Report | May 2025

Don’t Be the Next Headline
HOW TO HARDEN AGAINST RANSOMWARE

UK Retail Ransomware Campaign Mitigation Guideline

CTM360®

INDUSTRY Retail

COUNTRY UK

REGION Europe

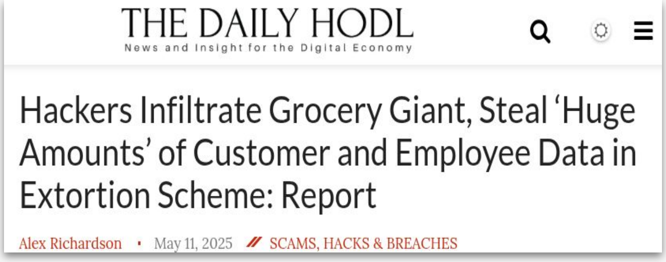
DATE 14-05-2025

Overview

In a series of recent ransomware attacks, major UK retailers experienced severe disruption. These incidents were not caused by advanced technical exploits or unknown vulnerabilities. Instead, they originated from the abuse of trusted systems, including identity platforms, remote access tools, and misconfigured cloud environments. These events serve as a reminder that trust, while essential to operations, can quietly become a vulnerability if not carefully monitored.

While various security vendors have referred to the group behind these incidents by different names, such as **Scattered Spider**, UNC 3944, Muddled Libra, Octo Tempest, and others, this report does not focus on attribution. Rather, it centres on the campaign itself: how the attackers gained access, escalated privileges, and ultimately deployed ransomware to encrypt business-critical systems.

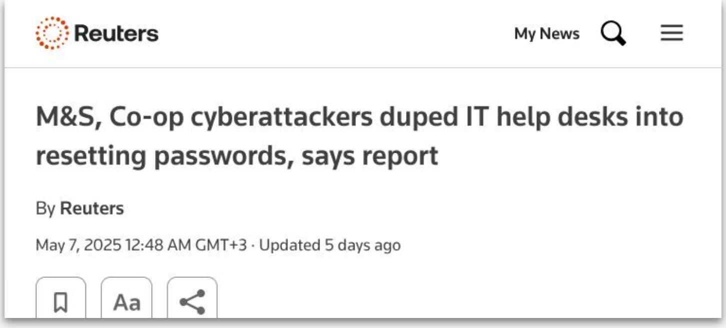
While most reports offer broad security recommendations, **this report takes a focused approach by offering a clear breakdown of the attack into three stages: Initial Access**, **Consolidation and Preparation**, and **Impact on Target**. For each phase, it delivers precise and actionable hardening controls to help strengthen your environment and make your organisation a harder target.



THE DAILY HODL
News and Insight for the Digital Economy

Hackers Infiltrate Grocery Giant, Steal 'Huge Amounts' of Customer and Employee Data in Extortion Scheme: Report

Alex Richardson • May 11, 2025 SCAMS, HACKS & BREACHES

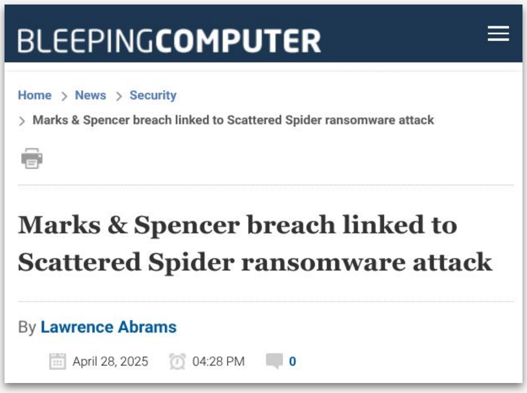


Reuters

M&S, Co-op cyberattackers duped IT help desks into resetting passwords, says report

