributed to ShinyHunters, a cybercriminal extortion group involved in high-profile breaches notably against Ticketmaster, AT&T and Snowflake.

The group reportedly stole data from a third-party vendor's database to compromise Louis Vuitton, indicating a realistic probability that other undisclosed Louis Vuitton branches may be impacted.

Dior, another LVMH entity, was compromised in May 2025; however, an LVMH spokesperson did not confirm whether the incidents were related.

Conversely, the retailer Adidas, also compromised in May 2025, is believed to be tied to the same incident, suggesting a likely supply chain incident.

Why It Matters...

The retail sector continues to be highly impacted by security incidents. A recent report found that the retail sector had the second most vulnerable cloud assets, highlighting the increasing implementation of cloud infrastructure, sometimes in insecure ways, and the corresponding exposure to misconfigurations and unpatched vulnerabilities.

The sector is also vulnerable to sophisticated social engineering and third-party dependencies as evidenced by the highly disruptive compromise of M&S by Scattered Spider.

The breaches at Louis Vuitton, allegedly stemming from a third-party compromise and associated with the same threat actor, evidence the sector's broader exposure to advanced and multi-layered campaigns.

Retailers are therefore recommended to strengthen network segmentation policies, implement role-based access control, notably on cloud environments, and enhance visibility over their supply chain and vendor ecosystems.

Intelligence Overview

Retail

Co-op confirmed a breach after TTPs linked to Scattered Spider were discovered. Fast action prevented ransomware deployment, but Co-op later disclosed that data of all 6.5 million members had been accessed, including names and contact details.

DragonForce claimed a ransomware breach impacting US retailer Belk, exfiltrating 150GB of internal data. Belk initiated system shutdowns, issued identity protection offers, but has not confirmed any ransom payment or negotiation.

Initial Access

Matanbuchus 3.0 has been reported as deployed via Microsoft Teams impersonation, tricking users into Quick Assist sessions to execute in-memory PowerShell loaders that deploy follow-on payloads.

Threat actors also ran a Red Bull-themed phishing operation, luring job seekers with fake vacancies. Victims were led through a CAPTCHA page to a spoofed Facebook login, enabling credential theft via exfiltration scripts.

Cybercriminal

An exploit in Google Gemini enabled prompt injection via hidden HTML, causing AI-generated summaries to display embedded phishing prompts disguised as instructions. The method used invisible styling to deceive the model.

Interlock ransomware using FileFix to deploy NodeSnake RAT through fake CAPTCHAs and staged prompts. The malware enabled data collection, lateral movement, and persistence via Cloudflare-based command and control channels.