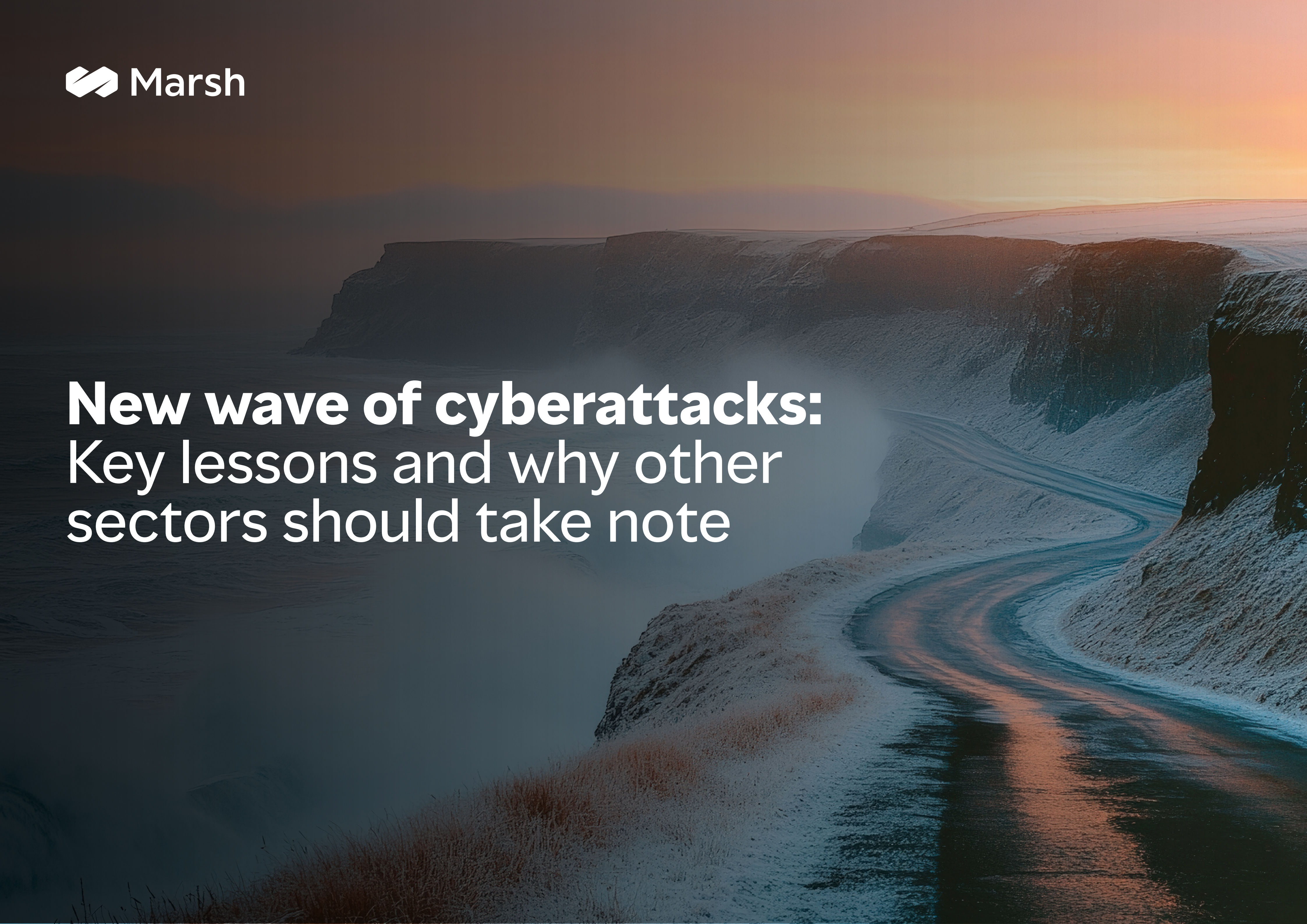
