ZEROFOX INTELLIGENCE

Flash

Arrests Made in Relation to UK Retail Cyber Attacks

F-2025-07-11a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Cyber Threat Actor, Digital Extortion, Law Enforcement

July 11, 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 09:00 AM (EST) on July 11, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Arrests Made in Relation to UK Retail Cyber Attacks

| Key Findings

- On July 10, 2025, four people were reportedly arrested in the United Kingdom as part of a National Crime Agency (NCA) investigation into a series of cyberattacks that occurred in late April 2025, targeting retail stores Marks & Spencer (M&S), Co-op, and Harrods.
- The series of cyberattacks targeting UK-based retail organizations began in mid-April 2025 when M&S publicly confirmed that it was managing an unspecified cyber incident.
- Initially, no cyber threat entity publicly claimed responsibility for the attacks, but widespread reporting alluded to the "Scattered Spider" threat collective being the perpetrators.
- If the arrested individuals are associated with Scattered Spider, it is likely that the collective's operational tempo will reduce—particularly in the short term—with targeting pivoting toward industries and regions less likely to garner media and law enforcement attention.

Details

On July 10, 2025, four people were reportedly arrested in the United Kingdom as part of an NCA investigation into a series of cyberattacks that occurred in late April 2025, targeting retail stores M&S, Co-op, and Harrods. Three male teenagers and one twenty-year-old woman were arrested on suspicion of offences related to the Computer Misuse Act 1990, blackmail, money laundering, and participating in the activities of an organised crime group.[1]

- This follows the widely-reported June 2025 arrests of individuals thought to be associated with the prominent deep and dark web (DDW) alias "ShinyHunters," as well as the reported February 2025 arrest of "IntelBroker."

The series of cyberattacks targeting UK-based retail organizations began in mid-April 2025, when M&S publicly confirmed that it was managing an unspecified cyber incident. This was followed by early May 2025 statements from Harrods and Co-op, which both disclosed that they had also been implicated in cyberattacks.[2][3][4] Initially, no cyber threat entity publicly claimed responsibility for the attacks, but widespread reporting alluded to the Scattered Spider threat collective being the perpetrators.[5] As of the writing of this report, the NCA has not stated whether the arrested individuals are suspected of being associated with Scattered Spider.

- In the weeks following the initial attacks against UK-based retail organizations, multiple reporting sources suggested that the attackers had shifted their focus toward U.S.-based organizations—first targeting those in the retail sector, followed

[1] hXXps://www.nationalcrimeagency[.]gov[.]uk/news/retail-cyber-attacks-nca-arrest-four-for-attacks-on-m-s-co-op-and-harrods
[2] hXXps://www.reuters[.]com/business/retail-consumer/british-retailer-ms-discloses-cyber-incident-2025-04-22/
[3] hXXps://www.reuters[.]com/business/retail-consumer/harrods-is-latest-british-retailer-be-hit-by-cyber-attack-2025-05-01/
[4] hXXps://www.co-operative[.]coop/media/news-releases/cyber-incident-update
[5] hXXps://www.bleepingcomputer[.]com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/

by those in the insurance sector.[67] ZeroFox did not observe a wider increase in the targeting of these industries by digital extortion collectives during this time.