By Reuters

May 7, 2025 12:48 AM GMT+3 · Updated 5 days ago



BLEEPINGCOMPUTER

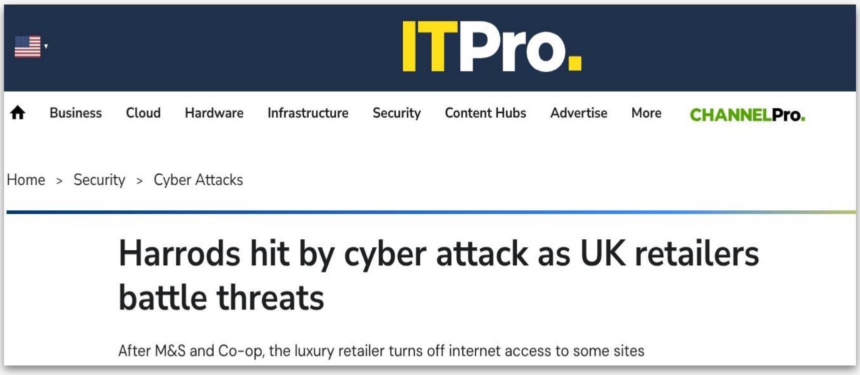
Home > News > Security

> Marks & Spencer breach linked to Scattered Spider ransomware attack

Marks & Spencer breach linked to Scattered Spider ransomware attack

By Lawrence Abrams

April 28, 2025 04:28 PM 0



ITPro.

Home > Security > Cyber Attacks

Harrods hit by cyber attack as UK retailers battle threats

After M&S and Co-op, the luxury retailer turns off internet access to some sites

Analysis of the UK Retail Ransomware Campaign

The attackers behind these campaigns execute credential-driven ransomware attacks that exploit identity, misconfigurations, and misplaced trust within retail environments. This section outlines their tactics across each phase of the attack, highlighting the techniques used and the specific controls organisations can implement to harden their environments.

Phase 1: Initial Access

Where the attacker gained a foothold by exploiting human trust

These campaigns begin not with malicious code, but with manipulation. In the initial phase, the attackers focus on gaining entry by targeting people rather than exploiting vulnerabilities.

They began by impersonating the company's internal IT support, contacting employees through **phishing emails** and **SMS messages (smishing)**. These messages direct victims to fake login pages, such as [brandname]-sso[.]com, designed to harvest usernames and passwords, later to be used for privilege escalation.

Once credentials are obtained, the attackers potentially used **SIM-Swapping technique** by manipulating telecom customer service to transfer ownership of targeted employees' phone numbers to SIM cards under their control. This allows them to intercept **multi-factor authentication (MFA) codes** and access internal systems using **valid credentials**.

> SIM swapping is where a fraudster is able to gain control of your mobile phone number by convincing the phone provider to transfer the service to a SIM in their possession. You may notice that your mobile is no longer connecting and you are unable to make calls or texts.

According to sources in February 2025, the attackers stole the **NTDS.dit** file from the domain controller, a database containing password hashes for all domain accounts. This allowed them to crack passwords, **escalate privileges**, and perform **lateral movement**, ultimately giving them administrative access across the network.

While many ransomware attacks nowadays focus solely on data exfiltration as a single-extortion tactic, this campaign went further by using double extortion tactic, exfiltrating sensitive data and then encrypting systems to directly disrupt business operations.

MITRE ATT&CK Techniques used

- T1566.004 – Spear Phishing via Voice (vishing)
- T1566 – Phishing (emails or smishing)
- T1078.002 – Valid Accounts: Domain Accounts
- T1621 – MFA Request Generation (push fatigue attack)
- T1451 – SIM Card Swap
- T1003.003 – OS Credential Dumping: NTDS

Actionable Security Controls

The following security measures are Group Policy Object (GPO)-based configurations intended for organisation-wide implementation and tailored for the attack phase. These controls can be enforced using Software Restriction Policies (SRP) or AppLocker and should ideally be tested in a staging environment before full deployment.

1. Account Lockout Policy (MFA Fatigue Mitigation)

Purpose: Prevent brute-force and push fatigue attempts. Enforcing an account lockout policy restricts the number of failed login attempts, blocking excessive authentication attempts and alerting defenders to suspicious activity.

- **Aligned MITRE Techniques:**
  - **T1078.002 – Valid Accounts: Domain Accounts** (Prevents repeated unauthorized login attempts using stolen credentials)
  - **T1621 – MFA Request Generation (Push Fatigue Attack)** (Limits abuse of repeated MFA prompts to wear down user response)
- **Threshold:** 5 attempts
- **Duration:** 15 minutes
- **GPO Path**: Computer Configuration → Windows Settings → Security Settings → Account Lockout Policy

2. Block Credential Stealing from LSASS (ASR)

Purpose: Prevent malware or attackers from dumping stored credentials.

