Harrods the next UK retailer targeted in a cyberattack

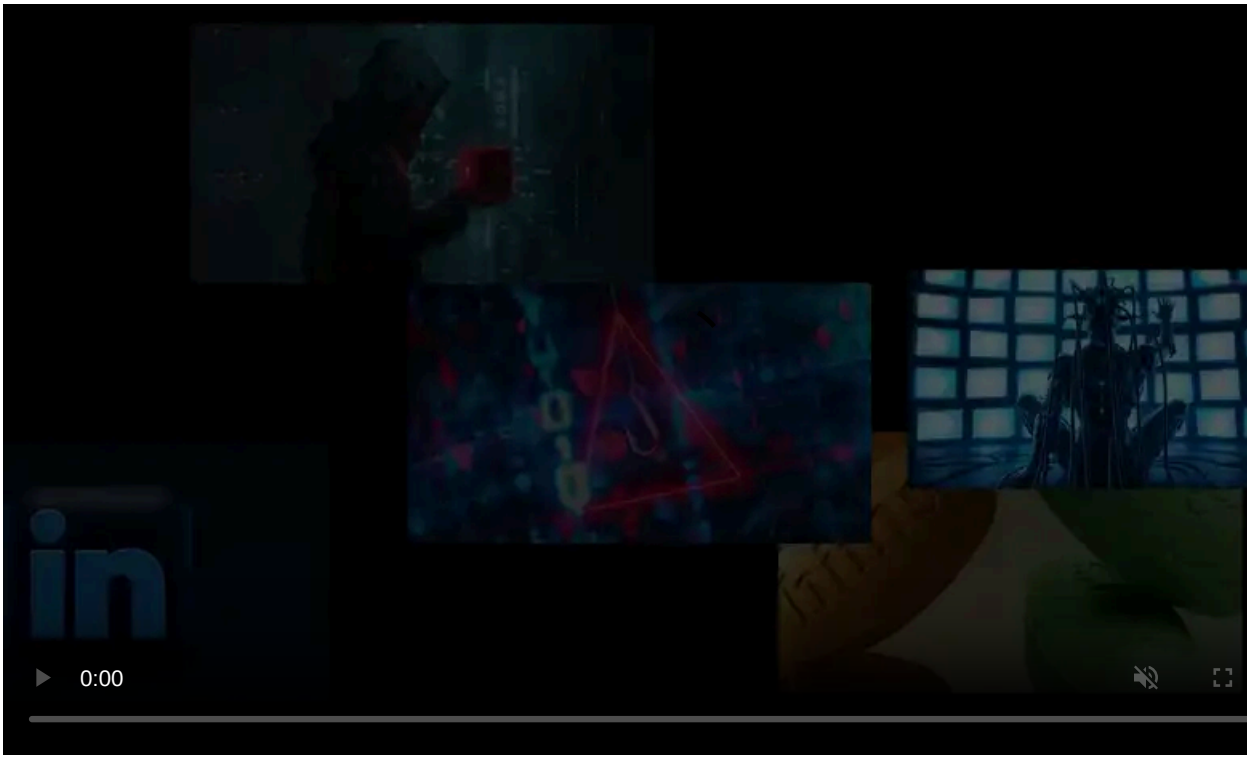
By Lawrence Abrams

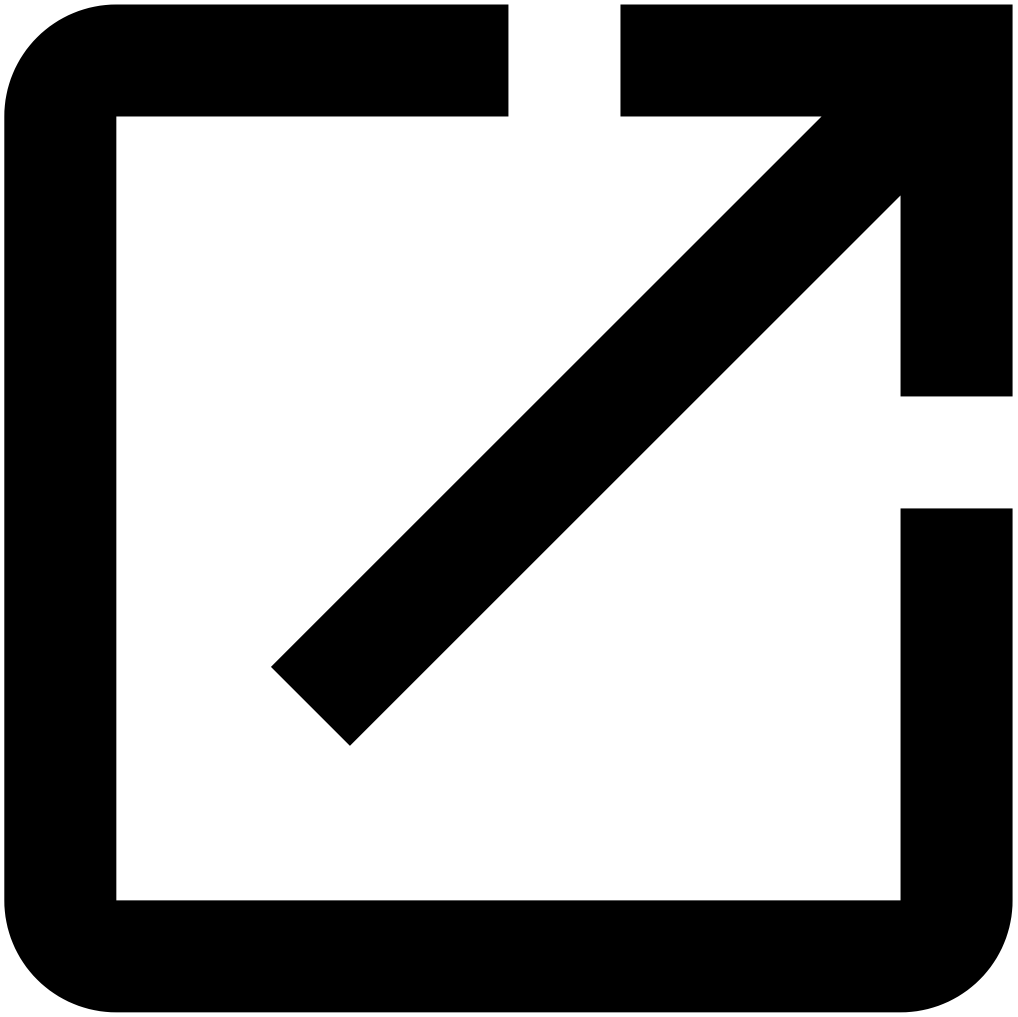
Published: 2025-05-01 · Archived: 2026-04-05 16:03:28 UTC