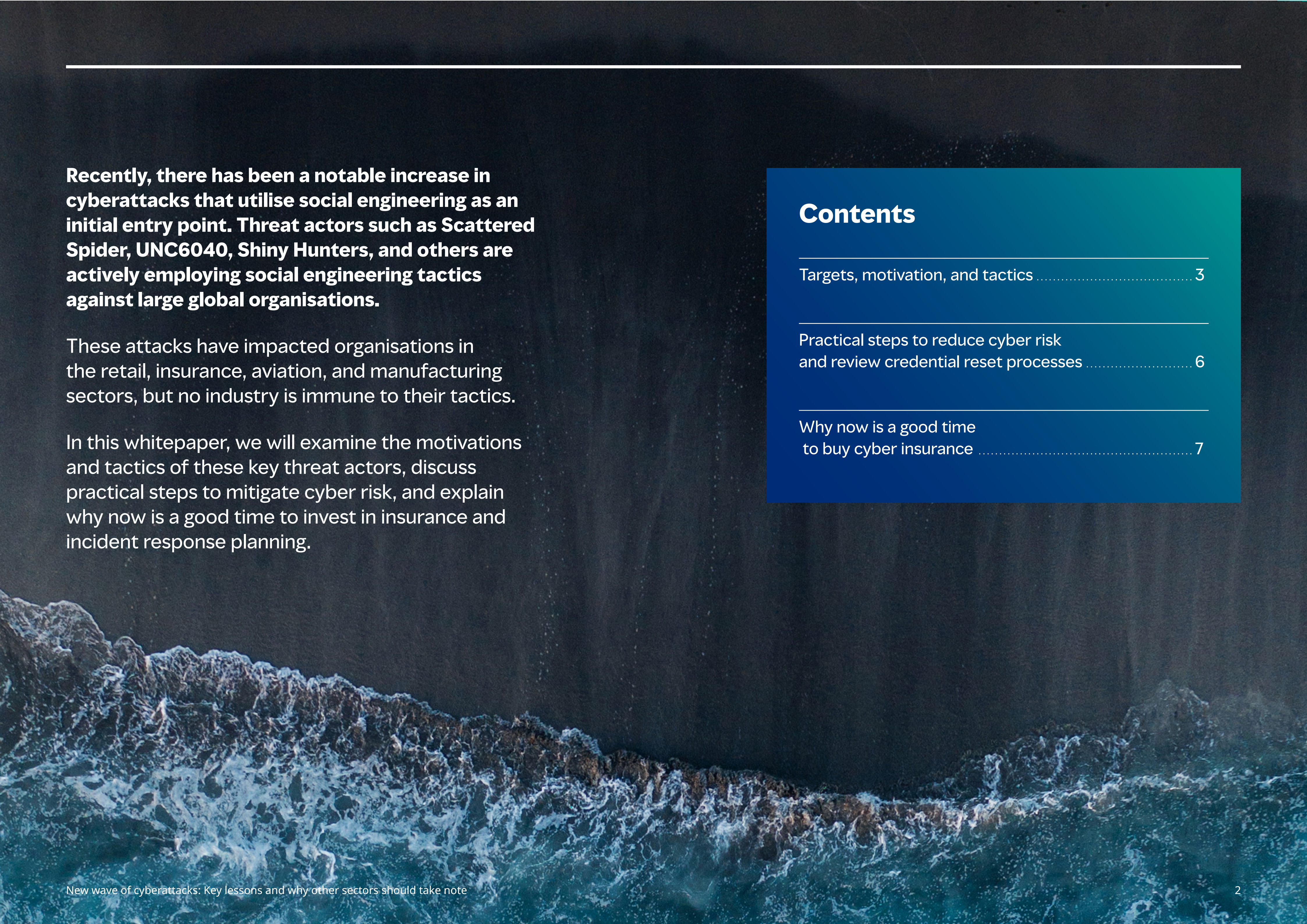
Marsh