- **Aligned MITRE Techniques:**
  - **T1003.001 – OS Credential Dumping: LSASS Memory** (Blocks in-memory credential theft)
- **Rule ID:** 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
- **GPO Path:** Computer Configuration → Administrative Templates → Windows Components → Microsoft Defender Antivirus → Microsoft Defender Exploit Guard → ASR Rules
- **Action:** Enabled (Block Mode)

3. Disable Browser Password Managers

Purpose: Prevent info-stealer malware from extracting browser-stored credentials.

- **Aligned MITRE Techniques:**
  - **T1078.002 – Valid Accounts: Domain Accounts** (Prevents theft and reuse of saved credentials for unauthorized login)
  - **T1621 – MFA Request Generation (Push Fatigue Attack)** (Reduces likelihood of credential theft used in such attacks)
- **Google Chrome:**
  Computer Configuration → Administrative Templates → Google → Google Chrome → Password Manager → Enable saving passwords to the password manager → Disabled

- **Microsoft Edge:**
  Computer Configuration → Administrative Templates → Microsoft Edge → Password manager and protection → Enable saving passwords to the password manager → Disabled

4: Disable RDP (Endpoint)

Purpose: Prevent unauthorised remote access and initial foothold via exposed RDP.

- **Aligned MITRE Techniques:**
  - **T1078.002 – Valid Accounts: Domain Accounts** (Blocks the use of compromised credentials for remote desktop access)
  - **T1621 – MFA Request Generation (Push Fatigue Attack)** (prevents use of RDP as a vector for triggering MFA prompts)
- **GPO Path:** Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections
- **Setting:** Allow users to connect remotely using Remote Desktop Services → Disabled

5. Protect Against SIM Swap Attacks

Purpose: Prevent unauthorized mobile number transfers that allow attackers to intercept MFA codes and compromise sensitive accounts.

- **Aligned MITRE Technique:**
  - **T1451 – SIM Card Swap** (Exploits telecom processes to hijack phone numbers and bypass SMS-based MFA)

Best Practices to Prevent SIM Swapping Abuse

- Turn on two-factor or multi-factor authentication (2FA/MFA) to keep threat actors out of your accounts, even if they know your passwords.

- Use a password consisting of three random words that only you will know and which are unique. You could add uppercase letters, numbers and symbols to make it more secure.

- Do not respond to unsolicited emails, texts or phone calls. These may allow attackers to access personal data which can then be used to convince the mobile network provider or bank that they are you.

Source: Police.uk

6. Block Script-Based Execution (ASR)

Purpose: Stop script-based attacks commonly used by phishing payloads.

- **Aligned MITRE Techniques:**
  - **T1566 – Phishing (Emails or Smishing)** (blocks execution of payloads delivered via phishing)
  - **T1078.002 – Valid Accounts: Domain Accounts** (limits post-access script-based abuse)

- **GPO Path:** Computer Configuration → Administrative Templates → Windows Components → Microsoft Defender Antivirus → Microsoft Defender Exploit Guard → ASR Rules

***Note:** Before implementing the Attack Surface Reduction (ASR) rules listed below, it is strongly recommended to thoroughly test each rule in your environment. These rules are designed to enhance protection against script-based and email-related attacks but may impact legitimate workflows, scripts, or business applications.*

- **Action:** Enabled (Block Mode)
  - **Rule Name:** Block use of copied or impersonated system tools
    - **Rule ID:** c0033c00-d16d-4114-a5a0-dc9b3a7d2ceb
  - **Rule Name:** Block process creations originating from PSExec and WMI commands
    - **Rule ID:** d1e49aac-8f56-4280-b9ba-993a6d77406c
  - **Rule Name:** Block Office applications from creating executable content
    - **Rule ID:** 3b576869-a4ec-4529-8536-b80a7769e899
  - **Rule Name:** Block Office applications from injecting code into other processes
    - **Rule ID:** 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
  - **Rule Name:** Block Office communication application from creating child processes
    - **Rule ID:** 26190899-1602-49e8-8b27-eb1d0a1ce869
  - **Rule Name:** Block JavaScript or VBScript from launching downloaded executable content
    - **Rule ID:** d3e037e1-3eb8-44c8-a917-57927947596d
  - **Rule Name:** Block executable content from email and webmail
    - **Rule ID:** be9ba2d9-53ea-4cdc-84e5-9b1eeee46550
  - **Rule Name:** Block execution of potentially obfuscated scripts
    - **Rule ID:** 5beb7efe-fd9a-4556-801d-275e5ffc04cc

Phase 2: Consolidation & Preparation

Where the attacker strengthens access and prepares for operational disruption

Following the initial breach, the attackers shifted their focus from entry to persistence. Rather than immediately deploying ransomware, they quietly worked to expand their access and prepare for further compromise.

