



| Flash |

Marks & Spencer Cyber Incident

F-2025-04-30b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Actor, Digital Extortion

April 30, 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 8:00 AM (EDT) on April 30, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Marks & Spencer Cyber Incident

| Key Findings

- On April 22, 2025, Marks & Spencer (M&S), one of the United Kingdom's leading retailers, publicly confirmed that it was managing a cyber incident.
- While M&S has not officially stated a cyberattack has occurred, the characteristics observed in this incident are consistent with ransomware attacks.
- Investigations remain ongoing, with M&S confirming it has called in the UK's National Cyber Security Centre to assist in containing and resolving the incident. M&S has also reported the incident to the Information Commissioners Officer (ICO).
- The M&S cyber incident highlights the growing cybersecurity risks faced by the UK retail sector. Disruption to services critical to customer experience can have an immediate impact on reputation and consumer trust.

| Details

On April 22, 2025, Marks & Spencer, one of the UK's leading retailers, publicly confirmed that it was managing a cyber incident.¹ As part of subsequent containment efforts, M&S paused online orders across the UK and Ireland. Although stores remained open and online browsing accessible, this cyber incident led to publicly noticeable service disruptions across multiple services critical to customer experience and business operations.

Customers were forced to use the chip and pin method or cash for in-store transactions, as contactless payment services were disrupted. Although online browsing remains available, M&S has restricted all transactional services to protect systems.²

M&S shares experienced volatility since the announcement of the cyber incident, dropping approximately 5 percent.³ Since the reported cyber incident, customers have publicly expressed dissatisfaction on social media platforms.⁴ In response to the growing frustration, CEO Stuart Machin issued a public apology to customers, acknowledging the disruption and highlighting that the business is taking proactive steps to contain and resolve the incident.⁵

Investigations remain ongoing, with M&S confirming it has sought the UK's National Cyber Security Centre's assistance in containing and resolving the incident.⁶ M&S has also reported the incident to the Information Commissioners Officer (ICO).⁷

¹ [hXXps://www.reuters\[.\]com/business/retail-consumer/british-retailer-ms-discloses-cyber-incident-2025-04-22/](https://www.reuters.com/business/retail-consumer/british-retailer-ms-discloses-cyber-incident-2025-04-22/)

² [hXXps://www.theguardian\[.\]com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders](https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders)

³ [hXXps://corporate.marksandspencer\[.\]com/investors/our-performance-updates/share-price](https://corporate.marksandspencer.com/investors/our-performance-updates/share-price)

⁴ [hXXps://x\[.\]com/rut85826/status/1916813798540824818](https://x.com/rut85826/status/1916813798540824818)

⁵

⁶ [hXXps://www.theguardian\[.\]com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders](https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders)

⁷ [hXXps://www.itpro\[.\]com/business/m-and-s-calls-in-ncsc-after-cyber-incident-disrupts-customer-payments-online-orders](https://www.itpro.com/business/m-and-s-calls-in-ncsc-after-cyber-incident-disrupts-customer-payments-online-orders)

⁷ [hXXps://www.bbc\[.\]co\[.\]uk/news/articles/c9djvzwn858o](https://www.bbc.com/news/articles/c9djvzwn858o)

| Analyst Commentary

While M&S has not officially confirmed a cyberattack occurred, the disruption of online services and payments—coupled with the pre-emptive suspension of online orders and lack of publicly available detail around the nature of the incident—indicate a likely chance that this incident is linked to a ransomware attack. Reports have emerged suggesting threat collective Scattered Spider, a financially motivated threat group known for targeting large organizations using social engineering and extortion tactics, may be behind the attack. However, attribution to this threat collective remains unconfirmed as of this writing.

The M&S cyber incident highlights the growing cybersecurity risks faced by the UK retail sector. Disruption to services critical to customer experience can have an immediate impact on reputation and consumer trust. As retailers continue to expand their digital operations, they become increasingly appealing to threat actors seeking to disrupt critical operations, compromise sensitive customer data, or exploit vulnerabilities. In an increasingly competitive retail space, safeguarding customer information and preserving the availability of services is essential even in the midst of a cyber incident, not only for regulatory compliance but also to protect brand image and maintain customer trust.

| Scattered Spider Overview

Scattered Spider is a financially motivated threat collective that conducts advanced social engineering and digital extortion attacks and was first observed in approximately May 2022. The collective—which is composed of native English-speaking members from Europe and the United States—has been observed collaborating with other prominent extortion collectives, such as RansomHub and the now-defunct ALPHV/BlackCat.⁸

Scattered Spider campaigns are well-organized and prolific. The group exhibits a high operational tempo and fluidity, leveraging an extensive toolkit to compromise and maintain persistence in secure environments and rapidly exfiltrating large volumes of data.