New wave of cyberattacks: Key lessons and why other sectors should take note





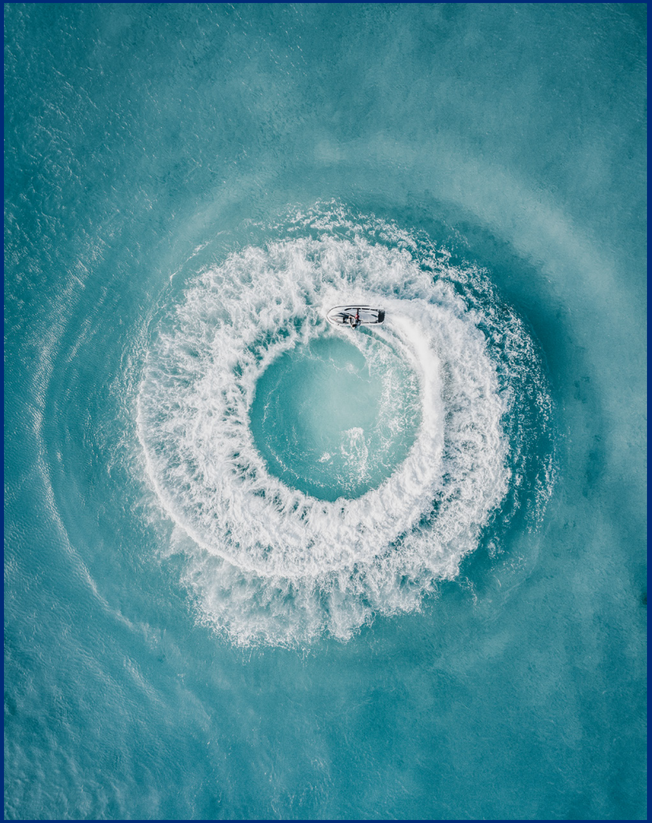
Recently, there has been a notable increase in cyberattacks that utilise social engineering as an initial entry point. Threat actors such as Scattered Spider, UNC6040, Shiny Hunters, and others are actively employing social engineering tactics against large global organisations.

These attacks have impacted organisations in the retail, insurance, aviation, and manufacturing sectors, but no industry is immune to their tactics.

In this whitepaper, we will examine the motivations and tactics of these key threat actors, discuss practical steps to mitigate cyber risk, and explain why now is a good time to invest in insurance and incident response planning.

Contents

Targets, motivation, and tactics



Originating in 2022, Scattered Spider is linked to a series of high-profile cyber incidents, primarily focusing on social engineering and credential theft.

The name “Scattered Spider” was coined by security researchers to describe a loose affiliation of primarily native English-speaking cybercriminals — some as young as 16 — who have emerged from an cybercrime collective known as “The Community” or “The Com”. Scattered Spider has gained notoriety since 2023 as “big game hunters”. The outfit has been particularly successful in using native English speakers to call organisations’ IT help desks, impersonating legitimate employees and persuading agents to reset passwords and/or multifactor authentication (MFA) for the relevant account.

Also linked to The Com is a group known as UNC6040, which has recently launched a highly successful voice phishing (vishing) campaign against IT support personnel in order to obtain user credentials and steal data environments. The Federal Bureau of Investigation has warned the public about the dangers of answering smartphone calls and messages from specific threat groups and campaigns.

In a public cybersecurity advisory, I-051525-PSA, the FBI has reported an ongoing threat campaign since April 2025 that employs malicious text and voice messages impersonating senior US officials, including individuals in federal and state government positions, to gain access to personal information and ultimately valuable online accounts.

Targets and motivation

Initially focused on cryptocurrency theft, Scattered Spider and other groups have pivoted to ransomware, as law enforcement scrutiny increased and blockchain tracing technologies improved. Unlike most ransomware threat actors who target victims opportunistically, Scattered Spider, for example, focuses on a small set of high-profile targets within specific industries. While it remains unclear if this strategy has been financially successful, it has proven effective in generating publicity and enhancing the group’s reputation as persistent hackers. Their motivations appear to be a mix of desire for financial gain, “bragging rights,” and causing chaos.

