Large Retailers Land in Scattered Spider's Ransomware Web

By Becky Bracken

Published: 2025-05-20 · Archived: 2026-04-05 18:39:44 UTC

Source: Picturelibrary via Alamy Stock Photo

Large retailers across the UK and US experiencing a high volume of calls into IT help desks regarding password resets might want to consider that they have a Scattered Spider cyberattack on their hands.

Fancy French fashion house Dior has joined the growing list of retailers falling victim to cyberattacks in recent weeks. The hack comes on the stilettos of previous breaches of Harrods, the Co-Op Group, and Marks & Spencer. Dior was compromised on May 7, and the attackers made off with the sensitive data of an undisclosed number of customers across China and South Korea.

The group broadly assumed to be behind the recent spate of cyberattacks is a loosey-goosey affiliation of English-speaking cybercriminals called Scattered Spider, also tracked as UNC3944. Known for brazenly calling up and scamming IT help desks into handing over credentials, this threat actor collective has racked up big hacks, most notably Las Vegas casinos MGM Resorts and Caesars Entertainment in 2023.

Related:Blast Radius of TeamPCP Attacks Expands Amid Hacker Infighting

Alleged members of the Scattered Spider group have been arrested, but that doesn't appear to have dampened the group's cybercrime ambitions.

Now it's 2025, and retail has become the sector of the moment for Scattered Spider. The group also swapped out its ransomware-as-a-service (RaaS) operation, trading in ALPHV/BlackCat for DragonForce. Members of the RaaS group claimed responsibility for the attacks on Marks & Spencer, Harrods, and the Co-Op Group, though it's unclear what role Scattered Spider actors may have played.

Researchers following the group have warned that suspected Scattered Spider adversaries have made a distinctive pivot from the UK to US retailers, based on recently observed malicious activity. On May 14, Google Threat Intelligence Group chief analyst John Hultquist raised eyebrows by posting a link on X to Google Mandiant threat intel on Scattered Spider, along with the ominous caption, "Shields up US retailers. They're here."

Retail Is Just the Latest Scattered Spider Target

It's not so much the retailer data the group is after; it's notoriety along with a payday, Hultquist explains. And the group can also be wily and unpredictable.

"This actor has a history of focusing their efforts on a single sector at a time, but we've also seen them abandoning an operation in the middle of an intrusion and switching their focus to a different victim in a completely unrelated industry," Hultquist says. "A part of what they want to do is to gain clout, and that can come from targeting any industry."

Related:Iran Deploys 'Pseudo-Ransomware,' Revives Pay2Key Operations

Brands like Dior and Harrods are also household names, maximizing their media impact as well, says Tim Rawlins, senior advisor and director at NCC Group. Experts also point out that retailers have historically operated with an underprotected software supply chain.

"The breaches we're seeing today often come from weaknesses that have been there for years," Dray Agha, operations manager with Huntress, says. "What's new is that attackers are now seemingly going after them more deliberately. These aren't random hits anymore; cybercriminals are picking targets they know are vulnerable and profitable."

Huntress has also observed the Scattered Spider attackers — who, it adds, are purely financially motivated — using phishing and credential abuse to either deploy ransomware or steal data, Agha notes.

Organizations can't predict when or if they will be the next Scattered Spider victim, so they need to take proactive measures to counter social engineering. This includes verifying callers, taking password resets out of the IT help desk, and using tools like Microsoft Entra self-service password reset (SSRP), which requires both multifactor verification and a secret passphrase for authentication, according to Rawlins. He also suggests using Slack or Teams to confirm a password reset.

Related:China Upgrades the Backdoor It Uses to Spy on Telcos Globally

"The good news is there are typically multiple opportunities to detect and/or deter this threat actor," Hultquist adds. "Currently, this threat actor is mostly calling help desks to reset passwords, so organizations should inform their users to reject unexpected MFA prompts, but also report that activity immediately."

About the Author

Senior Editor, Dark Reading

Becky Bracken is a senior editor with Dark Reading who brings decades of journalism experience across, radio, print, online and video channels. Becky lends her particular voice and cybersecurity expertise to the Dark Reading Confidential podcast as the host and producer, and moderates the Dark Reading editorial webinars. In addition, she oversees the site's Commentary section, hosts Dark Reading's Black Hat News Desk, and contributes regularly as a writer and reporter. Prior to joining Dark Reading, Becky covered cybersecurity and hosted webinars for Threatpost. Other national media outlets she has contributed to include PBS, SheKnows, Complex, and more.