A key step in this stage involved modifying the organisation's identity systems. By adding a rogue **identity provider (Idp)** to the **single sign-on (SSO)** configuration, they created a hidden route to log in repeatedly, even after password resets. **They also registered their multi-factor authentication (MFA) tokens**, giving them continued access without drawing attention.

The attackers closely observed internal activity by reading Teams chats, joining helpdesk calls, and monitoring how the organisation handled security alerts. This gave them an understanding of how to avoid detection and delay response efforts.

They also used legitimate remote access tools, including **Tactical RMM** and similar IT management software, to move across the network. Their goal was to collect credentials, access internal documentation, and identify critical systems such as **Active Directory, SharePoint,** and **VMware infrastructure.**

This stage was about staying undetected while quietly setting the conditions for widespread disruption. By the time ransomware was deployed, the attackers had already mapped the environment and removed many obstacles that might have limited the damage.

MITRE ATT&CK Techniques used

- T1484.002 – Domain Trust Modification
- T1136 – Create Account
- T1219 – Remote Access Software
- T1074 – Data Staged
- T1018 – Remote System Discovery
- T1059 – Command and Scripting Interpreter

Actionable Security Controls

The following security measures are Group Policy Object (GPO)-based configurations intended for organisation-wide implementation and tailored for the attack phase. These controls can be enforced using Software Restriction Policies (SRP) or AppLocker and should ideally be tested in a staging environment before full deployment.

1. Restrict Remote Desktop Services

Purpose: Limit lateral movement via native or abused remote access.
Note: *This control supports mitigation across multiple attack stages, including both phase 1 and phase 2.*

- **Aligned MITRE Techniques:**
  - **T1484.002 – Domain Trust Modification** (limits access to systems where trust settings can be changed)
  - **T1136 – Create Account** (restricts interactive account creation via RDP sessions)
  - **T1074 – Data Staged** (reduces ability to manually stage data through interactive sessions)

- **GPO Path:** Computer Configuration ➔ Administrative Templates ➔ Windows Components ➔ Remote Desktop Services ➔ Remote Desktop Session Host ➔ Connections
- **Setting:** Disable "Allow users to connect remotely using Remote Desktop Services"

2. ASR Rule – Advanced Ransomware Protection

Purpose: Detect pre-encryption staging activities (e.g., reconnaissance, privilege escalation)

- **Aligned MITRE Techniques:**
  - **T1484.002 – Domain Trust Modification** (detects tools/scripts used for trust manipulation)
  - **T1136 – Create Account** (detects scripting and tools used for staged account creation)
  - **T1074 – Data Staged** (detects data preparation activities common before encryption)
  - **T1018 – Remote System Discovery** (detects script-based recon and system enumeration)

- **Rule ID:** c1db55ab-c21a-4637-bb3f-a12568109d35
- **Action:** Enabled (Block)
- **GPO Path:** Computer Configuration ➔ Administrative Templates ➔ Windows Components ➔ Microsoft Defender Antivirus ➔ Microsoft Defender Exploit Guard ➔ ASR Rules

3. Restrict Windows Scripting and Command-Line Binaries (Software Restriction Policy)

Purpose: Prevent leveraging built-in Windows tools (LOLBins) like PowerShell, CMD, or scripting engines to execute payloads or move laterally within the network.

