# Tyler Buchanan extradited over links to cyberattack that paralysed M&S online sales



Last week, British retailer Marks & Spencer (M&S) faced significant challenges due to a cyberattack that severely disrupted its IT systems. While the investigation into the hack is ongoing, Tyler Buchanan, a 23-year-old from Dundee, was extradited to the United States, where he awaits trial on multiple charges linked to his alleged role as an ringleader in a cybercriminal group known as Scattered Spider.

Scattered Spider is believed to be behind the recent cyber onslaught that led M&S to suspend online sales for over a week, causing substantial losses and erasing hundreds of millions from its market value. The company's response has been carefully guarded, with little information disclosed about the nature of the attack or any ransom demands made.

DragonForce, another group operating in the cybercriminal landscape, claimed responsibility for the attacks affecting M&S as well as Co-op and Harrods, although experts are cautious not to exclude Scattered Spider's involvement. Analysts have suggested that DragonForce and Scattered Spider may be collaborating to exploit retailers like M&S, utilising ransomware tactics to extort funds.

Buchanan, who had spent ten months awaiting extradition after his arrest in Spain last summer, is the only British citizen among six people implicated in the activities of Scattered Spider. During his arrest, authorities seized a cryptocurrency wallet containing over $26 million (£20 million) in Bitcoin. His modest appearance—a stark contrast to typical depictions of cybercriminals—showed him donning low-slung jeans and a T-shirt.

Buchanan was denied bail during his court appearance in California last Thursday, classified as a flight risk. While it remains unclear whether he played a direct role in executing the M&S attack, his indictment alongside several younger American men paints a picture of a network where youth predominates. Phishing and SIM swapping are cited as primary methods used by the group to access sensitive information and facilitate financial theft.

Family and friends have expressed disbelief about Buchanan's alleged involvement, with his father stating that his son had a long-standing interest in computers since childhood. However, authorities argue that Buchanan's online activities—characterised by a clear digital footprint—suggest a lack of sophistication in his cyber operations.

The criminal enterprise of Scattered Spider extends beyond M&S, having targeted numerous businesses across the globe— including operations in the US, Canada, and India. The group's tactics range from phishing and SIM swapping to deploying ransomware that encrypts systems to demand payment for unlocking.

Similar high-profile attacks have drawn significant attention to Scattered Spider, including the cyber-related interruptions experienced by gaming giant MGM Resorts International, which faced estimated losses of around $100 million following an infiltration of its management system. Such incidents have highlighted the growing threat posed by this faction, described by Microsoft as "one of the most dangerous financial criminal groups" currently active.

In the broader landscape of cyber threats, Buchanan is also associated with a darker community known as "The Com," which has raised alarms among law enforcement about corrupting young individuals into committing serious crimes through online manipulation.

Buchanan's legal counsel has emphasised that he is entitled to the presumption of innocence, with his lawyer asserting there is no direct link between him and the M&S hack. Meanwhile, as M&S cooperates with cybersecurity experts from various agencies, including the National Cyber Security Centre, retail leaders are urged to bolster their digital security measures in light of the ongoing risk posed by organised cybercrime.

As the legal proceedings surrounding Tyler Buchanan unfold, the impact of cyberattacks on national retailers continues to resonate, prompting discussions on the vulnerabilities of businesses in today's digital age.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.thehackernews.com/2024/06/uk-hacker-linked-to-notorious-scattered.html> - This article reports on the arrest of Tyler Buchanan, a 22-year-old from Dundee, Scotland, who is believed to be a key member of the Scattered Spider cybercrime group. He was arrested in Spain in June 2024 during an investigation by the U.S. Federal Bureau of Investigation (FBI).
* <https://siliconangle.com/2024/06/16/suspected-key-member-scattered-spider-cybercrime-group-arrested-spain/> - This source details the arrest of Tyler Buchanan in Spain, highlighting his alleged role as the ringleader of the Scattered Spider group, which has targeted numerous companies and individuals in the U.S. The article also mentions the seizure of $27 million in Bitcoin during his arrest.
* <https://www.metacurity.com/ringleader-scattered-spider-allegedly-arrested-spain/> - This article discusses the arrest of Tyler Buchanan, identified as a SIM swapper operating under the alias 'Tyler.' It provides insights into the operations of the Scattered Spider group and their methods, including social engineering and SIM-swapping techniques.
* <https://www.itpro.com/security/cyber-crime/alleged-scattered-spider-ringleader-taken-down-in-spain-after-law-enforcement-crackdown> - This source reports on the arrest of a 22-year-old believed to be a prominent figure behind the Scattered Spider hacking group. It mentions the group's involvement in high-profile breaches, including attacks on MGM Resorts and other organizations.
* <https://www.computerweekly.com/news/366616372/Brit-charged-in-US-over-Scattered-Spider-cyber-attacks> - This article details the charges brought against Tyler Buchanan by the U.S. Department of Justice over his alleged involvement in the Scattered Spider cyber attacks. It discusses the group's use of social engineering techniques to gain access to corporate accounts and steal sensitive information.
* <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a> - This advisory from the Cybersecurity and Infrastructure Security Agency (CISA) provides information on the Scattered Spider threat actor group, including their tactics, techniques, and procedures (TTPs). It highlights the group's use of social engineering and ransomware in their cyberattacks.
* <https://www.dailymail.co.uk/news/article-14672725/The-shocking-truth-baby-faced-British-ringleader-shadowy-international-criminal-network-Scattered-Spider-experts-believe-devastating-M-S-hack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data