Hackers behind UK retail attacks now targeting US companies

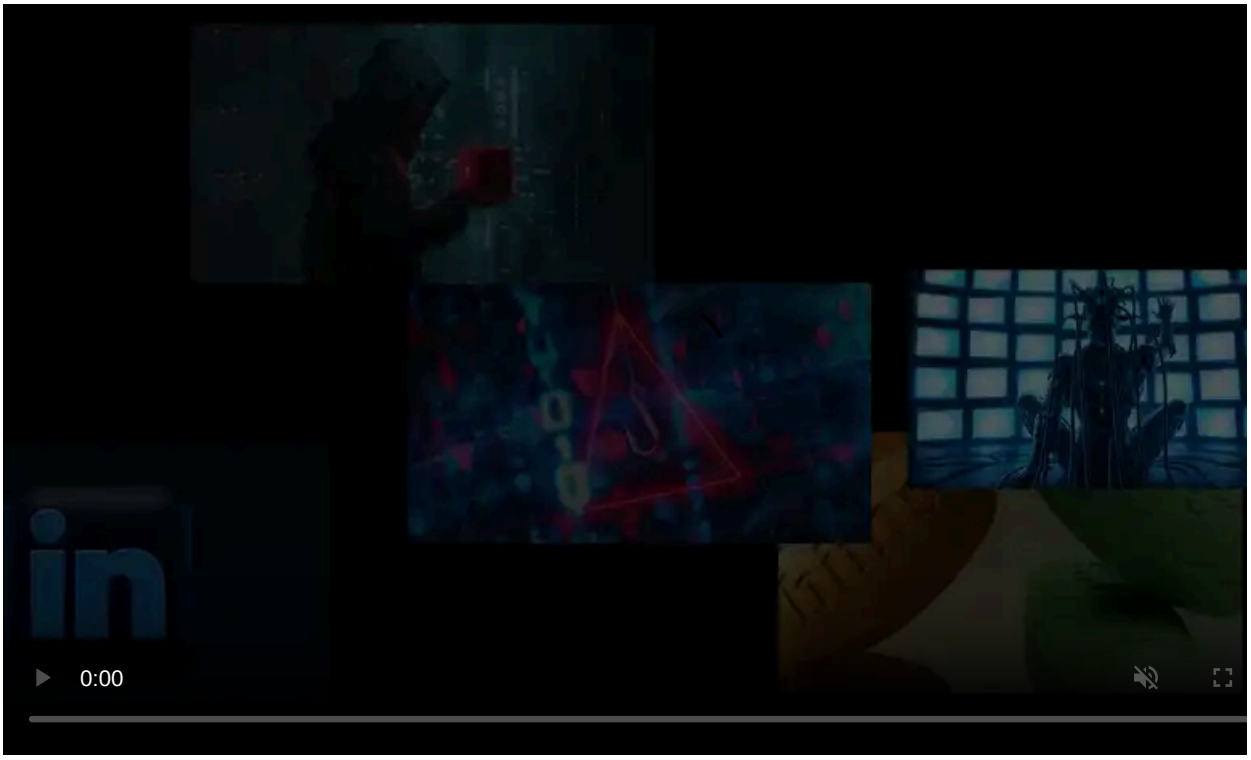
By Sergiu Gatlan

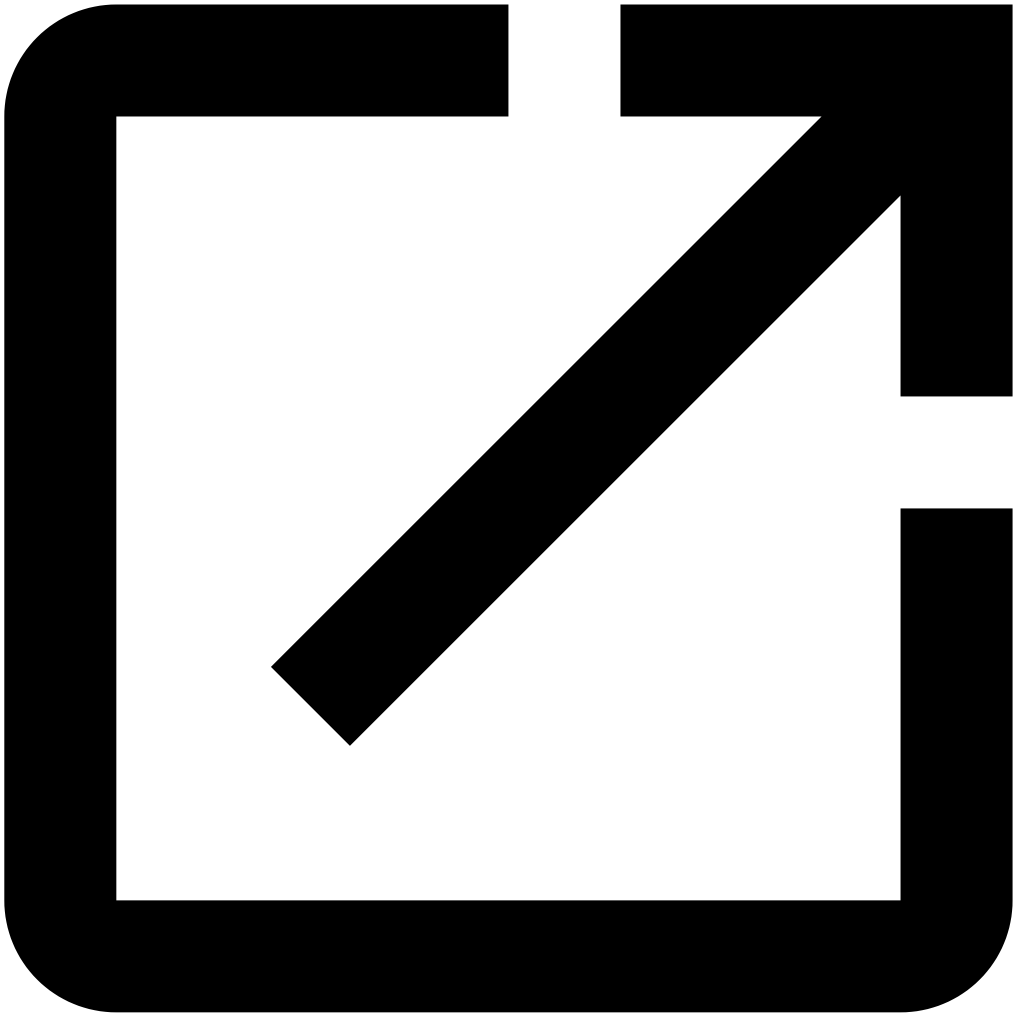
Published: 2025-05-14 · Archived: 2026-04-05 18:25:04 UTC

