CYXCEL® TRACE

October 2025

The TRACE Brief

Welcome to the TRACE Brief,
CyXcel's monthly Cyber Threat Intelligence briefing.

In Focus: NCSC Annual Review 2025

In October, the NCSC published its annual review for 2025, highlighting a significant escalation in cyber threats to the UK. The past year has seen a record number of attacks, threatening national security, critical national infrastructure and the wider economy, largely driven by a surge in ransomware targeting various sectors, with several high-profile attacks including M&S, the Co-Op and Jaguar Land Rover.

The NCSC supported a record number of nationally significant incidents, up 130% from the previous year.

1,727
Cyber incident reports received from partners and organizations

429
Formally managed by NCSC

204
Nationally significant attacks

18
Highly significant attacks

There are seventeen nationally significant cyber attacks targeting UK organizations every week.

CYXCEL® TRACE

October 2025

In Focus: NCSC Annual Review 2025

The report highlights the ongoing threat from nation state actors, with China a technically proficient threat, alongside capable, though often irresponsible actors, from countries including Iran, Russia and North Korea.

Russia

- Cyber integrated into military and criminal ecosystems.
- **25% increase** in state-linked attacks on NATO members.
- Targets include government networks, think tanks, and logistics.

China

- Identified as the **most technically capable** and globally expansive threat actor.
- Groups targeting telecoms, defense, academia and infrastructure.
- Use of **AI and botnets** to scale reconnaissance.

Iran

- Increasingly **aggressive cyber posture**, intensified by regional conflict.
- Groups focusing on espionage, influence campaigns, and spyware targeting journalists and communities.

North Korea

- Operations are **financially motivated**, led by **Lazarus Group**.
- Targets cryptocurrency, defense, research, and policy institutions.
- Increasing use of **Chinese and Russian infrastructure** to mask origins.

CYXCEL® TRACE

October 2025

In Focus: NCSC Annual Review 2025

In terms of financially motivated threat actors, ransomware remains the largest threat, with more groups than ever before working within the ransomware as a service ecosystem and taking advantage of advances in AI to enhance operations even with a limited skill set.

Supply chains are a growing risk vector, highlighted by notable attacks targeting the weakest link in a supply to gain access to larger organizations, or the broad disruption caused to smaller supply chain partners, as highlighted in the Jaguar Land Rover attack.

The NCSC highlights a sharp rise in attackers leveraging AI to enhance cyber operations. AI is being used to automate reconnaissance, scale phishing campaigns and improve ransomware delivery, even by low-skilled threat actors. Nation state groups like China are deploying AI-driven botnets, while ransomware-as-a-service operators use AI to streamline attacks.

CYXCEL® TRACE

October 2025

In Focus: NCSC Annual Review 2025

To help close the gap between defenses and the complexity of modern cyber threats, the NCSC offers a range of free and proactive services designed to strengthen cyber resilience:

Early Warning Service: With over 13,000 organizations enrolled, this alerts businesses to signs of malware, vulnerabilities and suspicious activity based on threat intelligence feeds. Over 117,000 IPs and 47,000 servers were flagged in 2025.

Active Cyber Defense (ACD): which includes tools such as

- Check Your Cybersecurity – Self-service scans for vulnerabilities in email, browser and IP configurations.
- Suspicious Email Reporting Service (SERS) – Over 34 million reports have led to the removal of 351,000 scam URLs.

Cyber Essentials & Assurance Frameworks: Government-backed schemes to help organizations implement baseline security controls and demonstrate cyber maturity.

Key Takeaways

- ⓘ The report highlights the widening gap between national defenses and complexity of modern cyber threats.
- ⓘ Financially motivated ransomware groups remain the most prominent threat, with large scale attacks causing disruption not only to an organization, but its broader supply chain, as highlighted by the JLR attack, which at around £2b, is the costliest UK cyber attack against a single organization.
- ⓘ The global threat landscape shows the UK facing a complex network of threat actors seeking to use cyberattacks offensively to target critical infrastructure, sensitive data, for political or ideological reasons or to make a financial gain. Organizations must be on guard to disrupt and prevent attacks.

