



| Flash |

Series of Cyberattacks Target UK Retail Organizations

F-2025-05-06a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Ransomware, Threat Actor, Dark Web

May 6, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 8:30 AM (EDT) on May 6, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Series of Cyberattacks Target UK Retail Organizations

| Key Findings

- A series of prominent cyber incidents have targeted UK-based retail organizations in recent days, with Marks & Spencer (M&S), The Co-operative Group (Co-op), and Harrods allegedly implicated.
- DragonForce, a ransomware & digital extortion (R&DE) collective that operates as-a-service within deep and dark web (DDW) forums, has claimed responsibility for the attacks.
- As of the writing of this report, DragonForce's dark web [.]onion victim leak page is inaccessible, and it is unknown if M&S, Co-op, or Harrods have been named on the site.
- If DragonForce is responsible for these attacks and its extortion attempts are unsuccessful, it is very likely that stolen data will begin to be published to the collective's leak site in the coming weeks.

Details

A series of prominent cyber incidents have targeted UK-based retail organizations in recent days, beginning with the April 22, 2025, public statement from M&S previously reported by ZeroFox. Since then, both Co-op and Harrods have reported separate incidents, the details of which remain scarce as of the writing of this report.

- Initial reporting on April 22, 2025, covering the M&S cyber incident established a likely link to the Scattered Spider digital extortion collective.¹
- Reporting from April 30, 2025, indicated that Co-op had detected a network intrusion attempt, prompting a proactive shut down of some of its networks.² This was subsequently followed by a May 2, 2025, statement from a Co-op spokesperson claiming that, while some customer personally identifiable information (PII) such as names and contact details had been stolen, no passwords or personal financial information (PFI) had been compromised.³
- Reporting from May 1, 2025, indicated that iconic London department store Harrods had been implicated in a cyberattack that resulted in restricted access to its associated web domains. Little information regarding customer or supply chain impact has been disclosed.

According to a May 2, 2025, *BBC* article, the media outlet had been in contact with DragonForce ransomware-as-a-service (Raas) operatives, who had claimed responsibility for the targeting of M&S, Co-op, and Harrods. According to the operatives, information associated with up to 20 million customers that had previously signed up for a Co-op membership had been stolen. A sample comprising 10,000 lines of customer data was also allegedly shared, which included names, addresses, and contact details.⁴

DragonForce is a R&DE threat collective that was first observed on December 11, 2023. Since then, the collective had maintained a relatively low attack tempo, averaging

¹

[hXXps://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/](https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/)

²

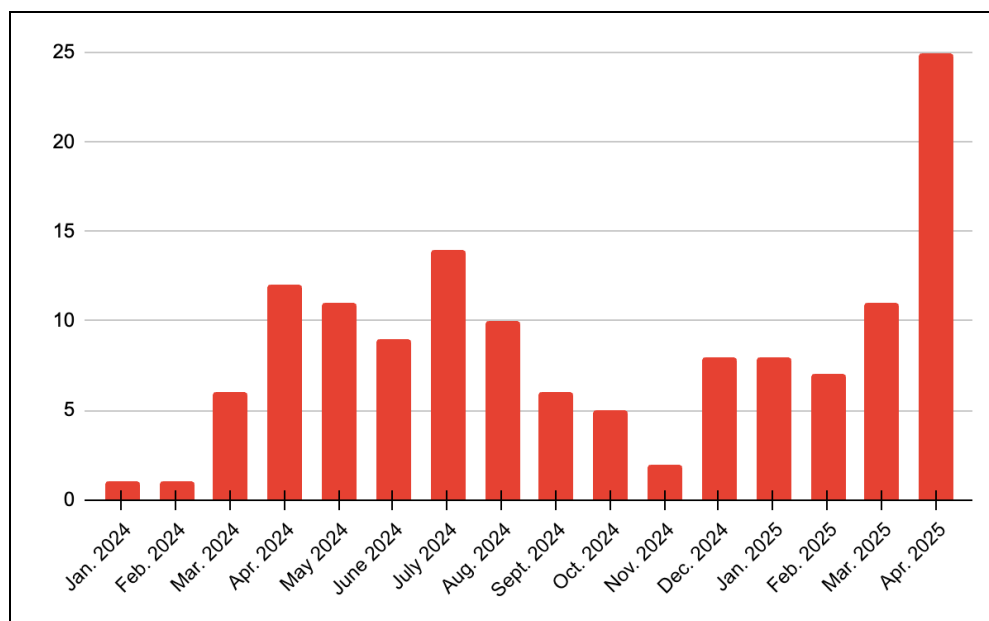
[hXXps://www.bleepingcomputer.com/news/security/uk-retailer-co-op-shuts-down-some-it-systems-after-hack-attempt/](https://www.bleepingcomputer.com/news/security/uk-retailer-co-op-shuts-down-some-it-systems-after-hack-attempt/)

³ [hXXps://www.co-operative.coop/media/news-releases/cyber-incident-update](https://www.co-operative.coop/media/news-releases/cyber-incident-update)

⁴ [hXXps://www.bbc.com/uk/news/articles/crkx3vy54nzo](https://www.bbc.com/uk/news/articles/crkx3vy54nzo)

approximately nine incidents per month. However, ZeroFox observed a significant uptick in activity beginning in early April 2025—leading to the collective’s most prominent month composed of at least 25 separate incidents.

