INTEL471

REPORT

UK 2025 THREAT LANDSCAPE: ‘RAMPANT CYBER CRIME’

Prepare for the UK Cyber Security and Resilience Bill and identify opportunities for proactive cyber risk management.

TLP:CLEAR

Introduction

UK organisations are preparing for proactive cyber security risk management, stronger board level oversight of cyber risks, and a dramatic improvement to their monitoring of physical and digital supply chain risks.

This report by Intel 471 — a trusted provider of premier cyber threat intelligence (CTI), exposure management, and intelligence-driven threat hunting packages to many of the UK's largest organisations — aims to identify opportunities for organisations of all sizes and CTI maturity to implement proactive cyber security risk management measures in preparation for the UK's proposed ***Cyber Security and Resilience (CSR) Bill***, and to better defend against the growing frequency and impact of cyberattacks. These include:

- External attack surface management and third-party monitoring
- "Trust but verify" with SaaS and third-party breach and credential monitoring
- Intelligence-driven threat hunting

In April, the British Government unveiled its policy statement for the CSR Bill, the proposed update to the UK's pre-Brexit, EU-based 2016 "NIS1" cyber security directive. The government's policy statement suggests the Bill will align more closely with the EU's updated *Network and Information Systems Directive (NIS2)*, which brought thousands more entities, sectors, and sub-sectors in scope, as well as more stringent rules for cyber risk management, tougher sanctions, stronger enforcement powers for authorities, and C-level accountability.

The UK threat landscape: 'Rampant cyber crime'

Regardless of regulatory updates, the rising frequency and severity of breaches has made cyber security a board-level concern for many organisations. Pending the specifics of the CSR, highly disruptive breaches, such as the ransomware incident impacting UK retailer, Marks & Spencer in May, will likely consolidate cyber risk as a C-suite and board-level concern. The National Cyber Security Centre (NCSC) noted in its advisory following the incident: "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." The NCSC's CEO Richard Horne called these cyberattacks and businesses' failure to prepare themselves for them "plainly intolerable."

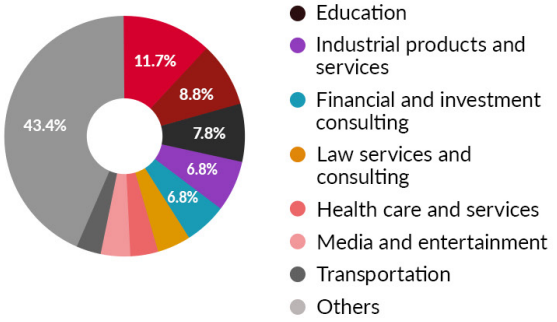
Ransomware and IAB activity impacting UK victims between May 2024 and May 2025

	Claimed UK victim entities	Threat actor/ groups	Industries impacted
Ransomware-as-a-Service	205	43	44
Initial Access Brokers	254	64	46

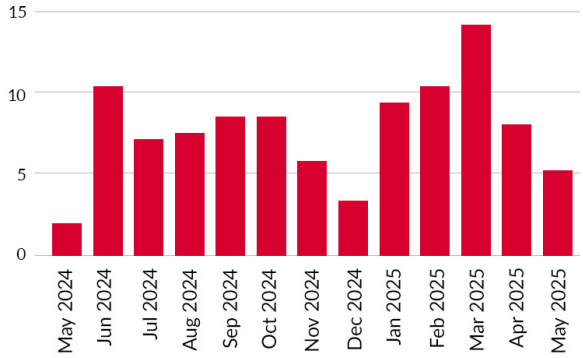
Ransomware impact on UK between May 2024 to May 2025

