# DragonForce launches advanced ransomware attacks on UK retailers causing major disruption



Almost daily, cyber correspondent Joe Tidy finds his phone buzzing with messages from hackers across the spectrum, from the benign to the sinister. Recently, one communication stood out, leading him to engage with individuals claiming responsibility for significant cyber attacks on major UK retailers, including Marks & Spencer (M&S) and the Co-op. Over a five-hour exchange, the hackers displayed a surprising level of sophistication—fluent English and detailed evidence of the attacks they had carried out. They claimed to have stolen a considerable amount of private customer and employee information, an assertion Tidy verified before securely deleting the data.

This communication came against a backdrop of widespread disruption in UK grocery stores, where shoppers have encountered empty shelves due to these attacks. The Co-op confirmed significant data theft, affecting an estimated 6.2 million members, sparking serious security concerns; although sensitive information like financial details was left intact, the potential for targeted phishing attacks remains high. The attackers, who work under the name DragonForce, expressed frustration at the Co-op's refusal to comply with their ransom demands, which reportedly amounted to a substantial sum in Bitcoin. Following Tidy's inquiries, the Co-op swiftly acknowledged the breach, revealing it had narrowly averted a more severe situation thanks to prompt intervention in the chaos that ensued after their systems were compromised.

The DragonForce group exemplifies the emergent trends in cybercrime, particularly with their ransomware-as-a-service model that has gained traction since the downfall of other notorious entities in the space, such as LockBit. This shift allows cybercriminals to pursue their malicious activities with the backing of a support network that offers tools and infrastructure for attacks. Cybersecurity experts have noted that DragonForce has scaled its operations significantly, providing various features to affiliates, including 24/7 customer support, sophisticated client panels, and advanced negotiation tools—elements that not only enhance their operational capabilities but also their appeal to would-be attackers.

In light of the chaos triggered by these incidents, the UK's National Cyber Security Centre (NCSC) has attempted to bolster the defences of affected retailers. The NCSC’s guidance underlines the pressing need for robust cybersecurity measures, particularly in the retail sector, where hackers have diminished service availability and customer trust. Recommendations call for meticulous reviews of security protocols, especially those related to assistance systems like helpdesk password resets, which often prove vulnerable to social engineering tactics.

The recent attacks on M&S, Co-op, and other major players such as Harrods reflect a sobering reality for the retail industry. Collectively, these cyber incidents have not only disrupted services and affected organisation reputations, leading to an estimated £30 million loss in annual profits for M&S alone, but they also highlight the sector's ongoing challenges in combatting sophisticated cyber threats. As DragonForce and similar groups refine their operations, the need for enhanced cybersecurity measures has never been more crucial to protect sensitive customer data and safeguard businesses from crippling extortion.

The fallout from these attacks raises broader questions about the nature of cybercrime in the retail environment and the resilience of organisations under constant threat. As Tidy’s interactions with the hackers reveal, the landscape is shifting; power struggles amongst groups, innovative strategies for extortion, and an evolving web of crime indicate a new chapter in the dark world of cybercriminality. It serves as a reminder that the stakes for companies and consumers alike are higher than ever in this digital age.

### Reference Map

1. Paragraph 1 - [[1]](https://www.bbc.com/news/articles/cgr5nen5gxyo)
2. Paragraph 2 - [[1]](https://www.bbc.com/news/articles/cgr5nen5gxyo), [[4]](https://www.cpomagazine.com/cyber-security/the-co-op-confirms-significant-data-theft-from-an-apparent-dragonforce-ransomware-cyber-attack/)
3. Paragraph 3 - [[2]](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos), [[6]](https://www.infosecurity-magazine.com/news/dragonforce-goup-ms-coop-harrods/)
4. Paragraph 4 - [[3]](https://www.bleepingcomputer.com/news/security/uk-shares-security-tips-after-major-retail-cyberattacks/), [[4]](https://www.cpomagazine.com/cyber-security/the-co-op-confirms-significant-data-theft-from-an-apparent-dragonforce-ransomware-cyber-attack/)
5. Paragraph 5 - [[5]](https://www.itv.com/news/2025-05-01/dragonforce-the-software-cyber-security-experts-believe-was-used-to-hit-m-and-s), [[7]](https://www.retail-week.com/grocery/co-op-cyber-attack-more-extensive-than-initially-reported/7048641.article)
6. Paragraph 6 - [[6]](https://www.infosecurity-magazine.com/news/dragonforce-goup-ms-coop-harrods/), [[7]](https://www.retail-week.com/grocery/co-op-cyber-attack-more-extensive-than-initially-reported/7048641.article)

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.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos> - This article delves into the aftermath of the cyberattack on Marks & Spencer (M&S), highlighting significant disruptions such as empty shelves and online order suspensions. It discusses the financial impact, estimating a £30 million loss in annual profits, and explores the involvement of the DragonForce ransomware group, which has been linked to similar attacks on other retailers like Co-op and Harrods. The piece also touches upon the tactics used by the attackers and the broader implications for the retail sector's cybersecurity.
3. <https://www.bleepingcomputer.com/news/security/uk-shares-security-tips-after-major-retail-cyberattacks/> - Following cyberattacks on major UK retailers including Marks & Spencer, Co-op, and Harrods, the UK's National Cyber Security Centre (NCSC) issued guidance to strengthen cybersecurity defenses. The article details the nature of the attacks, the methods employed by the attackers, and the NCSC's recommendations for companies to bolster their security measures. It emphasizes the importance of reviewing helpdesk password reset processes and staying vigilant against social engineering tactics used by cybercriminals.
4. <https://www.cpomagazine.com/cyber-security/the-co-op-confirms-significant-data-theft-from-an-apparent-dragonforce-ransomware-cyber-attack/> - The Co-op confirmed a significant data theft resulting from a DragonForce ransomware attack, affecting over 6.2 million members. The stolen data includes personal details such as names and contact information, posing risks of targeted phishing attacks. However, sensitive information like account passwords and financial data were not compromised. The article discusses the company's response, the involvement of the National Cyber Security Centre (NCSC) and the National Crime Agency (NCA), and the broader implications for data security in the retail sector.
5. <https://www.itv.com/news/2025-05-01/dragonforce-the-software-cyber-security-experts-believe-was-used-to-hit-m-and-s> - Cybersecurity experts believe that the DragonForce ransomware was used in the cyberattack against Marks & Spencer (M&S). The article outlines the nature of the attack, its impact on M&S's services, and the methods employed by the attackers. It also provides background on DragonForce, including its origins and previous incidents involving the ransomware. The piece highlights the significance of the attack as one of the largest cyber incidents targeting a private UK company.
6. <https://www.infosecurity-magazine.com/news/dragonforce-goup-ms-coop-harrods/> - This article provides an in-depth look at DragonForce, the cybercriminal group linked to attacks on Marks & Spencer, Co-op, and Harrods. It discusses the group's origins, evolution, and the ransomware-as-a-service model they operate. The piece also explores the tactics used in the recent attacks, the challenges in attributing cyber incidents, and the broader implications for cybersecurity in the retail sector. Insights from cybersecurity experts are included to shed light on the group's operations and impact.
7. <https://www.retail-week.com/grocery/co-op-cyber-attack-more-extensive-than-initially-reported/7048641.article> - The article reveals that the cyberattack on Co-op was more severe than initially reported, with hackers claiming access to personal information of 20 million members. It details the evidence provided by the attackers, including screenshots of extortion messages and samples of stolen data. The piece also discusses the company's response, the involvement of the National Cyber Security Centre (NCSC), and the broader implications for cybersecurity in the retail industry.