- DragonForce has recently captivated DDW speculation surrounding its alleged relationship with RansomHub following RansomHub’s cessation of activity in early April 2025 and a series of subsequent DragonForce messages in dark web forums and victim leak pages.
- During 2024, the majority of DragonForce attacks targeted organizations located in the North America region (approximately 56 percent). However, this reduced to approximately 38 percent in Q1 2025—significantly below the 66 percent observed across the R&DE threat landscape.
- Victims located in Europe accounted for approximately 36 percent of DragonForce attacks during Q1 2025, which is higher than the average of 17 percent observed across the R&DE threat landscape.
- The majority of DragonForce attacks targeted organizations within the Manufacturing industry, comprising approximately 20 percent of the collective’s attacks. Construction and Professional services are also heavily targeted, which together with Manufacturing account for approximately 48 percent of attacks. These trends are largely consistent with averages observed across the threat landscape during Q1 2025.
- During Q1 2025, DragonForce targeted organizations within the Retail sector in approximately 3 percent of their attacks. This is notably below the threat landscape average during the same time period, which was approximately 12 percent.



DragonForce attacks by month, January 2024–April 2025

Source: ZeroFox Intelligence

Scattered Spider is a threat collective composed of native English-speaking members from Europe and the United States that was first observed in approximately May 2022. Scattered Spider does not operate an RaaS; as such, it has previously been observed leveraging ransomware associated with other prominent threat collectives—including the now-defunct ALPHV/BlackCat and Ransomhub (the most prominent R&DE collective of 2024). It is very likely that the majority of Scattered Spider activity is not attributed to the collective, as affiliates are often not involved in post-compromise negotiations.

- In 2023, Scattered Spider was responsible for R&DE attacks against two large U.S. casino operators, which reportedly resulted in total victim costs of approximately USD 115 million.⁵
- Since 2023, several U.S. and Scottish members of Scattered Spider ranging from 17–25 years old have been charged by law enforcement entities, resulting in their extradition to the United States.⁶

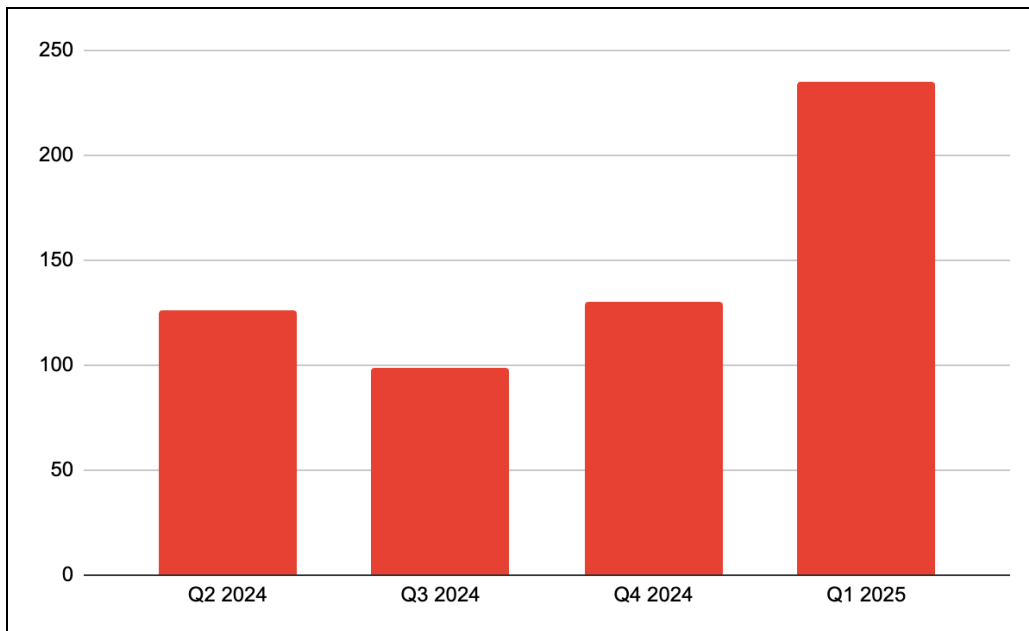
⁵

[hXXps://theweek\[.\]com/crime/scattered-spider-who-are-the-hackers-linked-to-m-and-s-and-co-op-cyberattacks](https://theweek.com/crime/scattered-spider-who-are-the-hackers-linked-to-m-and-s-and-co-op-cyberattacks)

