# Young hacker Tyler Buchanan leads Scattered Spider in billion-pound cyberattack on UK retailers



A recently identified hacking gang, Scattered Spider, is drawing alarm as experts warn of the risks posed by cybercriminal groups led by relatively young individuals. Central to these concerns is Tyler Buchanan, a 23-year-old from Dundee, Scotland, who emerges as a key figure within this organisation, accused of orchestrating crippling cyber attacks on major retail companies, including Marks & Spencer.

Buchanan's alleged activities are not only notable due to their sheer scale—an estimated £20 million bitcoin scam—but also because of the sophisticated techniques employed by Scattered Spider. The group has been linked to significant disruptions across multiple sectors. Reports indicate that a recent attack on Marks & Spencer resulted in the loss of sensitive customer data and a staggering £1 billion reduction in the retailer's market value. Chief executive Stuart Machin noted, however, that the leak did not include usable payment details, prompting the company to request customers reset their passwords as a precautionary measure.

The group's modus operandi typically hinges on social engineering tactics, which involve manipulating individuals into divulging critical login credentials. This method has proven effective; it has enabled the gang to launch coordinated attacks that have reportedly affected not only Marks & Spencer but also major players such as the Co-op and Harrods. The UK National Cyber Security Centre has highlighted the inherent vulnerabilities in the retail sector, where outdated systems and extensive customer databases make them prime targets for such cyber incursions.

Buchanan's background reveals a troubling narrative. Following a raid in February 2023, where a gang showed up at his mother’s home demanding access to his cryptocurrency accounts, Buchanan went into hiding, reportedly fleeing Scotland. Law enforcement officials seized numerous devices believed to be linked to his activities with Scattered Spider, and U.S. court documents indicate his involvement in wire fraud and identity theft, where victims were compelled to provide access under false pretences of account safety.

While Buchanan's father has distanced himself from the allegations, describing his son as a mere "computer whizz," experts like Graeme Pearson, a former head of the Scottish Crime and Drug Enforcement Agency, caution that the rise of such younger hackers represents a new breed of cybercriminals. Pearson stated, “They are rarely violent people but motivated by the sheer challenge,” which in turn places them on the radar of organised crime networks seeking to exploit their skills for profitable ventures.

Professor Bill Buchanan, an established authority on applied cryptography, echoes this sentiment, underscoring the existential threat that hacking groups pose to essential infrastructure across Scotland. He warned that large-scale ransomware attacks targeting critical services such as healthcare and education are a real possibility. "Many organisations still do not encrypt their personally sensitive information," he noted, highlighting a significant gap in protective measures that could facilitate further breaches.

The far-reaching implications of Scattered Spider’s activities cannot be understated. The group, which comprises a loose network of around 1,000 teenagers and young adults, has been implicated in crimes that span both sides of the Atlantic. Reports suggest they have adopted an increasingly sophisticated approach, often collaborating with notorious entities such as the ALPHV/BlackCat ransomware operation. As they leverage phishing, multi-factor authentication fatigue, and SIM swapping, their capability to inflict damage on both private and public sectors continues to grow.

In light of these threats, experts advocate for enhanced cybersecurity measures and a collective industry response. This includes not only implementing robust encryption practices but also fostering partnerships between business sectors and academic institutions to develop more effective strategies against the relentless tide of cybercrime.

As the battle against cyber threats evolves, the question remains as to whether the existing frameworks can adequately respond to and thwart the activities of groups like Scattered Spider, before they cause irreparable harm to trust in systems that underpin our economy.

### Reference Map

* Paragraph 1: [[1]](https://www.dailyrecord.co.uk/news/scottish-news/dangerous-hacking-gang-led-young-35219101)
* Paragraph 2: [[2]](https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9)
* Paragraph 3: [[1]](https://www.dailyrecord.co.uk/news/scottish-news/dangerous-hacking-gang-led-young-35219101)
* Paragraph 4: [[1]](https://www.dailyrecord.co.uk/news/scottish-news/dangerous-hacking-gang-led-young-35219101)
* Paragraph 5: [[1]](https://www.dailyrecord.co.uk/news/scottish-news/dangerous-hacking-gang-led-young-35219101)
* Paragraph 6: [[1]](https://www.dailyrecord.co.uk/news/scottish-news/dangerous-hacking-gang-led-young-35219101)
* Paragraph 7: [[3]](https://www.bleepingcomputer.com/news/security/fbi-shares-tactics-of-notorious-scattered-spider-hacker-collective/)
* Paragraph 8: [[1]](https://www.dailyrecord.co.uk/news/scottish-news/dangerous-hacking-gang-led-young-35219101)
* Paragraph 9: [[4]](https://www.lemonde.fr/pixels/article/2024/11/21/cinq-membres-du-groupe-de-pirates-scattered-spider-arretes_6407020_4408996.html)
* Paragraph 10: [[6]](https://www.axios.com/2024/11/20/scattered-spider-us-arrests)
* Paragraph 11: [[3]](https://www.bleepingcomputer.com/news/security/fbi-shares-tactics-of-notorious-scattered-spider-hacker-collective/)

