Marsh

UK retailers: Protecting against cyber threats

A business of Marsh McLennan

What do we know?

Multiple retailers hit by separate cyber incidents in the last week in a highly targeted, sophisticated campaign

Who is behind the attacks?

- Initial intel suggests that the same threat group may be behind the attacks – Scattered Spider.
- They are a criminal collective that originated in 2022.
- They gained notoriety after attacks on Caesars Casino & MGM Casino in the US in 2023.
- They are notable for having UK & US based operatives and for launching sophisticated campaigns against multiple targets within the same industry.

What are their tactics?

- Use of UK operatives makes them particularly effective at persuading IT helpdesks into resetting passwords and MFA devices using data obtained from LinkedIn and/or public websites.
- They have also been known to spam employees' inboxes and then pretending to be the IT helpdesk, persuading employees to divulge credentials.
- They are known to target specific organisations, gain access and dwell in systems for significant amounts of time before stealing data and then deploying ransomware.

What should you do if you suspect a compromise?

Activate your incident response and/or crisis management plans, and stand up your incident response team.

Shift to out of band communication platforms, such as CYGNVS.

Call the CYGNVS hotline to create your secure incident room and invite relevant internal and external stakeholders to join.

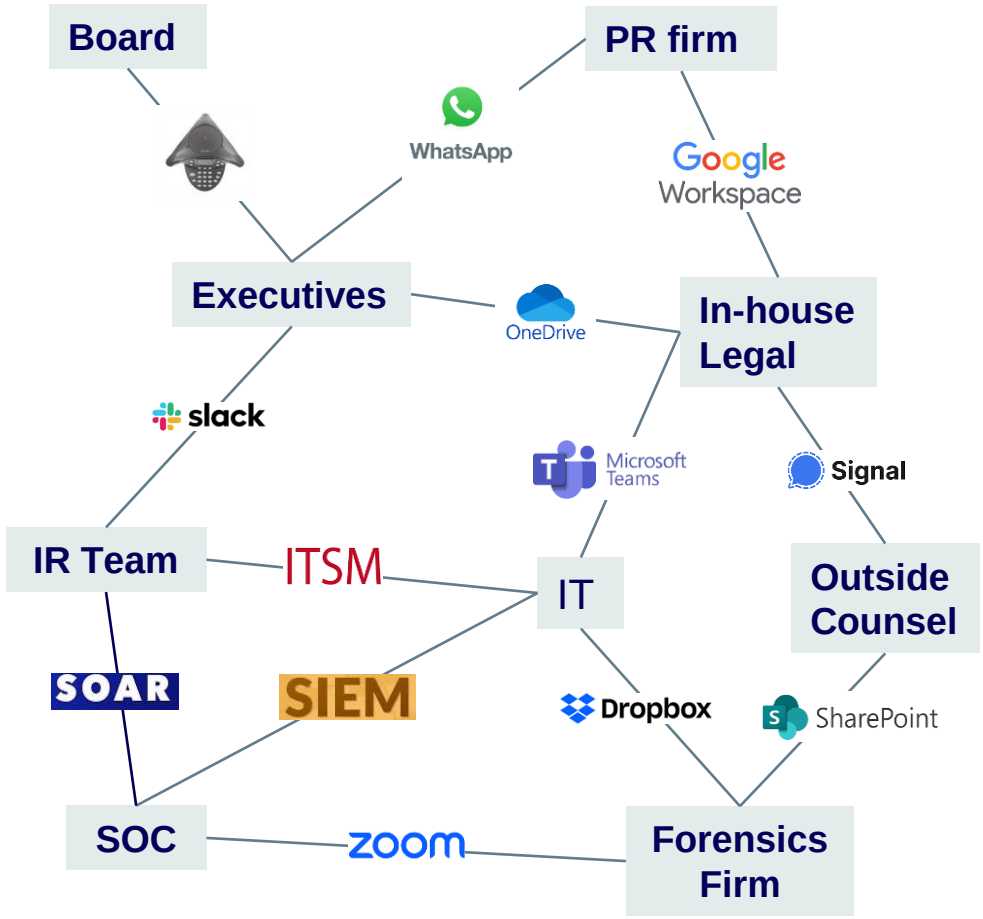
Notify Marsh Cyber Incident Management team via our dedicated 24/7 CYGNVS hotline.

Notify cyber insurers promptly.

Seek expert support and do not engage with the threat actor.

CYGNVS

Take the chaos out of Incident Response



Calling to Arms

Mobilise remote business teams rapidly when existing systems may be compromised

Conducting a Symphony

Manage activity and access across diverse internal Business Teams and External Providers

Ticking Clock

Ensure required steps are performed by deadlines and critical documents are at your fingertips – it's a plan in your pocket.

Proving Compliance

Document chain of custody of data with audit trail for reporting to regulators and customers

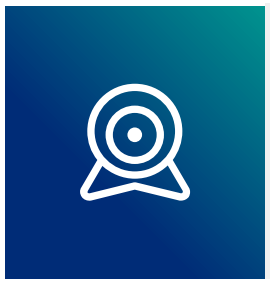
What steps can you take to protect your organisation now?

Check your logs and investigate any recent false positives. Harden environment against the published IOC’s and TTP’s of scattered spider

Alert your IT service desk to investigate suspicious passwords and/or MFA resets over the last few months.

Review your MFA policy and remove the ability for individuals to authenticate with a phone number.

Refresh employee training on phishing, social engineering and deepfake threats. Emphasise the importance of verifying requests for sensitive information.



Establish verification protocols for requests for information and resetting credentials, requiring secondary confirmation via a different communication channel

Train helpdesk staff to recognise signs of social engineering attempts and implement strict verification processes for sensitive requests.

Claims and Incident Management

How you respond makes all the difference

Prepare

Creating and testing IR plans reduces losses by $1.49 M on average – *IBM Cost of a Data Breach Report 2023*

- CIM onboarding*
- Review and Develop Incident response plans
- Incident response vendor selection

Test

Well-practiced teams know their roles, responding quickly and effectively.

- Tabletop Exercises & Crisis Simulations

Respond

A coordinated, holistic effort is vital for effective incident response.

- Active Incident Response (AIR) support*
- Secure incident response platform (Marsh CIM Tool)*
  powered by CYGNVS

Recover

Expert support ensures proactive navigation of cyber claims complexity, maximizing insurance claims recovery

- Forensics Accounting
- Claims Advocacy*

Enhance

Convert learnings and challenges into opportunities for growth

- Resilience Roadmap Development
- Enhanced Claims Feedback*

*UK Core Services

Marsh