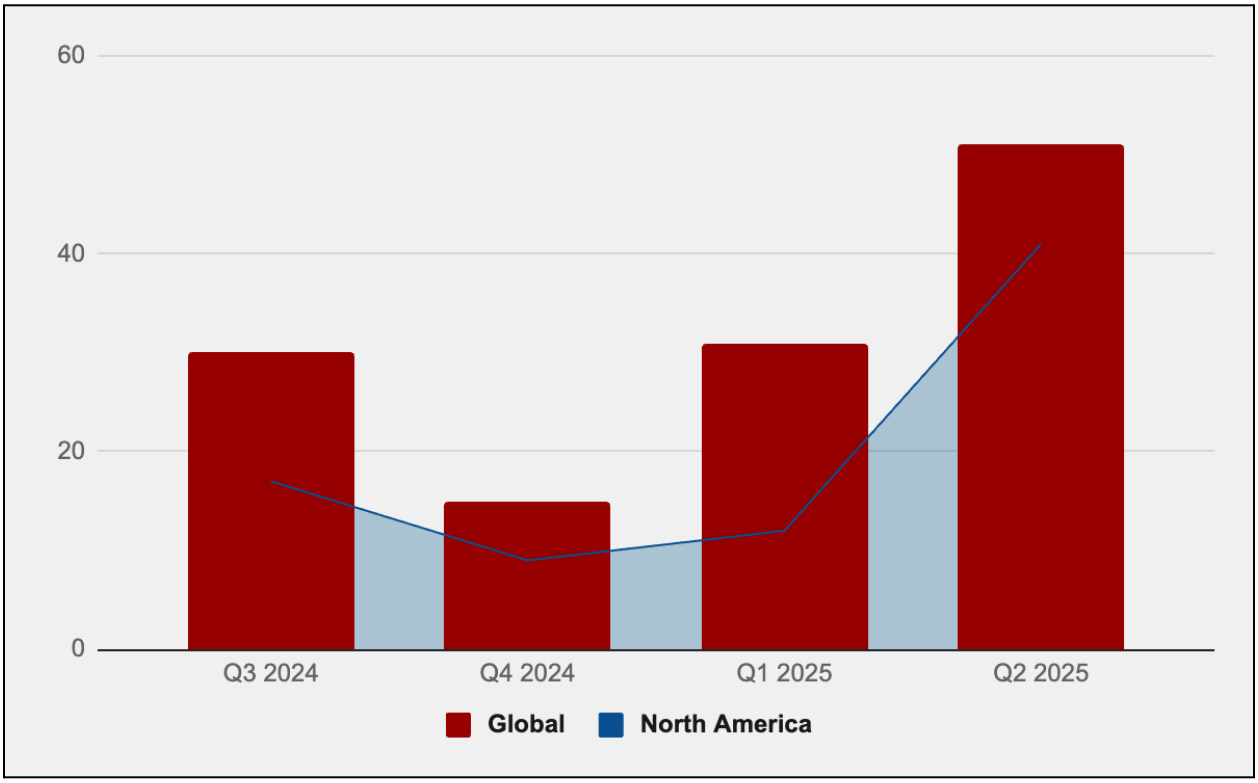
Scattered Spider is a threat collective composed primarily of native English-speaking members located in Europe and North America–first observed in approximately May 2022. Since its inception, the collective has been observed leveraging various different prominent ransomware strains in digital extortion attacks, including the now-defunct ALPHV/BlackCat and RansomHub, as well as DragonForce.[8]

- Scattered Spider has been observed exhibiting a high operational tempo, as well as the ability to quickly adjust regional and industry targeting preferences.
- The collective also leverages a highly-sophisticated and diverse offensive toolkit, manifested by targeted social engineering techniques, extensive reconnaissance, exploitation of contemporary security vulnerabilities, and the ability to exfiltrate large quantities of victim data.
- Since 2023, several alleged American and Scottish members of Scattered Spider, ranging from 17-25 years of age, have been charged by law enforcement entities for their alleged involvement, resulting in their reported extradition to the United States.[9]

According to a *BBC* article published on May 2, 2025, 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.[10] DragonForce is a ransomware and digital extortion (R&DE) threat collective first observed in December 2023. Since then, the collective has maintained a relatively low attack tempo, averaging approximately 10 incidents per month. However, ZeroFox observed a significant uptick in activity in early April 2025—leading to the collective's most prominent month, which involved at least 25 separate incidents. This was repeated in June 2025.

6 hXXps://www.theguardian[.]com/technology/2025/may/16/scattered-spider-hackers-uk-cyber-attacks-google-us-retailers
7 hXXps://www.bleepingcomputer[.]com/news/security/google-warns-scattered-spider-hackers-now-target-us-insurance-companies/
8 hXXps://www.culture[.]ai/resources/blog/scattered-spider-and-dragonforce
9 hXXps://www.theguardian[.]com/technology/2025/may/01/how-native-english-scattered-spider-group-linked-to-ms-attack-operate
10 hXXps://www.bbc[.]co[.]uk/news/articles/crkx3vy54nzo

- In 2024, the majority of DragonForce attacks targeted organizations located in the North America region (approximately 56 percent). This increased to 84 percent in Q2 2025—significantly above the 57 percent observed across the R&DE threat landscape. Manufacturing was the collective's most targeted industry in Q2 2025, accounting for approximately 16 percent of the collective's attacks. However, this is slightly below broader R&DE targeting proportions.



DragonForce attacks by quarter

Source: ZeroFox Intelligence

As of the writing of this report, it is unclear whether the arrested individuals are associated with the Scattered Spider collective, though there is a roughly even chance that any connection will either be confirmed or denied by law enforcement entities upon gathering sufficient evidence. The size and structure of Scattered Spider is largely unknown; accordingly, the subsequent impact of the arrests upon the collective's operational tempo cannot be deduced. However, it is likely that attributed attacks will reduce—particularly in the short term—with targeting pivoting toward industries and regions less likely to garner media and law enforcement attention.

Numerous prominent cyber threat entities—including ransomware collectives, individuals, and those associated with DDW hacking forums—have been targeted in large-scale law enforcement operations in the past year. Such activity is very likely to prolong a previously observed trend of cyber threat actors demonstrating increased caution surrounding operating procedures, online security, forum affiliations, and skepticism of peers.

Recommendations

- 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 multi-factor authentication (MFA), establish 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 tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**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.	**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	Clear
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.	**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%