Marks & Spencer breach linked to Scattered Spider ransomware attack

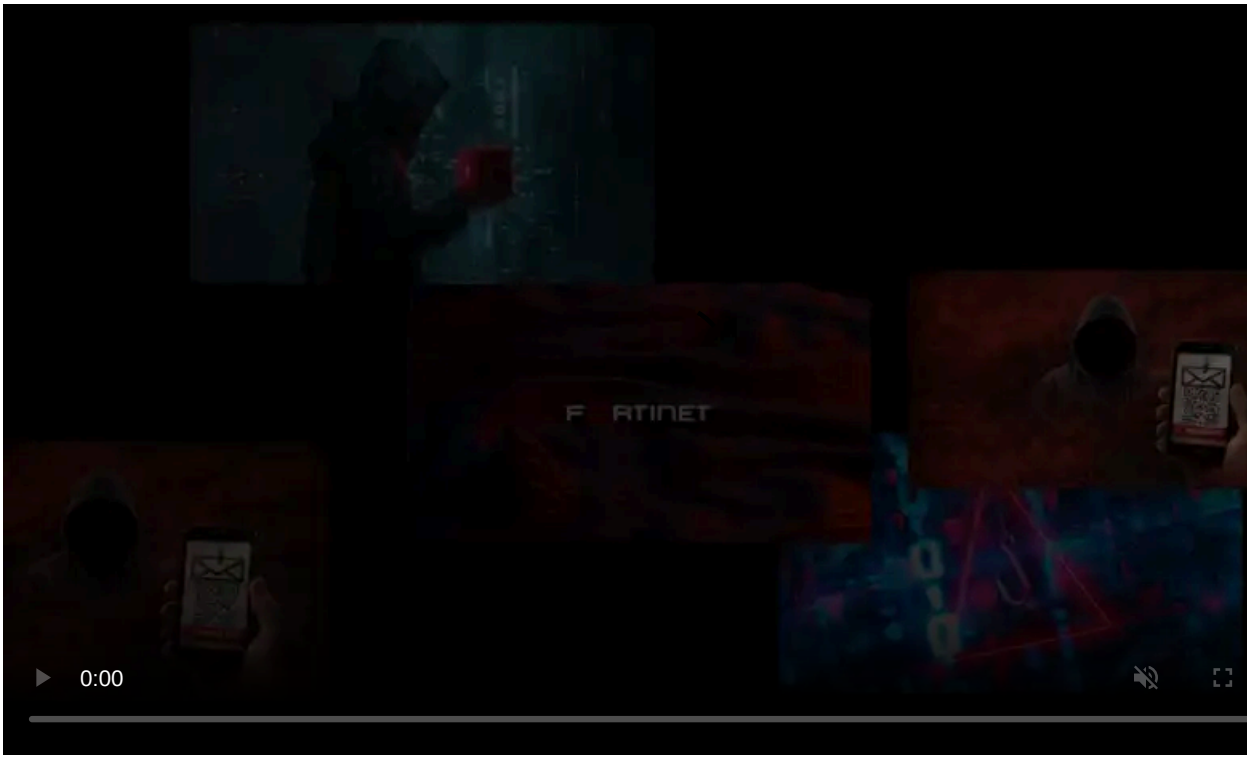
By Lawrence Abrams

Published: 2025-04-28 · Archived: 2026-04-05 23:09:42 UTC

Ongoing outages at British retail giant Marks & Spencer are caused by a ransomware attack believed to be conducted by threat actors known as "Scattered Spider" BleepingComputer has learned from multiple sources.

Marks & Spencer (M&S) is a British multinational retailer that employs 64,000 employees and sells various products, including clothing, food, and home goods in over 1,400 stores worldwide.

Last Tuesday, M&S confirmed it suffered a cyberattack that caused widespread disruption, including to its contactless payment system and online ordering. Today, Sky News reported that the disruption continues, with around 200 warehouse workers told to stay home as the company responds to the attack.


F RTINET
0:00

BleepingComputer has now learned that the ongoing outages are caused by a ransomware attack that encrypted the company's servers.

The threat actors are believed to have first breached M&S as early as February, when they reportedly stole the Windows domain's NTDS.dit file.

An NTDS.dit file is the main database for Active Directory Services running on a Windows domain controller. This file contains the password hashes for Windows accounts, which can be extracted by threat actors and cracked offline to gain access to associated plain-text passwords.

Using these credentials, a threat actor can then laterally spread throughout the Windows domain, while stealing data from network devices and servers.

Sources told BleepingComputer that the threat actors ultimately deployed the DragonForce encryptor to VMware ESXi hosts on April 24th to encrypt virtual machines.

BleepingComputer has learned that Marks and Spencer asked for help from CrowdStrike, Microsoft, and Fenix24 to investigate and respond to the attack.

The investigation so far indicates that hackers associated with tactics known as Scattered Spider, or as Microsoft calls them, Octo Tempest, are behind the attack.

When contacted with this information, M&S said that they could not go into details about the cyber incident.

Do you have information about this or another cyberattack? If you want to share the information, you can contact us securely and confidentially on Signal at LawrenceA.11, via email at lawrence.abrams@bleepingcomputer.com, or by using our tips form.

Who is Scattered Spider?

Scattered Spider, also known as 0ktapus, Starfraud, UNC3944, Scatter Swine, Octo Tempest, and Muddled Libra, is a classification of threat actors that are adept at using social engineering attacks, phishing, multi-factor authentication (MFA) bombing (targeted MFA fatigue), and SIM swapping to gain initial network access on large organizations.

These threat actors include young English-speaking people (as young as 16) with diverse skill sets who frequent the same hacker forums, Telegram channels, and Discord servers. These mediums are then used to plan and conduct attacks in real time.

Some are believed to be part of the "Com" - a loose-knit community involved in violent acts and cyber incidents that have gained wide media attention.

While the media and researchers commonly refer to Scattered Spider as a cohesive gang, it is actually used to denote threat actors who utilize certain tactics when conducting attacks. As attacks associated with Scattered Spider tactics are commonly conducted by different individuals from a loose network of threat actors, it makes it difficult to track them.

The threat actors initially started in financial fraud and social media hacks but later advanced to extremely sophisticated social engineering attacks to steal cryptocurrency from individuals or breach corporations in extortion attacks.

Scatted Spider escalated its attacks in September 2023 when they breached MGM Resorts utilizing a social engineering attack impersonating an employee when calling the company's IT help desk. In this attack, the threat actors deployed the BlackCat ransomware to encrypt more than 100 VMware ESXi hypervisors.

This was a pivotal moment in the ransomware landscape as it was the first known indication that English-speaking threat actors were working with Russian-speaking ransomware gangs.

Since then, threat actors classified as Scattered Spider have been known to act as affiliates for various ransomware operations, including RansomHub, Qilin, and now, DragonForce.

DragonForce is a ransomware operation that launched in December 2023 and has recently begun promoting a new service where they allow cybercrime teams to white-label their services.

Researchers commonly associate attacks with Scattered Spider based on specific indicators of compromise, including credential-stealing phishing attacks targeting SSO platforms, SIM swaps, social engineering attacks impersonating IT help desktop, and other tactics.

Cybersecurity firm Silent Push released a report earlier this month outlining Scattered Spider's most recent phishing attacks.

Over the past two years, law enforcement has been increasingly targeting these threat actors, arresting people in the US, the United Kingdom, and Spain.

Update 4/29/25: Updated story to make it clearer that Scattered Spider is not a specific group of individuals.
