Incidents impacting retailers – recommendations from the NCSC

A joint blog post by the NCSC's National Resilience Director, Jonathon Ellison, and Chief Technology Officer, Ollie Whitehouse.

Jonathon Ellison, Ollie Whitehouse

A pervasive threat

Cyber criminality, including extortion and ransomware, is one of the most pervasive cyber threats facing UK organisations. It affects organisations of all sizes, from the largest, to the very smallest. No one is immune from this threat. It is both opportunistic and indiscriminate.

Criminals continue to adapt their business models to gain efficiencies and maximise profits, including a clear shift towards 'ransomware as a service' where criminals – often with little technical knowledge or skill comparably – are able to launch attacks using pre-developed tools. This includes tailoring their methods of attack depending on what is most likely to yield the most significant payments.

We all have firsthand knowledge of how devastating attacks can be for victims, with real-world impacts on society, on business, and on individuals. Recovery can be lengthy. And costly.

Recent attacks on the retail sector

The NCSC is working with organisations affected by the recent incidents to understand the nature of the attacks and to minimise the harm done by them, and providing advice to the wider sector and economy.

Whilst we have insights, we are not yet in a position to say if these attacks are linked, if this is a concerted campaign by a single actor or whether there is no link between them at all. We are working with the victims and law enforcement colleagues to ascertain that.

We are also sharing what we know with the companies involved and the wider sector (through our sector-focussed Trust Groups run by the NCSC), and encouraging companies to share their experiences and mitigations with each other.

There are still a lot of unknowns. But there is also a lot we do know.

So what?

Preparation and resilience does not mean just having good defences to keep out attackers. No matter how good your defences are, sometimes the attacker will be successful.

It also means detecting threat actors when they are using your employees' legitimate access (or are on your network, or in your cloud services) whilst being able to *contain* attackers to prevent damage, and to *respond* and *recover* when an attack has got through your defences. There has been speculation in the press that some of these incidents have been carried out by a group known as 'Scattered Spider', as well as discussion about whether social engineering had been used by threat actors targeting IT helpdesks to perform password and MFA (multi-factor authentication) resets, a technique that the group has been reported to use in the past.

We have provided specific guidance to the sector. But we believe by following best practice, all companies and organisations can minimise the chances of falling victim to actors like this.

As well as following NCSC guidance on Mitigating malware and ransomware attacks, organisations are strongly encouraged to:

- ensure 2-step verification (multi-factor authentication) is deployed comprehensively
- enhance monitoring against unauthorised account misuse; for example, looking for 'risky logins' within Microsoft Entra ID Protection, where sign-in attempts have been flagged as potentially compromised due to suspicious

activity or unusual behaviour, especially where the detection type is 'Microsoft Entra Threat intelligence'

- pay specific attention to Domain Admin, Enterprise Admin, Cloud Admin accounts, and check if access is legitimate
- review helpdesk password reset processes, including how the helpdesk authenticates staff members credentials before resetting passwords, especially those with escalated privileges
- ensure your security operation centres can identify logins from atypical sources such as VPNs services in residential ranges through source enrichment and similar
- ensure that you have the ability to consume techniques, tactics and procedures sourced from threat intelligence rapidly whilst being able to respond accordingly

Criminal activity online – including, but not limited to, ransomware and data extortion – is rampant. Attacks like this are becoming more and more common. And all organisations, of all sizes, need to be prepared.

Alongside international partners, the NCSC co-sealed a cyber security advisory highlighting the tactics, techniques, and procedures (TTPs) utilised by Scattered Spider threat actors against a range of sectors. The advisory can be read on CISA's website: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

PUBLISHED

4 May 2025

/

WRITTEN BY

Jonathon Ellison
Director of National Resilience, NCSC

WRITTEN BY

Ollie Whitehouse
Chief Technology Officer (CTO), NCSC

PART OF BLOG

NCSC publications