Tactics

The behaviours of Scattered Spider and other groups include:

- **Social engineering prowess:** Threat actors employ sophisticated social engineering campaigns, often targeting IT helpdesks. They are experts in “hacking the human”. By using social manipulation techniques that evade traditional filters, adopting local accents, and leveraging publicly available information about key employees, they can convince helpdesk staff to reset accounts quickly. They may also purchase access from initial access brokers on the dark web.

- **Exploitation of legacy VPN and remote desktop protocol (RDP) vulnerabilities:** Once inside a network, the threat actors leverage unpatched legacy virtual private network (VPN) gateways and vulnerable remote desktop protocol (RDP) endpoints to maintain persistence and escalate privileges within retailer networks. They exploit single sign-on (SSO) services and have previously used infrastructure from major mobile carriers and internet providers to conduct attacks, complicating containment efforts for defenders.

- **Endpoint detection and response (EDR) monitoring tools fail to detect attacks on the hypervisor:** Scattered Spider, in particular, also uses virtualisation management systems, also known as hypervisor hosts (which manage virtual machines on host systems), to conduct attacks. These systems are attractive to attackers because they cannot be protected by common security tools like endpoint detection and response (EDR) technology that responds to threats on devices such as computers, servers, and mobile devices. After compromising a hypervisor, Scattered Spider can create new virtual machines, disguising them as legitimate to maintain persistence and stage further exploitation.

> “Hypervisor hosts appeal to all attackers — not just Scattered Spider — because they control multiple devices within a network, enable users to create new virtual machines, and cannot be protected by common security tools like EDR.”
>
> **James Tytler, Senior Associate, Cyber Incident Response, S-RM**

- **Manual ransomware deployment:** Unlike automated ransomware attacks, Scattered Spider and other threat group operators typically deploy ransomware payloads manually, only after carefully mapping out network assets. This ensures maximum disruption and increased leverage for ransom demands.

- **Data exfiltration prior to encryption:** Before encrypting systems, threat actors exfiltrate sensitive customer data and corporate information. This “double extortion” tactic adds pressure on victims to pay ransoms to prevent public data leaks and further harm to their brand reputation.

- **Targeting the supply chain:** In recent retail attacks, it is possible that Scattered Spider exploited the weaker security postures of third-party vendors connected to retailers, thereby gaining indirect network access. This approach allows stealthy lateral movement without immediate detection.

- **Denial-of-service (DDoS) attacks as a diversion:** In some cases, Scattered Spider and other threat groups launch distributed denial-of-service (DDoS) attacks against retailer websites concurrent with ransomware deployment, overwhelming IT teams and complicating response efforts.

- **Use of media as a pressure tactic:** In the recent retail attacks, Scattered Spider used the media to apply pressure on organisations. Instead of naming companies on the dark web, threat actors have been drip-feeding journalists with information, which is how much of the news about these attacks has been disseminated.

Practical steps to reduce cyber risk and review credential reset processes

1. **Ensure you have visibility across all your devices:** Continuous monitoring and threat hunting are essential. Proactive monitoring using behavioural analytics can detect abnormal activity early, such as unusual data transfers or privilege escalations linked to attackers' reconnaissance phases.

2. **Bolster cybersecurity basics:** To enhance your security posture against threats like social engineering, it's crucial to understand what exists on your network edge, as most network intrusions result from easily exploitable vulnerabilities. Having a human in the loop to monitor and respond to alerts is essential to ensure that potential threats are addressed promptly and effectively.

3. **Prioritise employee awareness and training:** Regular, targeted training, alongside AI-powered email security platforms, is critical for identifying and blocking highly convincing phishing attempts. Additionally, ensure your VPN has multi-factor authentication, regularly scan for software vulnerabilities, and actively look for exposed credentials. Also, ensure your IT and customer help desks are trained to detect social engineering attempts.