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

## Bibliography

1. <https://www.dailyrecord.co.uk/news/scottish-news/dangerous-hacking-gang-led-young-35219101> - Please view link - unable to able to access data
2. <https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9> - This article discusses recent cyber attacks on major UK retailers, including Marks and Spencer (M&S), the Co-op, and Harrods, attributed to the Scattered Spider hacking group. The attacks have led to significant operational disruptions and financial losses, with M&S experiencing a £600 million drop in value. Experts suggest a coordinated effort by Scattered Spider, known for manipulating individuals to gain system access. The National Cyber Security Centre has urged businesses to take cybersecurity seriously, highlighting the vulnerability of retailers due to their vast customer data and reliance on legacy systems.
3. <https://www.bleepingcomputer.com/news/security/fbi-shares-tactics-of-notorious-scattered-spider-hacker-collective/> - The FBI and CISA released an advisory about Scattered Spider, a loosely knit hacking collective collaborating with the ALPHV/BlackCat Russian ransomware operation. The group employs social engineering tactics like phishing, MFA fatigue, and SIM swapping to gain initial network access. Members, some as young as 16, are part of a decentralized network, making tracking difficult. The advisory recommends mitigations such as application controls, monitoring remote access tools, securing RDP usage, maintaining offline backups, and implementing network segmentation to protect against Scattered Spider attacks.
4. <https://www.lemonde.fr/pixels/article/2024/11/21/cinq-membres-du-groupe-de-pirates-scattered-spider-arretes_6407020_4408996.html> - Five men in their twenties were charged by U.S. authorities on November 20, suspected of being part of the Scattered Spider hacking group. They are accused of bank fraud and identity theft. The group is linked to notable attacks, including the hacking of MGM Resorts casinos in the U.S., costing approximately $100 million. The suspects, aged 20 to 25, were arrested at various times and locations, including a Briton in Spain. Scattered Spider uses phishing and SIM swapping techniques to access company networks and steal funds, primarily in cryptocurrency, totaling over $11 million.
5. <https://www.thehackernews.com/2024/06/uk-hacker-linked-to-notorious-scattered.html> - A 22-year-old man from the UK was arrested in Spain for his alleged involvement with the notorious cybercrime group Scattered Spider. The individual, known as 'Tyler' and believed to be Tyler Buchanan, is associated with several high-profile ransomware attacks performed by Scattered Spider. The arrest is part of a joint effort between the U.S. Federal Bureau of Investigation (FBI) and the Spanish National Police, initiated in May. Scattered Spider is known for orchestrating sophisticated social engineering attacks to gain initial access to organizations.
6. <https://www.axios.com/2024/11/20/scattered-spider-us-arrests> - The U.S. Justice Department has charged five men—Ahmed Hossam Eldin Elbadawy, Noah Michael Urban, Evans Onyeaka Osiebo, and Joel Martin Evans—who are allegedly part of the Scattered Spider hacker group. This group is accused of targeting multiple U.S. corporations, stealing millions of dollars in cryptocurrency, and deceiving employees with phishing texts. The charges include aggravated identity theft, conspiracy to commit wire fraud, and conspiracy to commit a crime. Scattered Spider has been linked to high-profile attacks on MGM Resorts and Caesars Entertainment, among others, with estimates suggesting the group has targeted around 100 organizations in total. If convicted, each defendant could face up to 20 years in federal prison for the wire fraud charges alone.
7. <https://www.cbsnews.com/news/scattered-spider-blackcat-hackers-ransomware-team-up-60-minutes/> - Scattered Spider and BlackCat both claimed credit for the September 2023 ransomware attack on MGM Resorts, which cost the hotel and casino giant more than $100 million. It disrupted operations at a dozen of the most renowned hotels and casinos on the Las Vegas Strip: including MGM Grand, Aria, Mandalay Bay, New York-New York and the Bellagio. Anthony Curtis, who publishes the 'Las Vegas Advisor,' was in an MGM property during the ransomware attack. He says people were left dumbfounded as thousands of slot machines suddenly stopped functioning properly. 'So all of a sudden now people are going 'How do I get my money? What's wrong?' And the people were sitting there waiting and couldn't get paid,' Curtis said. As a result of the cyberattack, elevators were malfunctioning, parking gates froze, and digital door keys wouldn't work. As computers went down, reservations locked up and lines backed up at the front desks. 'Anything that required technology was not working,' Curtis said.