# Scotland Yard investigates M&S cyber attack linked to teenage hacker group Scattered Spider



Scotland Yard detectives have launched an investigation into the severe IT disruption that has paralysed Marks & Spencer (M&S), with suspicions falling on a teenage hacking group known as Scattered Spider. This cyber attack, which began impacting the retailer over Easter, has now left M&S struggling to process online orders for more than a week.

The Metropolitan Police’s cyber crime unit is actively probing the incident, working alongside the National Cyber Security Centre and the Information Commissioner’s Office (ICO). A Metropolitan Police spokesman confirmed that no arrests had been made yet and that inquiries were ongoing.

Scattered Spider is an elusive collective reportedly composed of around 1,000 predominantly young men and teenagers, mainly from the UK and the US. The group has previously been implicated in timing and impactful cyber attacks on major global brands, earning a reputation for their sophisticated methods. Industry sources indicate that such criminal entities often demand ransoms on the scale of up to £10 million to restore company access to compromised IT systems.

According to the trade website Bleeping Computer, multiple sources have confirmed that Scattered Spider allegedly infiltrated M&S servers as early as February before launching their attack in earnest over the Easter period. As a consequence, M&S was forced to halt its click and collect service, preventing customers from collecting online purchases in-store.

In response to the crisis, M&S has sought assistance from technology experts at Microsoft and cybersecurity firms CrowdStrike and Fenix24 to restore their systems. The retailer has refrained from publicly commenting on the details of the attack, including whether any ransom has been paid.

Cybersecurity experts have highlighted the complexity and calculated nature of these attacks. Julius Cerniauskas from Oxylabs explained, “Their goal is simple: the greater the disruption, the greater the pressure on the firm to pay the ransom.” Ed Williams from Trustwave emphasized that such incursions require criminals who understand not only technical vulnerabilities but also human factors within large organisations. Nathaniel Jones of Darktrace described Scattered Spider as posing a “sophisticated threat,” noting that the group consists of native English speakers who exploit both technological weaknesses and manipulate personnel, particularly IT help desk staff.

Scattered Spider has been known to employ phishing attacks, sending deceptive messages to employees’ mobile phones to gain system access. The FBI has previously classified this gang as a significant threat, comparable to state-sponsored hacking groups from China and Russia.

Notable past targets of Scattered Spider include the US casino company Caesars Entertainment, which suffered a crippling attack in September 2023 and ultimately paid hackers £12 million to recover its network. The group is also known by aliases such as Scatter Swine and Muddled Libra and has been active in cyber raids since May 2022.

US authorities charged five alleged members of the gang last year, including 22-year-old Tyler Buchanan from Dundee, who was extradited to California from Spain on charges connected to attacks on casino operators. In separate probes, a 17-year-old from Walsall was arrested last July. More recently, a leading member, Noah Urban, pleaded guilty to multiple online fraud offences in a Florida court and faces up to 60 years in prison, with orders to repay over £10 million.

Commenting on the wider implications, George Weston, chairman of Associated British Foods—owner of Primark and Twinings—remarked, “All of business, certainly us, have been very aware of cyber risk for some time... We look at what’s happened [at M&S] with sadness. Whatever we can do to help, we would do – but it’s a threat to all of us.”

Meanwhile, the ongoing attack has further exacerbated difficulties for M&S. Photographs from recent days have shown empty shelves in stores, while the suspension of online orders continued for a fifth day. The company’s home and clothing division typically generates around £11 million in daily sales, with approximately one-third of this revenue coming from online transactions. The prolonged outage could therefore be causing M&S losses approaching £3.7 million each day the website remains offline.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.reuters.com/business/retail-consumer/britains-ms-says-cyber-attack-has-hit-food-availability-some-stores-2025-04-29/> - This article reports that Marks & Spencer (M&S) disclosed a cyber attack that disrupted food item availability in some of its stores, leading to the suspension of online clothing and homeware orders and issues with contactless payments and click-and-collect services over the Easter weekend.
2. <https://www.ft.com/content/1d46953a-5f2d-4395-85b9-af337a4747db> - This piece details how M&S suffered a suspected cyberattack that caused nearly £700 million to be wiped from its market valuation, with the share price dropping 7% since the incident began, and discusses the operational disruptions, including halting online clothing and homeware orders and experiencing issues with contactless payments and store returns.
3. <https://www.reuters.com/technology/cybersecurity/ms-tells-warehouse-agency-staff-stay-home-cyber-incident-continues-2025-04-28/> - This article reports that M&S instructed approximately 200 agency staff at its Castle Donington distribution center to stay home following an ongoing cyber incident that has disrupted its online operations, leading to a 5% drop in its share price.
4. <https://www.reuters.com/technology/cybersecurity/us-charges-five-scattered-spider-hacking-scheme-2024-11-20/> - This report details that U.S. prosecutors charged five individuals connected to the hacking group known as Scattered Spider, alleging their involvement in a series of phishing attacks targeting employees of various U.S. companies to steal login credentials, confidential information, and cryptocurrency.
5. <https://www.computerweekly.com/news/366616372/Brit-charged-in-US-over-Scattered-Spider-cyber-attacks> - This article discusses the charges against five individuals, including a 22-year-old British national named Tyler Robert Buchanan, over their alleged involvement in the Scattered Spider cyber attacks, detailing their use of social engineering techniques to gain access to IT helpdesks and their attacks on companies like Caesars Entertainment and MGM Resorts.
6. <https://www.bloomberg.com/news/articles/2023-10-04/clorox-suspected-of-being-hacked-by-same-scattered-spider-group-that-hit-mgm> - This article reports that Scattered Spider, the group behind the MGM and Caesars cyberattacks, is also suspected of being behind a recent cyberattack against Clorox Co., leading to a nationwide shortage of its cleaning products.
7. <https://www.dailymail.co.uk/news/article-14661627/Notorious-hackers-M-S-cyber-raid-Retail-giant-calls-Scotland-Yard-finger-pointed-gang-blackmails-firms-millions.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data