# Hackers claim responsibility for M&S and Co-op ransomware attacks as costs soar



In a striking series of events, a recent interaction between a BBC journalist and alleged hackers behind the cyberattacks on Marks & Spencer (M&S) and Co-op has unveiled unsettling details about the growing menace of ransomware in the retail sector. Joe Tidy, the journalist in question, reported receiving a Telegram message from hackers claiming responsibility for the disruption, which has left shoppers facing empty shelves and retailers scrambling to address significant data breaches.

The hackers revealed they had successfully infiltrated the systems of both retailers, stealing substantial amounts of private customer and employee information. This alarming disclosure aligns with broader reports that M&S has been grappling with a ransomware attack linked to a group known as 'Scattered Spider', which reportedly gained access as early as February 2025. According to expert analyses, this group has used the DragonForce encryptor, resulting in widespread operational chaos, severely impacting services such as online orders and contactless payments.

The urgency of the hackers' efforts appeared to stem from frustration over Co-op's handling of the ransom demands, suggesting that they had not relented in their claims. This interaction highlighted not just the technical prowess of the threat actors but also the psychological warfare employed in modern cybercrime, wherein conversations and negotiations can take a provocative turn, as evidenced by the hackers’ subsequent furious letter to Tidy.

Experts have noted that the DragonForce group, which has rebranded itself as a diversified cartel offering advanced tools for cybercriminals, embodies a new level of sophistication in ransomware operations. Their services include 24/7 support and customisation options for hackers, enhancing their already formidable reach. These innovations have emerged in a landscape marked by fierce competition among cybercriminal elements after police crackdowns on notorious groups like LockBit, which have left a power vacuum.

The ramifications of these attacks extend beyond the immediate operational disruptions; they reflect broader vulnerabilities within the retail sector and underscore an urgent need for enhanced cybersecurity measures. Estimates suggest that M&S has faced daily losses of around £30 million due to the attack, resulting in not just financial strain but operational disruptions, including significant food waste and clothing shortages.

In response to the recent spate of cyberattacks, the UK’s National Cyber Security Centre (NCSC) has issued guidance aimed at bolstering cybersecurity protocols across major retailers. This advisory highlights the necessity for robust password management practices and vigilant monitoring of systems to thwart such breaches in the future.

As the situation evolves, the complexities surrounding attribution in cybercrime remain a significant challenge. Cybersecurity experts are continuing to investigate the interplay among various groups, noting the characteristics that might indicate operational links between Scattered Spider and DragonForce. Understanding these dynamics is crucial, not just for national security, but for the integrity of consumer trust in digital retail environments.

In this era of heightened cybersecurity threats, the incident serves as a stark reminder of the need for vigilance and resilient security strategies in the face of a rapidly evolving landscape of cyber threats.

### Reference Map

* Paragraph 1: Sources [[1]](https://www.bbc.com/news/articles/cgr5nen5gxyo), [[3]](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos)
* Paragraph 2: Sources [[2]](https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/), [[4]](https://cybernews.com/news/marks-spencer-ransomware-scattered-spider-attack/)
* Paragraph 3: Sources [[1]](https://www.bbc.com/news/articles/cgr5nen5gxyo), [[6]](https://www.itv.com/news/2025-05-01/dragonforce-the-software-cyber-security-experts-believe-was-used-to-hit-m-and-s)
* Paragraph 4: Sources [[3]](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos), [[5]](https://www.bleepingcomputer.com/news/security/uk-shares-security-tips-after-major-retail-cyberattacks/)
* Paragraph 5: Sources [[5]](https://www.bleepingcomputer.com/news/security/uk-shares-security-tips-after-major-retail-cyberattacks/), [[6]](https://www.itv.com/news/2025-05-01/dragonforce-the-software-cyber-security-experts-believe-was-used-to-hit-m-and-s)
* Paragraph 6: Sources [[4]](https://cybernews.com/news/marks-spencer-ransomware-scattered-spider-attack/), [[7]](https://www.infosecurity-magazine.com/news/dragonforce-goup-ms-coop-harrods/)

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

## Bibliography

1. <https://www.bbc.com/news/articles/cgr5nen5gxyo> - Please view link - unable to able to access data
2. <https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/> - BleepingComputer reports that Marks & Spencer (M&S) experienced a ransomware attack attributed to the 'Scattered Spider' group. The attackers infiltrated M&S's systems as early as February, stealing sensitive data and deploying the DragonForce encryptor on April 24, 2025, leading to widespread disruptions in M&S's operations. The company engaged external cybersecurity experts to investigate and manage the incident, which affected online orders, contactless payments, and the Click & Collect service.
3. <https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos> - The Guardian provides an in-depth look at the aftermath of the M&S cyberattack, highlighting significant operational disruptions, including clothing shortages, food waste, and daily losses estimated at £30 million. The attack was linked to the 'Scattered Spider' group, which is believed to have used the DragonForce ransomware to cripple M&S systems under a ransomware-for-hire arrangement. The article also discusses the broader implications for the retail sector and the need for enhanced cybersecurity measures.
4. <https://cybernews.com/news/marks-spencer-ransomware-scattered-spider-attack/> - Cybernews reports that the 'Scattered Spider' ransomware group is behind the M&S cyberattack, which began over the Easter weekend. The attackers gained access to M&S's systems by extracting the NTDS.dit file from the company's Active Directory domain controller, allowing them to crack encrypted passwords and move laterally within the network. The DragonForce ransomware was then deployed, leading to significant operational disruptions, including the suspension of online orders and contactless payments.
5. <https://www.bleepingcomputer.com/news/security/uk-shares-security-tips-after-major-retail-cyberattacks/> - Following cyberattacks on major UK retailers like M&S, Co-op, and Harrods, the UK's National Cyber Security Centre (NCSC) issued guidance to strengthen cybersecurity defenses. The attacks were attributed to the DragonForce ransomware group, with M&S and Co-op breaches involving tactics associated with the 'Scattered Spider' group. The NCSC emphasized the importance of reviewing helpdesk password reset processes and other security measures to prevent similar incidents.
6. <https://www.itv.com/news/2025-05-01/dragonforce-the-software-cyber-security-experts-believe-was-used-to-hit-m-and-s> - ITV News reports that cybersecurity experts believe the DragonForce ransomware was used in the M&S cyberattack. The article discusses how DragonForce operates as a ransomware-as-a-service, offering its software to affiliates who share a percentage of the ransom. Experts highlight that such attacks often exploit known vulnerabilities and weak passwords, emphasizing the need for robust cybersecurity practices to prevent similar incidents.
7. <https://www.infosecurity-magazine.com/news/dragonforce-goup-ms-coop-harrods/> - Infosecurity Magazine examines the DragonForce group, which has been linked to cyberattacks on M&S, Co-op, and Harrods. The article discusses the group's origins as a pro-Palestine hacktivist collective and its evolution into a ransomware-as-a-service operation. It also explores the potential involvement of the 'Scattered Spider' group, noting that the attacks exhibit behavioral characteristics consistent with this collective. The piece underscores the complexity of attributing cyberattacks and the challenges in understanding the dynamics between different threat groups.