KROLL™

Enhancing Retail Sector Resilience against Threat Actors - Scattered Spider and Cl0p

Threat Overview

- Recent cyberattacks targeting the retail industry have crippled logistics, delayed inventory and triggered significant financial losses. Profits and market valuations have been affected.
- Impacted retailers: Cartier, Adidas, Victoria Secret, Marks & Spencer, Harrods, Co-op.
- Intelligence sources indicated that threat groups, Scattered Spider and Cl0p are a high risk to the retail sector. Scattered Spider, which works with the DragonForce ransomware cartel, is known for its speed and proficiency. Cl0p focuses on self-hosted file transfer solutions and subsequent extortion of sensitive data.
- Retailers are targeted due to their vast stores of customer data, complex supply chains and heavy dependence on digital systems.

Kroll experts discuss vulnerability of the retail sector to cyberattack in **CYBERSECURITY DIVE** and on **BBC Radio 5 Live.**

KROLL

Cyber Incidents in Retail

Marks and Spencer

- **Feb** — Initial breach suspected; NTDS.dit file exfiltrated from Active Directory domain controller.
- **April 22** — Cyberattack publicly disclosed causing disruptions to online orders and contactless payments.
- **April 24** — DRAGONFORCE ransomware deployed on VMware ESXi hosts, encrypting virtual machines.
- **April 28** — BleepingComputer attributes the attack to KTA243, detailing the tactics used.

Co-op Group

- **April 30** — Cyberattack disclosed, organization limited access to their infrastructure impacting back office and call centers.

Harrods

- **May 1** — Cyber security incident via unauthorized access announced.

Adidas

- **May 27** — Data breach affecting customer data disclosed. Reportedly due to unauthorized external access gained through third-party.

Victoria's Secret

- **May 29** — Security incident led to the shutdown of its US website and the halting of some in-store services.

Jaguar Land Rover

- **Aug 31** — Cyberattack, attributed to HELLCAT ransomware group, forced Jaguar Land Rover to pause production for nearly six weeks, impacting supply chains and delaying vehicle deliveries.

Sources: BBC, BleepingComputer, Bloomberg, Reuters

Marks & Spencer

- **Lost £650 million** in value
- **30% drop in profits** for current year
- Online orders and contactless payments **halted for 46 days**

Jaguar Land Rover

- Cost **£1.9bn**
- **17.1% drop in retail sales** for the July–September quarter
- **Production halted** for 5 weeks
- **Full recovery ongoing** until 2026

Key Recommendations and Related Services

Recommendation	How we can help
Empower your teams • Evaluate your help desk policies and educate your workforce • Ensure employees are trained to recognize and report the latest social engineering tactics	• Cyber threat intelligence briefings • Help desk social engineering testing and policy/playbook reviews • Employee education and training
Rapidly strengthen your detection capability • Use up-to-date threat intelligence and indicators of compromise (IOCs) to spot emerging attacks and rapidly contain threat activity • Conduct regular red teams and threat emulation assessments—ideally using threat playbooks from groups like Scattered Spider—to identify and address gaps	• Security operations assessments, focused on logging, detection engineering and response playbooks, prioritization of exposures and risks • Testing of capabilities leveraging offensive security experts mimicking targeted threat actors (Red Teams, Breach and Attack Simulation Platforms)
Focus on key security controls • Review identity and access management policies • Enforce least-privilege principles • Consider FIDO2 authentication for sensitive roles • Equip all endpoints with EDR and next-gen antivirus solutions to detect and stop suspicious activity early • Ensure cloud services and identities are secure and compliant with best practices	• Cloud security assessments • Identity security assessments, including SSO, MFA and Active Directory hardening • Endpoint security product configurations, aligned to vendor recommendations
Be prepared to respond • Establish one (or multiple) incident response retainers and touch base with your vendors regularly • Conduct incident response exercises—ideally focused on emulating a business aligned ransom and extortion event—to identify and address gaps	• Enterprise Risk Retainer with rapid incident response SLAs and credits to use across a wide variety of services • Tabletop exercises aligned to your business model and crisis management workflows, modeled after modern attack scenarios • Sensitive data discovery analytics in the event of data theft to support victim and regulator notification • Breach notification services

Need Support? Speak to our Experts

Simon Onyons
Managing Director
+44 207 029 5388
simon.onyons@kroll.com

Janet Burt
Managing Director
Restructuring
+44 782 578 1343
janet.burt@kroll.com

Max Henderson
Global Head of Digital Forensics and Incident Response
+1 813 382 1261
max.henderson@kroll.com

Adam Malone
Managing Director
+1 678 403 3245
adam.malone@kroll.com

Nicole Koopman
Managing Director
+1 212 833 3258
nicole.koopman@kroll.com

Sarah Raymant
Service Line Leader, Restructuring
+44 207 089 0910
sarah.rayment@kroll.com

Experiencing a Cyber Incident? Call Our 24/7 Hotlines

North America: +1 877 300 6816 | **Singapore:** 800 101 3633 | **UK:** +44 (0) 808 101 2168

Australia: 1800 870 399 | **Hong Kong:** 800 908 015 | **Brazil:** +55 0800 761 2318

Additional hotlines at:
kroll.com/hotlines

Or via email:
CyberResponse@kroll.com

Kroll Is a Trusted Leader in Cyber and Data Resilience

Kroll provides reactive, advisory, transformation and managed security services to support clients at every stage of their resilience maturity. Our services leverage frontline risk intelligence from thousands of incident response, regulatory response, financial crime and M&A due diligence engagements per year to anticipate the most likely risks to your business and reduce your unique threat profile.

World's largest IR provider with **over 1000+** IR casesa year

Preferred vendor for **over 85+** insurance carriers

Experience from **government and law enforcement, industry and consulting** backgrounds

EUROPOL

over 700+ experts across 19 countries

Over 100+ certifications

CISM CREST ISO 27001

Expertise in **AI, Crypto, Cloud, Data Analytics, Web 3.0 Security and Data** risk

Over 700k+ actively monitored endpoints

Rated as **industry leaders**

computing Security Excellence Awards 2023 WINNER

FORRESTER® Gartner SC awards 2022 WINNER

2023 Computing Security Awards WINNER

About Kroll

As the leading independent provider of financial and risk advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.