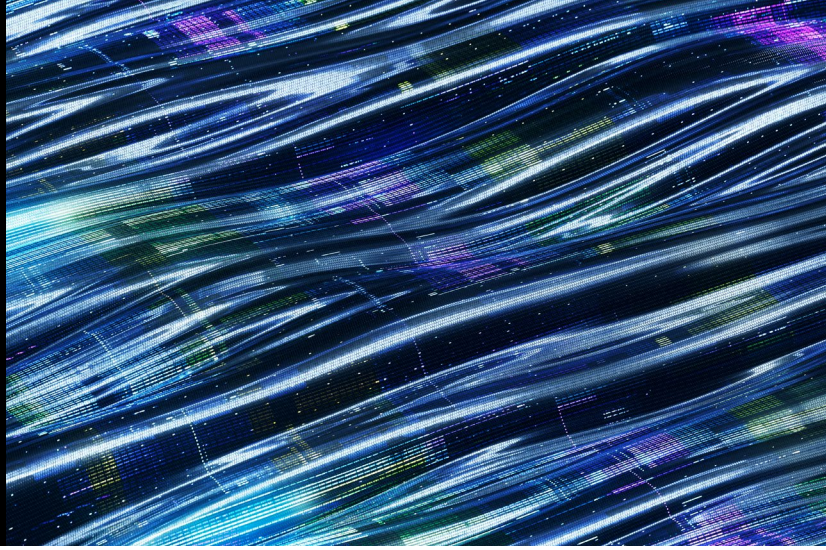
LOCKTON

Cyber and Technology

UK RETAIL SECTOR FACING INCREASED RANSOMWARE THREAT



This note covers why the retail sector is being targeted, steps for all organisations with or without cyber insurance, and technical advice from S-RM, an Incident Response firm supporting organisations in response to these events.

Background

Over the past few weeks, prominent UK retailers have suffered significant cyberattacks. They have caused operational disruption to online orders and the restocking of shelves. Customer data may also be in the hands of the hackers. For all, disruption is ongoing with a trickle effect on the full supply chain.

These cyberattacks may not be linked. However, some reporting suggests that a collective of hackers known as Scattered Spider are behind the attacks.

Scattered Spider are notable in their approach to compromising organisations. They conduct social engineering, often using targeted phishing and voice calls to IT helpdesks to gain access. They appear to be native English speakers, enhancing their ability to socially engineer UK firms.

Why retail?

Typically, cyber criminals target indiscriminately. However, occasionally these criminals will target certain sectors. Although we may never know why Scattered Spider is purportedly targeting retail, the fact that they hold rich customer data, have brand recognition, and busy operations with a complex supply chain make these organisations a prime target.

Whether or not you are in the retail sector cybercrime remains a pervasive threat and understanding the tactics of Scattered Spider may help prevent a future attack.

How is Scattered Spider attacking retail organisations, provided by S-RM

Social engineering	Identity protection	Hypervisor controls
Scattered Spider's principal method for breaking into networks and/or elevating their privileges is social engineering. The latest campaign against UK retailers appears to target IT helpdesks, likely leveraging both OSINT and information drawn from previous data breaches to convince helpdesk operators to change passwords and/or perform MFA resets on valid accounts.	Scattered Spider appear to focus on compromising multiple accounts in order to maintain persistent access to a network, where possible leveraging AD sync to traverse between both on prem and cloud-based environments. We have observed Scattered Spider gaining control of an account and remaining dormant on it before pivoting to use it once other footholds are discovered. This method of persistence is effective in larger environments where domain-wide password resets are challenging to complete rapidly.	Once inside a network, an important technique adopted by Scattered Spider involves traversing to hypervisor hosts, downloading .iso images and using these to deploy new virtual machines. These VMs can be used as a staging point for further exploitation and as a means of evading EDR.
Recommendation: Prevent modifications to any privileged user accounts via the help desk. Provide additional guidance and training to support helpdesk operators in identifying social engineering attacks.	**Recommendation**: Always ensure all active sessions are fully revoked across both cloud tenants and remote access methods such as VPNs following a suspected breach. Incorporate thorough threat hunting of your identity tenant as part of any containment strategy. Consider deploying specialist ID modules alongside your EDR, such as SentinelOne Identity or Microsoft Defender for Identity to improve detection of account-related threats within your tenant.	**Recommendation**: Conduct regular audits of your hypervisors to check for newly created or unexpected VMs. Consider additional role-based access controls to limit which accounts can add new VMs.

Read S-RM's in-depth **cyber threat advice** on the UK retail sector ransomware attacks.

Preparing your business against a cyber attack

Responding quickly and effectively to an incident is crucial to minimise damage. You can:

- ✓ Review and refresh your incident response plan. Confirm contact details are up to date and individuals and teams are aware of their roles and responsibilities.
- ✓ Keep hard copies of your plan.
- ✓ For those with cyber insurance, ensure you have offline contact details of your broking team and numbers to call in the event of an incident. We recommend notifying as soon as possible, to ensure you are supported with third party vendors without delay.
- ✓ For clients without cyber insurance, note that you can always contact your broker for advice. They will put you in touch with Lockton's Cyber and Technology Team (details below) who can recommend external technical, PR and legal companies that are well versed in supporting clients through cyberattacks.

The National Cyber Security Centre (NCSC) has published **a blog post**, that links to **advice on Mitigating malware and ransomware attacks**.

Are you facing a cyberattack?

Do you have cyber insurance? As soon as possible, notify Lockton Claims (**gctclaims@lockton.com**) and your insurer to get swift support that may minimise the impact of an attack.

Don't have a cyber insurance policy but need support? Contact your Lockton broker. We will happily provide recommendations for incident response, PR and legal companies to support your incident response.

For more information, reach out to your Lockton Global Cyber & Technology contact or your broker. Details on what a Cyber Insurance Policy typically covers can be found here.