- **Aligned MITRE Techniques:**
  - **T1484.002 – Domain Trust Modification** (blocks scripting tools used to modify trust relationships)
  - **T1136 – Create Account** (prevents use of built-in tools to create local/domain accounts)
  - **T1219 – Remote Access Software** (prevents script-based delivery/installation of remote tools)
  - **T1074 – Data Staged** (disrupts file collection and movement via scripts/LOLBins)
  - **T1018 – Remote System Discovery** (blocks standard command-line based recon techniques)
  - **T1059 – Command and Scripting Interpreter** (prevents abuse of cmd.exe and PowerShell for executing malicious scripts and commands)

- **GPO Path:** Computer Configuration → Windows Settings → Security Settings → Software Restriction Policies → Additional Rules → Right Click → New Path Rule → Enter each of the following paths and set Security Level: Disallowed

Paths to Restrict:

- %WinDir%\System32\cmd.exe
- %WinDir%\Syswow64\cmd.exe
- %WinDir%\System32\cscript.exe
- %WinDir%\SysWOW64\cscript.exe
- %WinDir%\System32\wscript.exe
- %WinDir%\SysWOW64\wscript.exe
- %WinDir%\System32\WindowsPowerShell\v1.0\powershell.exe
- %WinDir%\System32\WindowsPowerShell\v1.0\powershell_ise.exe
- %WinDir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
- %WinDir%\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe

- **Action:** Set each entry to Disallowed to block execution.

4. Restrict PowerShell to Only Run Signed Scripts (Execution Policy GPO)

Purpose: Ensure PowerShell can only execute scripts that are digitally signed by trusted publishers, reducing the risk of running unauthorised or malicious scripts.

- **Aligned MITRE Techniques:**
  - **T1136 – Create Account** (Prevents unauthorized script-based account creation via PowerShell)
  - **T1074 – Data Staged** (Blocks script-driven data collection and preparation for exfiltration)
  - **T1018 – Remote System Discovery** (Restricts use of PowerShell for internal network enumeration)
  - **T1059 – Command and Scripting Interpreter** (limits use of PowerShell for executing malicious scripts and post-exploitation commands)
- **GPO Path:** Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell
- **Setting:** Turn on Script Execution → Enabled
- **Execution Policy:** Allow only signed scripts

Note: *This control is recommended for endpoints or users that legitimately require PowerShell for administrative tasks. It ensures that while PowerShell remains available, only digitally signed scripts from trusted publishers can be executed; minimising the risk of abuse without disrupting authorised usage.*

5. AppLocker or WDAC (Windows Defender Application Control) Policy to Block Task Scheduler Tools

Purpose: Prevent attackers from using tools like schtasks.exe to schedule persistence mechanisms or automate malicious payloads.

- **Aligned MITRE Techniques:**
  - **T1136 – Create Account** (Blocks use of scheduled tasks to automate privilege escalation or persistence through newly created accounts)
  - **T1074 – Data Staged** (Prevents automated execution of staging scripts or payloads via scheduled tasks)

- **GPO Path:** Computer Configuration → Policies → Windows Settings → Security Settings → Application Control Policies → AppLocker → Executable Rules
- Create rules to **allow only trusted users** to execute scheduler-related tools.
- Or explicitly **deny schtasks.exe** for non-admin users.

Phase 3: Impact on Target

Where the attacker maximises disruption to force ransom payment

After spending time preparing silently within the network, the attackers moved to the final and most damaging stage of their campaign, the encryption of critical systems.

Before encryption began, sensitive data was exfiltrated to external cloud storage platforms, such as MEGA[.]NZ. This ensured that even if internal systems were restored, the attackers would retain **leverage for extortion through data exposure**.

The ransomware payload referred to as **DragonForce**, a variant associated with the BlackCat/ALPHV family, was then deployed across the **VMware ESXi infrastructure**. These targeted virtual machines are running essential business services, leading to the shutdown of critical operations. The impact was immediate and severe:

- Online ordering systems became unavailable
- Contactless payment systems failed
- In-store operations had to be run manually
- Internal teams were locked out of key environments
- Significant financial and reputational damage followed

At this point, the attackers no longer needed to hide. Their objective was clear: to hold operational and customer-facing systems hostage and demand payment in return for restoration and non-disclosure of exfiltrated data.

MITRE ATT&CK Techniques used

- T1486 – Data Encrypted for Impact
- T1567.002 – Exfiltration to Cloud Services
- T1114 – Email Collection
- T1530 – Data from Cloud Storage

Actionable Security Controls

The following security measures are Group Policy Object (GPO)-based configurations intended for organisation-wide implementation and tailored for the attack phase. These controls can be enforced using Software Restriction Policies (SRP) or AppLocker and should ideally be tested in a staging environment before full deployment.

