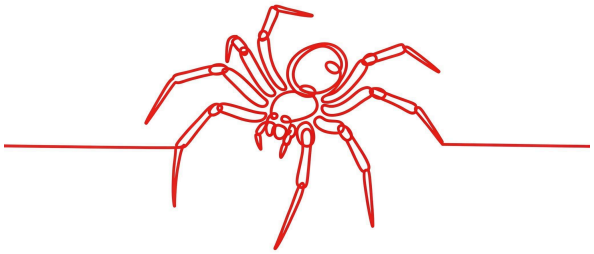
MONDAS
MINDING YOUR BUSINESS

Threat Intelligence Update: Scattered Spider



Mondas has issued this advisory due to the suspected involvement of the financially motivated threat group Scattered Spider (also known as 0ktapus, Scatter Swine, UNC3944, and Octo Tempest) in recent significant incidents across the UK retail, aviation and other high-risk sectors and organisations.

Active since May 2022, Scattered Spider has targeted major organisations like Microsoft and T-Mobile, engaging in data theft, extortion, ransomware deployment, and cryptocurrency theft.

The group has been linked to ransomware operations through affiliates such as RansomHub, Qilin, and most recently, DragonForce. Despite arrests in the US, UK, and Spain, Scattered Spider remains active and is believed to be shifting its extortion platform towards DragonForce, as RansomHub's infrastructure was previously used.

Threat Actor Tactics

Scattered Spider commonly uses social engineering, such as impersonating employees or IT staff, to deceive help desk personnel into resetting credentials or bypassing multi-factor authentication (MFA). These efforts are often supported by SIM swapping, MFA fatigue, and adversary-in-the-middle (AiTM) techniques. The group has also utilised the 0ktapus Phishing-as-a-Service kit and acquired stolen credentials to gain access.

Upon gaining initial access, Scattered Spider moves quickly from identity providers to internal systems, often within an hour. Their focus includes compromising privileged accounts, disabling security controls, and employing tools like Mimikatz, TruffleHog, and Ngrok for lateral movement and persistence.

They utilise living-off-the-land techniques and remote monitoring and management (RMM) tools to avoid detection. Infostealers such as Raccoon and VIDAR are used for data theft, either encrypted or exfiltrated (or both), followed by extortion.

Threat Landscape

Scattered Spider's targeting scope has expanded significantly from initial small campaigns against individuals to SIM swap operations targeting mobile and outsourced telecom providers for cryptocurrency theft from high-value targets. It's reported that Scattered Spider is targeting organisations across various sectors, including:

- Technology
- Financial services
- Hospitality
- Telecommunications
- Consumer goods
- Aviation
- Manufacturing
- Professional services
- Retail
- Individuals
- Media and entertainment

Speculation exists regarding their involvement in security issues that affected the Co-operative and M&S the financial impact of which was estimated to be £440m. They are believed to be linked to recent attacks on Qantas who experienced a breach on their third-party customer data platform used to store the personal data of six million people.

Mitigations

Scattered Spider continues to target high-profile organisations through sophisticated social engineering, exploitation of identity infrastructure, and rapid lateral movement.

The following mitigations are recommended to reduce risk:

- Help Desk Procedures: Review and enhance help desk procedures to prevent unauthorised credential resets. Implement stringent identity verification for all support interactions. Provide comprehensive training to support teams and administrative users to recognise and challenge social engineering attempts.

- Login Activity Monitoring: Mondas has implemented alarms for behavioural analytics and alerts to detect unusual login activity and high-risk access patterns.

- Multi-Factor Authentication (MFA): Mandate phishing-resistant MFA wherever possible and minimise reliance on SMS-based authentication methods.

- Access Controls: Restrict access between systems and enforce the principle of least privilege to limit lateral movement. Implement stricter administrative access controls, including using just-in-time access where feasible.

- Backups & Recovery: Validate your secure, immutable backups and test recovery processes

Response Recommendations

Increased vigilance from the SOC	Proactive threat hunting efforts	Monitor evolving threats
Intensify monitoring efforts to ensure swift identification and response to emerging threats such as Scattered Spider ransomware.	Take a proactive stance by actively searching for hidden risks and indications of attack and compromise within your systems.	Strive to keep informed on the latest threats and action mitigation efforts to reduce the risk of exposure and damage to business continuity.

Ready to start minding your business?

Contact me to discuss how Mondas can help to keep your business secure.

01252 494 020

george@mondas.co.uk

mondas.co.uk