4. **Test your incident response plan by conducting a tabletop exercise:** Develop a comprehensive incident response plan that outlines roles and responsibilities for cyberattack scenarios. Conduct regular tabletop exercises to review and practice responses to hypothetical cyber incidents. This will help your team develop muscle memory for incident response, enabling them to make quick and effective decisions.

> "It's all very well and good having the best incident response plan in the world. But if it lives in a drawer and never comes out, it's not worth the paper it's written on."
>
> **Helen Nuttall, Head of Cyber Incident Management, Marsh**

5. **Sign up for Marsh Central or another out-of-band communication platform :** Threat actors, such as Scattered Spider, are known for compromising Teams and other communication platforms to obtain information about the company, employees, and incident response strategies. Ensure you have an off-network platform, such as Marsh Central, at the ready.

6. **Make lateral movement difficult:** In the event of a breach, make lateral movement within the network as difficult as possible by implementing network segmentation to protect your most critical assets — your "crown jewels" — which typically include virtualisation environments. Immediate patching and upgrading of VPN and RDP services, combined with enforcing multi-factor authentication (MFA), is vital to prevent easy lateral movement.

7. **Implement zero trust network architecture:** Restrict internal network access to only what is strictly necessary, with continuous verification, to minimise damage from compromised accounts. While security will always involve a trade-off between user accessibility and protection, there are likely few instances where a user forgets both their password and loses access to their mobile device. Organisations should review their playbooks, considering whether it should be possible to reset both factors in a single session. If an employee has lost both their mobile device and password, it may be appropriate to require them to come into the office to reset their password.

8. **Conduct regular backup testing and segmentation:** Frequent, secure, and tested backups — isolated from the main network — can facilitate recovery without paying ransoms.

9. **Carry out supply chain security due diligence:** Regular cybersecurity assessments of third-party vendors and tightening network segmentation between retailer systems and external partners can reduce indirect attack surfaces.

Why now is a good time to buy cyber insurance

Insurance rates for cyber insurance have decreased across the board despite ongoing losses, especially in the UK, where competition between insurers is intense. In the first quarter of 2025, prices dropped 7% on primary layers, with more significant price drops becoming evident.

> “We are absolutely in a buyer-friendly environment. Clients have come to us midterm, saying the board wants more cyber insurance.”
>
> **Serena France-Hayhurst, UK Cyber Placement Leader, Cyber Risk at Marsh**

Many organisations have pursued higher limits this year, with 16% of Marsh clients extending their limit in the first quarter of 2025. The UK retail cyberattacks have sparked conversations with insureds, including those who recently renewed their programmes, as board members increasingly direct risk managers to acquire more cyber insurance.

From a capacity perspective, we are witnessing more and more insurers entering the market, offering broader protection, such as technology errors and omissions (E&O) coverage, and higher line sizes. From a product and coverage perspective, there is pressure to reduce waiting periods and retentions.

Additionally, insurers are competing in the range of risk management services they provide, aiming to help clients improve their risk profiles and prepare for potential events. Insurers in the market are offering more bursaries, which significantly aid in implementing additional risk management controls.

With the potential for significant financial loss higher than ever, it’s crucial to check that your cyber coverage reflects the current risk environment. A thorough review of your policy can help identify any gaps in coverage, making sure you are protected against a wide range of cyber incidents, including data breaches, ransomware attacks, and business interruption.

Numerous threat groups exist beyond Scattered Spider and UNC6040

The Scattered Spider attacks served as a wake-up call, not only for retailers and aviation companies, but for all large organisations with IT and customer helpdesks.

UNC6040’s campaign, in which operators impersonated IT support over the phone — deceiving employees into installing modified applications that granted access to sensitive data and enable lateral movement to other cloud services — shows the significant danger posed by these groups.