1. Restrict Windows Binaries Used for Exfiltration & Encryption (Software Restriction Policy)

Purpose: Block common system tools that attackers abuse for data exfiltration and ransomware deployment.

- **Aligned MITRE Techniques:**
  - **T1486 – Data Encrypted for Impact** (Blocks use of built-in tools to execute or assist in ransomware encryption)
  - **T1567.002 – Exfiltration to Cloud Services** (Prevents abuse of native tools used to upload stolen data to attacker-controlled cloud platforms)

- **GPO Path:** Computer Configuration → Windows Settings → Security Settings → Software Restriction Policies → Additional Rules → Right-click → New Path Rule → Enter each path below:
  - %WinDir%\System32\robocopy.exe
  - %WinDir%\System32\bitsadmin.exe
  - %WinDir%\System32\net.exe
  - %WinDir%\Syswow64\net.exe
  - %WinDir%\System32\net1.exe
  - %WinDir%\SysWOW64\net1.exe
  - %WinDir%\System32\vssadmin.exe
  - %WinDir%\SysWOW64\vssadmin.exe
  - %WinDir%\System32\certutil.exe
  - %WinDir%\SysWOW64\certutil.exe

- **Action:** Set all to **Disallowed**.

Conclusion

Modern attacks do not break down doors; they exploit trust and walk through open ones. Who you are and what you have access to is more valuable than any unpatched server. The attackers do not need the keys to the door, because they were already given to them, often without realising it.

The recent wave of ransomware campaigns against UK retailers has made one thing clear: attackers no longer need zero-day exploits to disrupt a business. Instead, they exploit human behaviour, identity systems, and the everyday tools organisations depend on to operate.

From impersonating IT teams to silently embedding within cloud environments, the attackers use trust as their weapon. The damage caused was not due to a lack of technology, but a lack of visibility, misconfigured access, and weak identity governance.

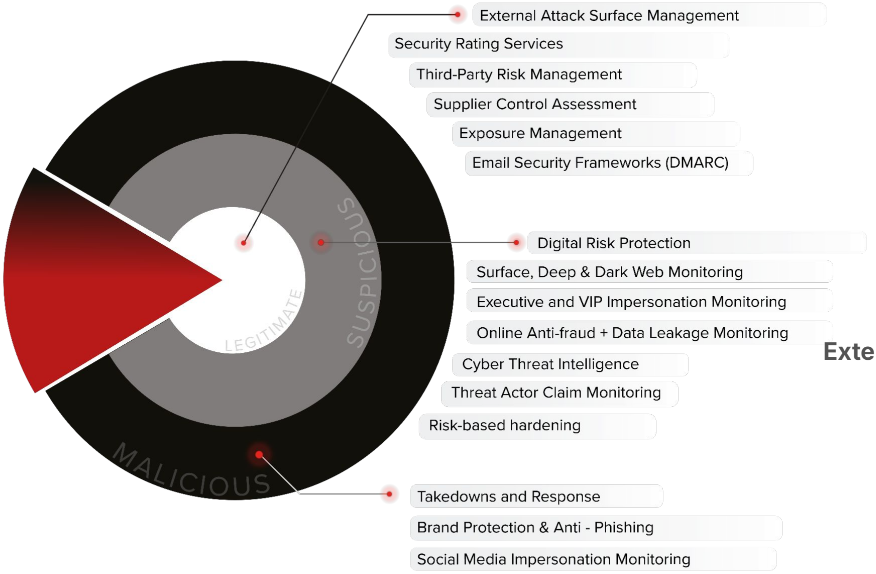
This analysis is part of a wider effort to understand repeatable patterns seen across ransomware groups. As we previously mentioned in our **2023–24 Threatscape Report** and further expanded in the **Ransomware Blindspot Report**, we observed how multiple ransomware groups use the same techniques and consistently exploit the same Windows binaries across organisations, sectors, and regions. These are not isolated events; they are symptoms of a broader issue where the same pathways to compromise are left open.

While this report focuses on the UK retail sector, the lessons are global. To defend against these evolving threats, **organisations must shift their focus to:**

- Understand how their organization appears from an attacker's point of view
- Audit and secure their supply chain digital exposure
- Apply precise, tested hardening controls that prevent abuse
- Strengthen identity and access management
- Monitor internal trust boundaries more closely

The next ransomware breach is unlikely to begin with a malware drop. It may begin with a phone call, a text message, or a login request. True readiness lies not only in technology but in mindset, visibility, and timely action.