⁸ [hXXps://www.cisa\[.\]gov/news-events/cybersecurity-advisories/aa23-320a](https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a)

High-profile incidents attributed to Scattered Spider include attacks on Twilio, MGM Resorts, and Caesars Entertainment. In August 2022, the collective compromised Twilio via SMS phishing, gaining access to the personal information of 163 Twilio customers.⁹ In September 2023, Scattered Spider used help desk impersonation to breach MGM Resorts, deploying ransomware that caused outages across hotel and casino services.¹⁰ Around this same time, the group accessed sensitive customer data from Caesar Entertainment and extorted a USD 15 million ransom to prevent leaking of the data.¹¹

Scattered Spider performs highly targeted social engineering attacks and leverages various techniques, including voice phishing (vishing) and SMS phishing (smishing) using victim-specific crafted domains and SIM-swapping to harvest credentials and bypass multi-factor authentication (MFA). Scattered Spider also utilizes Azure Data Factory to alter data pipelines and facilitate the extraction of large data volumes.¹²

These tactics reveal the group's focus on deep, persistent network infiltration, which often outmaneuvers traditional security systems. Scattered Spider leverages common endpoint detection and response (EDR) tools installed on victim networks to maintain endpoint access. The group exploits these tools' remote-shell capabilities and executes commands that elevate access.¹³

Consistent with typical ransomware operations, Scattered Spider frequently communicates with victim organizations and their personnel directly after encryption to negotiate or extort the ransom, providing samples of exfiltrated data. The group has historically been observed leveraging the now defunct-ALPHV data leak site as part of its extortion attempts.¹⁴

⁹

⁹ [hXXps://www.twilio\[.\]com/en-us/blog/august-2022-social-engineering-attack](https://www.twilio.com/en-us/blog/august-2022-social-engineering-attack)

¹⁰

¹⁰ [hXXps://westoahu.hawaii\[.\]edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/](https://westoahu.hawaii[.]edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/)

¹¹

¹¹ [hXXps://www.cnbc\[.\]com/2023/09/14/caesars-paid-millions-in-ransom-to-cybercrime-group-prior-to-mgm-hack.html](https://www.cnbc[.]com/2023/09/14/caesars-paid-millions-in-ransom-to-cybercrime-group-prior-to-mgm-hack.html)

¹²

¹² [hXXps://cloud.google\[.\]com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware](https://cloud.google[.]com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware)

¹³

¹³ [hXXps://blog.electiciaq\[.\]com/ransomware-in-the-cloud-scattered-spider-targeting-insurance-and-financial-industries](https://blog.electiciaq[.]com/ransomware-in-the-cloud-scattered-spider-targeting-insurance-and-financial-industries)

¹⁴ [hXXps://www.cisa\[.\]gov/news-events/cybersecurity-advisories/aa23-320a](https://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-320a)

Scattered Spider's techniques—such as tampering with security personnel accounts to impair security products and automatically delete emails—indicate high technical prowess, making it harder for traditional security measures to detect or prevent the group's activities.

| Appendix A: Associated Tools

The following list of tools associated with Scattered Spider is based on publicly available reporting and should not be considered conclusive or exhaustive. The collective adapts its tactics, techniques, and procedures (TTPs) regularly and will almost certainly continue to add new tools and techniques to its arsenal. Scattered Spider has been observed abusing the following legitimate tools:

- AnyDesk
- ASG Remote Desktop
- BeAnywhere
- Domotz
- DWservice
- Fixme[.]it
- Fleetdeck[.]io
- Hekatombe
- Italian Endpoint Manager
- Lazagne
- Level[.]io
- Logmein
- ManageEngine
- Mimikatz
- N-Able
- Ngrok
- PDQConnectAgent
- Pulseway
- Rport
- Rsocx
- ScreenConnect
- Sorillus
- Splashtop
- SSH RevShell
- Teamviewer
- TrendMicro Basecamp
- Trufflehog
- ZeroTier
- Zoho Assist

Scattered Spider has also been observed deploying the following malware:

- ALPHV/BlackCat Ransomware
- Meduza Stealer
- POORTRY
- Racoon Stealer
- Ratty
- TONESTOP
- Vidar Stealer
- WarZoneRAT

| Appendix B: Indicators of Compromise (IOCs)

The following IOCs have been publicly attributed to Scattered Spider activities:

IPV6

- 2a01:4f8:200:1097::2

IPV4

- 104.247.82[.]11
- 144.76.136[.]153
- 105.101.56[.]49
- 105.158.12[.]236
- 134.209.48[.]68
- 137.220.61[.]53
- 138.68.27[.]0
- 146.190.44[.]66
- 149.28.125[.]96
- 157.245.4[.]113
- 159.223.208[.]47
- 159.223.238[.]0
- 162.19.135[.]215
- 164.92.234[.]104
- 165.22.201[.]77
- 167.99.221[.]10
- 172.96.11[.]245
- 185.56.80[.]28
- 188.166.92[.]55
- 193.149.129[.]177
- 207.148.0[.]54
- 213.226.123[.]104
- 35.175.153[.]217
- 45.156.85[.]140
- 45.32.221[.]250
- 64.227.30[.]114
- 79.137.196[.]160

- 92.99.114[.]231
- 195.35.10[.]222
- 149.248.14[.]222
- 149.28.105[.]251
- 216.128.128[.]163
- 155.138.227[.]80
- 149.28.41[.]193
- 140.82.29[.]65
- 149.248.12[.]179
- 45.32.66[.]91
- 162.33.178[.]245
- 207.246.106[.]194
- 45.63.54[.]8
- 45.76.65[.]42
- 144.202.114[.]128
- 45.76.172[.]113
- 45.32.64[.]247
- 149.248.0[.]189
- 104.207.153[.]50
- 45.63.53[.]99
- 149.28.66[.]216
- 149.28.80[.]155
- 45.63.52[.]43

SHA-1

- b2f955b3e6107f831ebe67997f8586d4fe9f3e98
- 91568d7a82cc7677f6b13f11bea5c40cf12d281b
- 994e3f5dd082f5d82f9cc84108a60d359910ba79
- 0bec69c1b22603e9a385495fbe94700ac36b28e5
- 17bd8fda268cbb009508c014b7c0ff9d8284f850
- 5ed22c0033aed380aa154e672e8db3a2d4c195c4
- 78cd4dfb251b21b53592322570cc32c6678aa468
- c2387833f4d2fbb1b54c8f8ec8b5b34fle8e2d91
- cb25a5125fb353496b59b910263209f273f3552d

SHA-256

- acadf15ec363fe3cc373091cbe879e64f935139363a8e8df18fd9e59317cc918
- 3ea2d190879c8933363b222c686009b81ba8af9eb6ae3696d2f420e187467f08
- 4188736108d2b73b57f63c0b327fb5119f82e94ff2d6cd51e9ad92093023ec93
- 443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58
- 4f94155e5a1a30f7b05280dd5d62c3410bcc52aea03271d086afa5dc5d97e585
- 0440ef40c46fdd2b5d86e7feef8577a8591de862cfd7928cdbcc8f47b8fa3ffc
- 9b1b15a3aacb0e786a608726c3abfc94968915cedcbd239ddf903c4a54bfcf0c
- c8f9elad7b8cce62fba349a00bc168c849d42cfb2ca5b2c6cc4b51d054e0c497
- 5f6fec8f7890d032461b127332759c88a1b7360aa10c6bd38482572f59d2ba8b
- 6839fcae985774427c65fe38e773aa96ec451a412caa5354ad9e2b9b54ffe6c1
- 7f4555a940ce1156c9bcea9a2a0b801f9a5e44ec9400b61b14a7b1a6404ffdf6
- d7c81b0f3c14844f6424e8bdd31a128e773cb96cccef6d05cbff473f0ccb9f9c
- 8e035beb02a411f8a9e92d4cf184ad34f52bbd0a81a50c222cdd4706e4e45104
- 648c2067ef3d59eb94b54c43e798707b030e0383b3651bcc6840dae41808d3a9
- 0d10c4b2f56364b475b60bd2933273c8bled2176353e59e65f96 8c61e93b7d99
- 274340f7185a0cc047d82ecfb2cce5bd18764ee558b5227894565c2f9fe9f6ab
- 42b22faa489b5de936db33f12184f6233198bdf851a18264d31210207827ba25
- 982dda5eec52dd54ff6b0b04fd9ba8f4c566534b78f6a46dada624af0316044e
- b6e82a4e6d8b715588bf4252f896e40b766ef981d941d0968f29a3a444f68fef
- e23283e75ed2bdabf6c703236f5518b4ca37d32f78d3d65b073496c12c643cfe

MD5

- 1e5ad5c2ffffac9d3ab7d179566a7844
- 56fd7145224989b92494a32e8fc6f6b6
- 6639433341fd787762826b2f5a9cb202
- 828699b4133acb69d34216dcd0a8376e

| Appendix C: 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 D: 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%