Google warned today that hackers using Scattered Spider tactics against retail chains in the United Kingdom have also started targeting retailers in the United States.

"The US retail sector is currently being targeted in ransomware and extortion operations that we suspect are linked to UNC3944, also known as Scattered Spider," John Hultquist, Chief Analyst at Google Threat Intelligence Group, told BleepingComputer.

"The actor, which has reportedly targeted retail in the UK following a long hiatus, has a history of focusing their efforts on a single sector at a time, and we anticipate they will continue to target the sector in the near term. US retailers should take note."


0:00



As first reported by BleepingComputer, British retail giant Marks & Spencer (M&S) was first breached in a ransomware attack where threat actors encrypted virtual machines on VMware ESXi hosts with a DragonForce encryptor. This attack was attributed to Octo Tempest, Microsoft's name for Scattered Spider.

Co-op also experienced another cyber incident, confirming that attackers stole data from many current and former members. Harrods also disclosed on May 1st that it was forced to restrict internet access to sites after attackers tried to infiltrate its network, suggesting an active response to a cyberattack even though a breach has yet to be confirmed.

The DragonForce ransomware operation has claimed all three attacks, and BleepingComputer has learned that the attackers who orchestrated them have used the same social engineering tactics linked to Scattered Spider threat actors. DragonForce surfaced in December 2023 and has recently begun advertising a new service designed to allow other cybercrime groups to white-label their services.

Since Scattered Spider started targeting UK retailers in April, the UK National Cyber Security Centre (NCSC) has published guidance to help UK organizations strengthen their cybersecurity defenses and has also cautioned that these cyberattacks should be seen as a "wake-up call", as any of them could become the next target.

The UK NCSC has yet to attribute these incidents to a specific hacking group or threat actor and said it's still working with victims to determine that.

"Whilst we have insights, we are not yet in a position to say if these attacks are linked, if this is a concerted campaign by a single actor, or whether there is no link between them at all," stated the NCSC. "We are working with the victims and law enforcement colleagues to ascertain that."

The Scattered Spider threat actors

Scattered Spider (also tracked as 0ktapus, UNC3944, Scatter Swine, Starfraud, and Muddled Libra) is a term used to describe a fluid collective of threat actors known for breaching many high-profile organizations worldwide in sophisticated social engineering attacks that also involve phishing, SIM swapping, multi-factor authentication (MFA) bombing (also known as targeted MFA fatigue).

Their attacks escalated in September 2023 when they breached MGM Resorts, using the BlackCat ransomware to encrypt over 100 VMware ESXi hypervisors after breaching the network by impersonating an employee when calling the IT help desk.

Since then, they've also acted as affiliates for various other ransomware operations, including RansomHub, Qilin, and, now, DragonForce. Other attacks linked to Scattered Spider include those on Twilio, Coinbase, DoorDash, Caesars, MailChimp, Riot Games, and Reddit.

Some Scattered Spider threat actors are also believed to be part of the "Com," a loosely connected community involved in cyberattacks and violent acts that have often attracted media attention.

These cybercriminals are as young as 16, and most are English speakers who frequent the same Telegram channels, Discord servers, and hacker forums where they plan and conduct their attacks in real time.

Although news outlets and security researchers frequently use "Scattered Spider" to describe this collective as a cohesive gang, it refers to a loosely-knit group of threat actors who use specific tactics during their attacks, making it challenging to track their activities.

"These actors are aggressive, creative, and particularly effective at circumventing mature security programs. They have had a lot of success with social engineering and leveraging third parties to gain entry to their targets," Hultquist told BleepingComputer today.

To learn more about Scattered Spider tactics and how to harden your defenses, you can review our previous reporting and a new CTM360 report.