How CTM360 Can Help



External Attack Surface Management
Security Rating Services
Third-Party Risk Management
Supplier Control Assessment
Exposure Management
Email Security Frameworks (DMARC)

Digital Risk Protection
Surface, Deep & Dark Web Monitoring
Executive and VIP Impersonation Monitoring
Online Anti-fraud + Data Leakage Monitoring
Cyber Threat Intelligence
Threat Actor Claim Monitoring
Risk-based hardening

Takedowns and Response
Brand Protection & Anti - Phishing
Social Media Impersonation Monitoring

Making you a Harder Target in Cyberspace

External | Consolidated | Turn-key | Fully Managed

CTM360 empowers organisations to detect, manage, and mitigate cyber threats before they escalate, especially during the early stages of an attack. **Below are some use cases of how CTM360 can help strengthen your cybersecurity posture:**

External Attack Surface Management *(EASM)*

You cannot protect what you cannot see: CTM360 reports Indicators of Exposure (IOE) to highlight potential entry points across digital assets, including hosts, IPs and applications. This also includes exposure management.

Digital Risk Protection *(DRP)*

Stop attacks before they start: CTM360 identifies indicators of warning (IOW) and indicators of attack (IOA) to limit time and space for the threat actors to construct an attack.

Third-Party Risk Management *(TPRM)*

You are as secure as your vendor: CTM360 assesses and monitors risks across your supply chain, flagging exposed services, insecure configurations or vulnerable vendors to ensure that security teams can proactively address threats before they impact operations.

Cyber Threat Intelligence *(CTI)*

Risk-based environment hardening: CTM360 provides tailored, risk-based hardening guidelines mapped to real-world TTPs, ensuring your environment is secure, resilient and hardened.

Email Security *(DMARC)*

Fortify Your Email Ecosystem: Defend against domain spoofing and business email compromise (BEC) by gaining visibility across your email ecosystem, monitoring suspicious senders and accelerating DMARC deployment.

References

- https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/
- https://www.reuters.com/world/uk/britains-co-op-is-latest-retailer-be-hit-by-cyber-attack-2025-04-30/
- https://www.itpro.com/security/cyber-attacks/harrods-cyber-attack
- https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/
- https://www.bbc.com/news/articles/c4grn878712o
- https://www.independent.co.uk/news/business/m-s-coop-hack-scattered-spider-it-worker-b2745218.html
- https://gbhackers.com/dragonforce-ransomware-targets-major-uk-retailers/
- https://www.cityam.com/ms-harrods-and-co-op-attacks-expose-uks-growing-cybersecurity-risks/
- https://www.helpnetsecurity.com/2025/05/05/uk-retailers-under-cyber-attack-co-op-member-data-compromised/
- https://theweek.com/crime/scattered-spider-who-are-the-hackers-linked-to-m-and-s-and-co-op-cyberattacks
- https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers
- https://dailyhodl.com/2025/05/11/hackers-infiltrate-grocery-giant-steal-huge-amounts-of-customer-and-employee-data-in-extortion-scheme-report/
- https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-untrusted-and-unsigned-processes-that-run-from-usb
- https://attack.mitre.org/groups/G1015/

Contributor

***Ian Cook** is an internationally recognised cybersecurity expert with over 40 years of experience across global financial institutions and intelligence-driven organisations. His insights into adversary behaviour and defensive control mapping have helped shape the technical precision of this report. He was also inducted into the FIRST Hall of Fame in recognition of his long-standing contributions to global incident response and security collaboration. His career is marked by a consistent drive to bridge threat intelligence with actionable defence strategies at scale.*

in *https://www.linkedin.com/in/ian-cook-a3759922b/*

Disclaimer

The information contained in this document is meant to provide general guidance and brief information to the intended recipient pertaining to the incident and recommended action. Therefore, this information is provided "as is" without warranties of any kind, express or implied, including accuracy, timeliness, and completeness. Consequently, under NO condition shall CTM360®, its related partners, directors, principals, agents, or employees be liable for any direct, indirect, accidental, special, exemplary, punitive, consequential, or other damages or claims whatsoever including, but not limited to loss of data, loss in profits/business, network disruption...etc., arising out of or in connection with this advisory.