Lookout

Mobile Threat of the Month

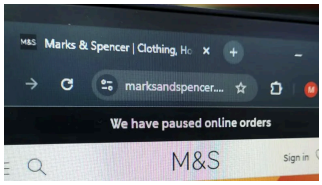
May 2025

Marks & Spencer Breach Linked to Scattered Spider Ransomware Attack

Multinational retailer Marks & Spencer (M&S) confirmed it suffered a cyberattack, causing widespread disruption.

Who was behind the attack?

It is widely reported that the notorious hacking group Scattered Spider is believed to be behind the attack. Known for their aggressive and highly sophisticated social engineering tactics, the group specialises in phishing, credential theft, and SIM-swapping attacks to infiltrate networks. Once inside, they systematically escalate access, ultimately extorting organisations into paying substantial ransoms. Social engineering, the psychological manipulation of people into divulging sensitive information or performing unsafe actions, is one of the fastest-growing cyber threats facing businesses today.



In September 2023, Scattered Spider breached MGM Resorts through a mobile-oriented social engineering attack, impersonating an employee calling the company's IT helpdesk. Recent attacks on large UK retailers, Co-Op and Harrods, have also demonstrated similar traits to the M&S attack.

How did the breach occur?

Scattered Spider is believed to have initially breached M&S by compromising an Active Directory Services database file containing password hashes for the company's Windows accounts. Armed with these credentials, the threat actors moved laterally across the Windows domain, exfiltrating data from network devices and servers. The attackers then deployed DragonForce ransomware, significantly increasing their leverage for extortion by encrypting critical systems and demanding payment to restore access.

The attack caused widespread disruption to M&S operations, including failures in its contactless payment system, delays in click & collect orders, and the temporary suspension of online customer orders. Employees were instructed to work remotely as the company worked to contain the incident. To mitigate further risk, M&S took several systems offline, safeguarding partners, suppliers, and broader business operations.

Lookout Mobile Security

Mobile social engineering attacks have become more proficient in leveraging SMS and messaging apps against employees to impersonate IT and support staff. iOS and Android devices are relied upon as the second form of authentication for MFA solutions, despite mobile users being more susceptible to social engineering. Threat actors that carry out these targeted attacks will conduct research, first identifying employees in positions that will typically have access to more sensitive information.

Lookout's AI-driven mobile threat defence helps customers to mitigate the risk of social engineering and credential theft by automatically detecting and blocking mobile phishing attempts and executive impersonation messages that intend to steal employee credentials.