CYXCEL® TRACE

July 2025

The TRACE Brief

Welcome to the first edition of The TRACE Brief, CyXcel's monthly cyber threat intelligence briefing.

UK Retail Under Siege

The rebuild continues for organizations impacted by the Scattered Spider attacks in April, with M&S CEO Stuart Machin stating that online services would "mostly be back by August" with legacy systems and infrastructure under reconstruction and full restoration of both back-end systems and customer-facing platforms projected to be completed by October or November. The M&S attack is forecast to cost around £300m in lost operating profits, and has been attributed to the Dragonforce ransomware group, part of the Scattered Spider network, with attackers exploiting a supply chain partner to gain access.

Co-op reported in mid-June that all stores had resumed normal trading after six weeks of disruption causing short-term stock shortage, shipment delays and temporary payment disruptions.

In other retail attacks, at the start of July threat actors gained unauthorized access to the IT systems of Louis Vuitton, accessing customer information, the third such attack on the LVMH group in as many months after attacks on Christian Dior and Louis Vuitton Korea, showing a worrying increase in attacks on luxury brands, with Harrods subjected to a cyberattack in April and Cartier in May.

Other UK retailers to have been targeted in recent months include Peter Green Chilled, Adidas and The North Face, whilst globally a significant cyberattack on United Natural Foods (UNFI), a major US food distributor caused widespread disruption across their food supply chain, leading to empty shelves and estimated losses of $15m.

On July 10, the NCA announced the arrest of four UK nationals – three teenage boys aged 17, 19 and 19, and a 20 year old woman in connection with the Scattered Spider attacks.

Key Takeaways

- ⓘ Retailers collect vast amounts of personal data attractive to threat actors and operate in a sector with a low tolerance for downtime, both attractive for financially motivated threat actors seeking leverage after attacks.
- ⓘ The interconnected nature of retail operations means a breach can have cascading effects throughout the supply chain.
- ⓘ Cyberattacks can cause lasting harm to brand reputation and customer trust; retailers need to plan effective communications and recovery strategies to reassure customers and stakeholders.

CYXCEL TRACE

July 2025

Public Sector in the Crosshairs

In mid-June Glasgow City Council became the latest public sector organization to suffer a cyber incident, with malicious activity identified on servers by their third-party ICT supplier. Systems were taken offline as a precaution, disrupting essential online service including planning applications, school absence reporting and bin collection schedules. An ICO notification was made as personal data submitted via web forms may have been compromised.

UK councils have become a prime target for attackers in recent months. In May Hounslow Council faced disruption to its email system and internal communications after a targeted phishing campaign. In March Leicester City Council was the victim of an IncRansom ransomware attack, who claimed to have exfiltrated up to 3TB of data, causing considerable disruption to IT and essential services.

IncRansom notoriously targeted Alder Hey hospital late last year, exfiltrating and publishing patient data and donor records, and has targeted several UK-based education providers, including academies in London and Sunderland in the past few months.

Key Takeaways

- Cyberattacks on local authorities often lead to widespread disruption to public services. Many councils rely on legacy infrastructure for some services that are difficult to patch and secure.
- Basic threats still work. Email-based attacks continue to bypass defences, underscoring the need for staff training, phishing simulations and email filtering.
- Modernisation and cyber resilience investment must be prioritized, especially for critical systems supporting health, welfare and housing.

CYXCEL

We offer fully integrated, customizable solutions that combine expertise in technology, cybersecurity, law, and geopolitics.

Rescue

All aspects of incident management and response, to ensure your business emerges from a breach swiftly, effectively, and more resilient.

Resolve

A full-spectrum suite of services to strengthen your business against disruption and threats, while protecting its rights and reputation.

Transform

A bespoke service to upgrade your digital and cybersecurity infrastructure, covering everything from design to delivery.

Operate

Hosted and managed security solutions, specialist industry services, and on-demand access to extra capacity and skills augmentation.

TRACE

CYXCEL® TRACE

July 2025

Attacks on Legal Services

The International Criminal Court (ICC) based in The Hague was hit by a “sophisticated and targeted” cyberattack in late June, coinciding with a NATO security summit held nearby. The incident was detected and contained by the court's internal security mechanisms, and a court wide impact assessment is being undertaken to assess the scope and implications of the incident.

The court faced a similar attack in September 2023, interpreted as a serious attempt to compromise the courts operations and jeopardize justice.

Attacks on courts and the broader legal sector in the UK continue to increase, impacting government legal agencies, law firms and courts of law.

In April, attackers accessed the digital services platform of the Legal Aid Agency (LAA), targeting systems used by law firms and legal aid providers. Attackers reportedly accessed and exfiltrated a significant dataset containing sensitive personal data for up to 2 million individuals who have utilized legal aid services since 2010.

Key Takeaways

- ⓘ The attacks underline the growing threat to international justice institutions, especially those engaged in politically or legally sensitive cases.
- ⓘ Increased geopolitical tensions often lead to a rise in attacks against courts and the legal sector, seeking to undermine or disrupt investigations or justice.
- ⓘ The sector is a key target for nation state actors seeking to gain access to confidential investigations, sensitive evidence or legal strategies that can be used for political leverage or espionage.

Our TRACE team monitors the dark web and digital communications platforms for client exposure and risk across three core areas.

CYXCEL® TRACE

Data, Credentials and Access

We monitor for threats which pose the greatest risks to your organization, searching across stealer marketplaces or initial access brokers offering valid credentials or access to your business, identification of leaked credentials and the offering for sale or exposure of company data.

Organizational Risk

Monitoring for adversarial chat which could indicate an impending or future cyberattack, the registration of domains which may be intended to spoof legitimate company infrastructure.

Supply Chain and Vendor Risks

We dig deeper, monitoring your critical supply chain partners to identify risks which might expose your data or risk downtime which might disrupt your business operations. If a breach does occur within your supply chain, we identify leaked data to allow you to assess the risks posed.