London's iconic department store, Harrods, has confirmed it was targeted in a cyberattack, becoming the third major UK retailer to report cyberattacks in a week following incidents at M&S and the Co-op.

In a statement shared with BleepingComputer, Harrods says threat actors recently attempted to hack into their systems, causing the company to restrict access to sites.

"We recently experienced attempts to gain unauthorised access to some of our systems," Harrods told BleepingComputer.


0:00



"Our seasoned IT security team immediately took proactive steps to keep systems safe and as a result we have restricted internet access at our sites today."

"Currently all sites including our Knightsbridge store, H beauty stores and airport stores remain open to welcome customers. Customers can also continue to shop via harrods.com."

"We are not asking our customers to do anything differently at this point and we will continue to provide updates as necessary."

Harrods has not shared any further details in response to BleepingComputer's questions, such as whether systems were breached or if data was stolen.

However, the decision to restrict access to some platforms indicates that they are actively responding to the attack.

This incident follows shortly after two other prominent UK retailers, Marks and Spencer and Co-op disclosed cyberattacks.

M&S and Co-op also hit by cyberattacks

Last week, Marks and Spencer confirmed it had suffered a cyberattack that led to disruption of its online ordering systems, contactless payments, and Click & Collect service.

BleepingComputer later confirmed the attack was linked to threat actors associated with the "Scattered Spider" tactics, who deployed the DragonForce ransomware on the company's network.

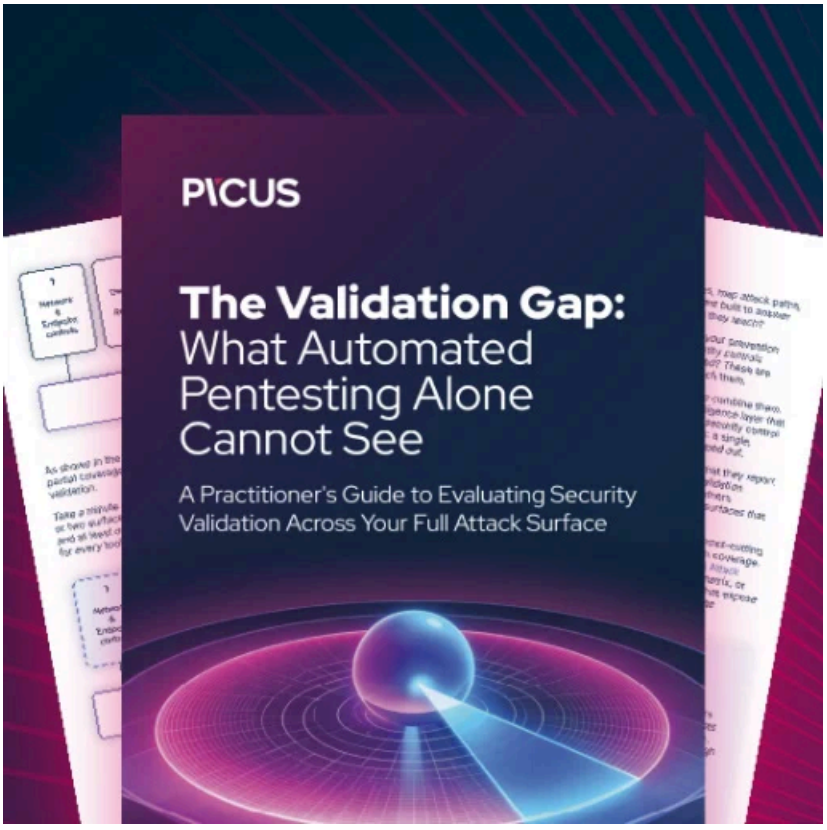
Yesterday, Co-op also disclosed a cyber incident, stating they experienced attempts to hack into their network.

However, an internal email sent by Chief Digital and Information Officer Rob Elsey and seen by ITV News indicates the breach is larger than initially stated, telling employees that VPN access was disabled and urging staff to be vigilant when using email and Microsoft Teams.

"When running a Microsoft Teams call, please ensure all attendees are as expected and that users are on camera," reads a portion of the email.

"Don't post sensitive information in the Teams chat function such as colleague, client, customer or member related data."

Law enforcement has not released an official advisory related to these attacks, but as M&S and Co-op are both believed to have started with social engineering attacks, we will likely see a bulletin released shortly.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/harrods-the-next-uk-retailer-targeted-in-a-cyberattack/