⁶

[hXXps://www.theguardian\[.\]com/technology/2025/may/01/how-native-english-scattered-spider-group-linked-to-ms-attack-operate](https://www.theguardian.com/technology/2025/may/01/how-native-english-scattered-spider-group-linked-to-ms-attack-operate)

As of the writing of this report, DragonForce’s dark web [.]onion victim leak page is inaccessible, and it is unknown if M&S, Co-op, or Harrods have been named on the site. If DragonForce is responsible for these attacks and extortion attempts are unsuccessful, it is very likely that stolen data will begin to be published to the site in the coming weeks. Any involvement of Scattered Spider in these attacks would likely be limited to initial network breaches—likely via social engineering techniques and the delivery of DragonForce malware.

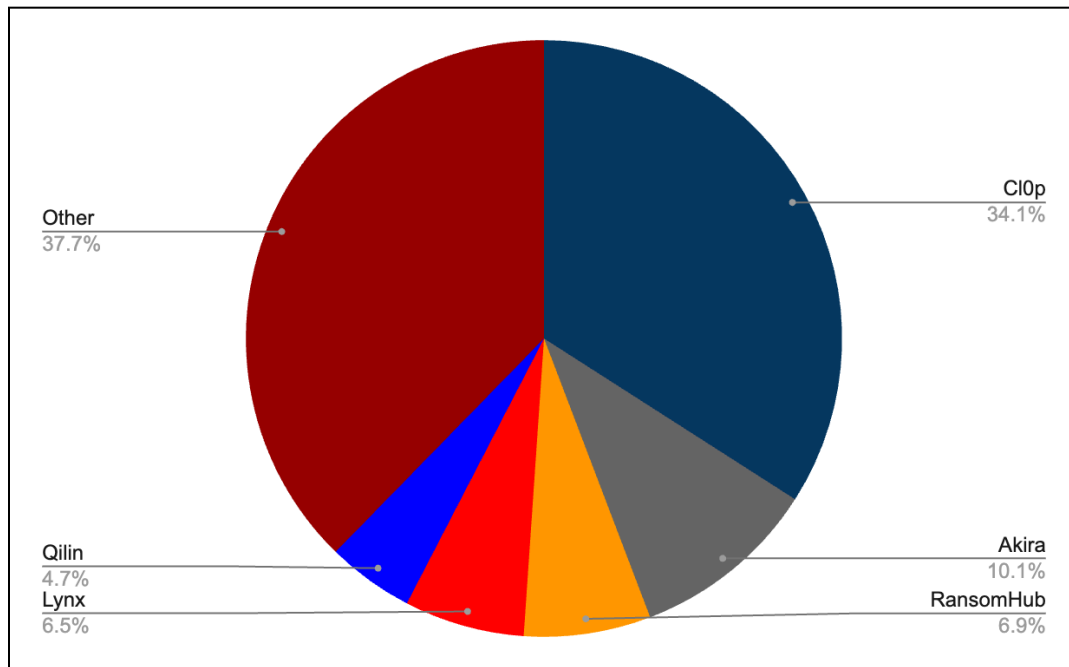


Global R&DE targeting of retail by quarter (Q2 2024–Q1 2025)

Source: ZeroFox Intelligence

According to ZeroFox research, the Retail industry has consistently been in the top five industries most targeted by R&DE attacks, accounting for 9.29 percent in 2024; Europe remains the second-most targeted region, accounting for 22.8 percent of all attacks last year (second only to North America).

- ZeroFox has observed an increase in the amount of R&DE attacks on the Retail industry from at least 130 in Q4 2024 (8.35 percent of all attacks) to at least 235 in Q1 2025 (11.93 percent of all attacks). This is partly due to an overall increase of R&DE attacks globally.
- The top five most prominent R&DE threat actors from Q1 2025 that targeted the Retail industry are CI0p, Akira, RansomHub, Lynx, and Qilin.



Retail industry victims by threat actor (2025)

Source: ZeroFox Intelligence

The UK's National Cyber Security Centre (NCSC) published a statement and multiple recommendations on its website on May 4, 2025, in response to the series of incidents. The NCSC did not specifically mention a threat actor but stated it is working with the affected organizations to "understand the nature of the attacks and to minimise the harm done by them."⁷

⁷ <https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers>

Recommendations

- Follow NCSC-issued guidance on how to improve resilience and demonstrate vigilance against malicious cyber activity targeting the Retail industry:
 - [hXXps://www\[.\]ncsc\[.\]gov\[.\]uk/blog-post/incidents-impacting-retailers](https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers)
- Ensure employees are educated as to contemporary Scatter Spider social engineering tactics, techniques, and procedures (TTPs), such as multi-factor authentication (MFA) fatigue attacks.
- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant MFA, secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use

TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may ONLY share

TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share

TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%