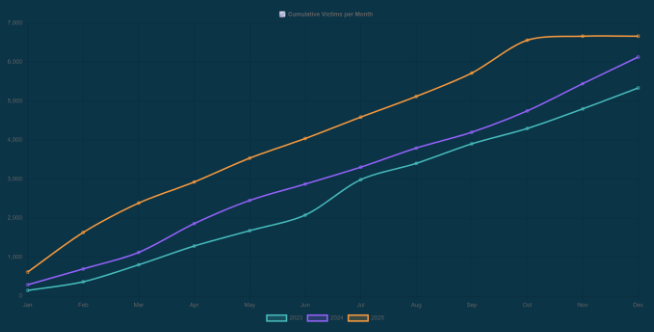
CYXCEL® TRACE

October 2025

Ransomware Round-up

Ransomware attacks show no sign of slowing in 2025, with over 6,500 organizations now published on dark web leak sites since January, more than the total (6,129) for last year and the highest ever.

The UK is the fourth most targeted country, with 222 organizations published to date, behind the US (2,284), Canada (303) and Germany (276).



Data from: ransomware.live

Notable Recent Attacks

In late September 2025, the Kido Nursery Group, operating 18 sites across London and internationally, was subjected to a ransomware attack by the group Radiant, exploiting system vulnerabilities to gain unauthorized access, deploying ransomware that encrypted operational files and exfiltrated sensitive personal data. Approximately 8,000 individuals were affected, including children, parents and staff. The compromised data included names, residential addresses, photographs, safeguarding notes and other personally identifiable information.

Notably, Radiant publicly released samples of the stolen data on dark web platforms and issued direct extortion demands to affected families, requesting payment of approximately £600,000 in Bitcoin.

Subsequently, the leaked data was removed from public access by the perpetrators after public outcry.

The Metropolitan Police launched an investigation, which led to the arrest of two 17-year-old suspects in the UK in early October 2025. The case remains under active investigation.

Also in late September, UK-based property maintenance contractor Dodd Group, which services the Ministry of Defence, was targeted in a sophisticated ransomware and data breach attack by the Russian-affiliated group *Lynx*. The attackers gained unauthorized access and exfiltrated approximately 4 terabytes of sensitive data related to eight Royal Air Force and Royal Navy bases.

The compromized data included controlled military documents, infrastructure plans, contractor records, and operational files for key military sites. Personal information, names, email addresses, and vehicle registrations of MoD personnel, was also exposed. Following failed ransom negotiations, portions of the stolen data were published on the dark web, prompting serious national security concerns.

Key Takeaways

- ⓘ Cyber incidents often result in not only a financial loss but brand trust erosion.
- ⓘ Supply chain providers holding sensitive data are often a target for both financially motivated and nation state actors.

CYXCEL® TRACE

October 2025

Disruptions to Cloud Services

In October, two major cloud service outages affected both Amazon Web Services (AWS) and Microsoft, disrupting access to key online services and office applications.

The AWS incident occurred on 20 October 2025, with a significant outage primarily affecting its US-East-1 region. This disruption cascaded through multiple AWS services, causing widespread failures and degraded performance for hours.

High-profile platforms dependent on AWS, including Snapchat, Prime Video, Signal and Coinbase, faced service interruptions. Despite swift multi-path mitigation, latency and backlogs persisted during recovery, highlighting the impact of infrastructure dependencies concentrated in a single region.

Just over a week later, on 29 October Microsoft Azure suffered a global outage triggered by an inadvertent configuration change within Azure Front Door, a critical content delivery and traffic management service. The misconfiguration led to timeouts, latency, and failures across numerous Azure services such as Microsoft 365 (Outlook, Teams, Power Apps), Xbox Live and third-party customers including Costco, Starbucks, and governmental entities. Recovery was gradual, requiring rollback of the faulty configuration and phased restoration, with full recovery achieved within 12 hours.

Key Takeaways

- The outages highlight the significant operational dependencies that organizations have on cloud infrastructure.
- Even short-lived disruptions can result in widespread service interruptions and business continuity risks.
- These incidents underscore the importance of enhancing cloud resilience through:
  - Architectural diversity, including multi-cloud and hybrid strategies;
  - Operational readiness, with robust incident response and recovery planning;
  - Strategic partnerships, to ensure support and continuity during service failures.