The attacks demonstrate how sophisticated, multi-stage intrusions can start through deceptively simple means, persuading employees manning helpdesks to grant access to systems.

However, Scattered Spider and UNC6040 are just two threat groups. The reality is that most ransomware events are not highly targeted and do not involve extensive reconnaissance. In fact, the majority take a scattergun approach, making anyone a potential victim, not just retailers. In today’s interconnected and digitised landscape, the inevitability of cyberattacks is no longer a question of “if” but “ when”.

Investing in layered defences, robust access controls, well-practiced incident response plans, and a culture of cybersecurity awareness remains the best defence against such persistent threat actors.

Knowing that you have sufficient coverage in place allows you to focus on your core business operations without the constant worry of potential cyber threats. Organisations should schedule a review of their current cyber insurance policy to ensure that limits are adequate and aligned with their risk profile.

Marsh's multi-disciplined team is here to assist you in navigating this complex landscape and to provide tailored solutions that meet your specific needs.

Authors

Helen Nuttall
Head of Cyber Incident Management at Marsh

Serena France-Hayhurst
UK Cyber Placement Leader, Cyber Risk at Marsh

James Tytler
Senior Associate, Cyber Incident Response, S-RM

Cyber Risk is Complex

Marsh simplifies it for you

Understand

You need to understand what's happening. We help you approach cyber risk with clarity and confidence.

Measure

You need to quantify your cyber risks. We use tools powered by risk intelligence.

Manage

You need to protect your organization. We help you find the right balance between cyber security and insurance solutions.

Respond

You need to be prepared and respond. We help you respond and build resiliency.

About Marsh

Marsh, a business of Marsh McLennan (NYSE: MMC), is the world's top insurance broker and risk advisor. Marsh McLennan is a global leader in risk, strategy and people, advising clients in 130 countries across four businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. With annual revenue of $23 billion and more than 85,000 colleagues, Marsh McLennan helps build the confidence to thrive through the power of perspective. For more information, visit marsh.com, or follow on LinkedIn and X.

This is a marketing communication.

The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

This publication contains third party content and/or links to third party websites. Links to third party websites are provided as a convenience only. Marsh is not responsible or liable for any third party content or any third party website nor does it imply a recommendation or endorsement of such content, websites or services offered by third parties.

Marsh Ireland Brokers Ltd (UK Branch) is authorised and regulated by the Financial Conduct Authority for General Insurance Distribution (Firm Reference No.973159). Marsh Ireland Brokers Limited. Registered in England and Wales Number: BR021174, Registered office: 1 Tower Place West, Tower Place, London EC3R 5BU. Branch VAT Number GB 244 2517 79.

Marsh Ireland Brokers Limited, trading as Marsh Ireland, Bowring Marsh, Charity Insurance, Echelon Claims Consultants, Guy Carpenter & Company, ILCS, Insolutions, Lloyd & Partners, Marsh Aviation Consulting, Marsh Claims Management Services, Marsh Claims Solutions, Marsh Specialty, Marsh Reclaim, and Marsh Risk Consulting, is regulated by the Central Bank of Ireland.

Marsh Ireland Brokers Limited is a private company limited by shares registered in Ireland under company number 169458. VAT Number IE 6569458D. Registered Office: Charlotte House, Charlemont Street, Dublin 2, Ireland, D02 NV26, Ireland, D02 RY98. Directors: A J Croft, P F Doyle, P G Dromgoole (British), J C Grogan, E Kelly, D McGovern, C Nelson (British) and C. Ryan.

Marsh Specialty is a trading name of Marsh Ltd. Marsh Ltd is authorised and regulated by the Financial Conduct Authority for General Insurance Distribution and Credit Broking (Firm Reference No. 307511). Copyright © 2025 Marsh Ltd. Registered in England and Wales Number: 1507274, Registered office: 1 Tower Place West, Tower Place, London EC3R 5BU. All rights reserved.

A business of Marsh McLennan

Copyright © 2025, Marsh LLC. All rights reserved.