VICTIM COUNT **205** RANSOMWARE VARIANTS **43** INDUSTRY **44**

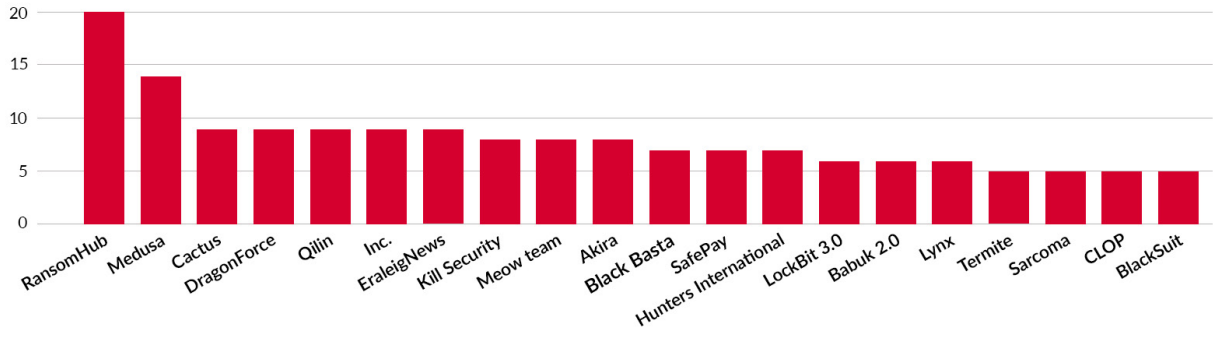
TOP 10 IMPACTED INDUSTRIES



RANSOMWARE BREACH PERCENTAGE PER MONTH



TOP 20 RANSOMWARE VARIANTS



INTEL471

Initial access brokers (IABs), or network intrusion specialists, are a key driver for ransomware-as-a-service (RaaS) groups, data extortion and other cyber attacks. IABs use a range of techniques to breach targets, such as compromised credentials and unpatched vulnerabilities. At Intel 471's **First Quarter 2025 Threat Briefing**[1] — an exclusive overview of threat landscape, threat actor activity, trends, and events for customers — our analysts noted that IAB threat actors were concentrating their efforts on compromising corporate remote access technologies, particularly VPN-based solutions and RDP-based services.

Intel 471 provided key intelligence to EU and U.S. authorities in their coordinated takedown of DanaBot malware infrastructure. This intelligence helps customers to proactively adapt their security controls to meet evolving threats and reduce business risk.

Between May 2024 to May 2025, Intel 471 CTI analysts observed IABs had offered access to 4,771 victims across 132 countries. The **UK was the second most impacted nation,** with 254 alleged victims by 64 IABs. A single threat actor, "sandocan," offered alleged access to 96 identifiable UK victim organisations in this period. Information-stealer malware, which collects logins and browser data on infected machines, are sold in "malware logs" on underground forums to other threat actors, enabling a higher-degree of targeting. This creates more risk for customers of software-as-a-service (SaaS) and cloud-based data platforms.

The Intel 471 Malware Intelligence team collects a vast amount of malware each month, providing customers with unmatched command-and-control level insights into malware targeting and activity covering over 60 malware families, which are currently dominated by information stealers (49%) and loader malware (44%). During the first quarter of 2025, the team linked 34 malware cases to the use of 18 publicly disclosed vulnerabilities (CVEs). This CTI provides customers with in-depth insights into the operations of malware services such as the DanaBot banking trojan that has been redesigning its service to support IABs. Intel 471 provided key intelligence to EU and U.S. authorities in their coordinated takedown of DanaBot infrastructure. This intelligence helps customers to proactively adapt their security controls to meet evolving threats and reduce business risk.

1 https://titan.intel471.com/report/fintel/19c923fdbb9d077e6e78bf23bd3471e9
(For access, please contact your Intel 471 sales representative)

Geopolitics and hacktivism: a dangerous mix for critical infrastructure

An already dangerous digital threat landscape is increasingly impacted by geopolitics, which often drive nation-state hacking and politically-motivated hacktivist cyber attacks.

Hacktivist activity trebled after Russia's invasion of Ukraine. In 2024, hacktivist groups started targeting critical national infrastructure (CNI) industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) equipment. CNI organisations have increasingly networked ICS for remote management, exposing them to remote attacks. In Q1 2025, **Intel 471 CTI analysts identified 34 geopolitical events** that likely corresponded to hacktivist claims, including the pro-Russian hacktivist group Z-PENTEST Alliance which claimed attacks against SCADA and human machine interfaces (HMIs) at multiple locations, including in the UK, U.S., France, Italy, and the Netherlands.

*In Q1 2025, **Intel 471 CTI analysts identified 34 geopolitical events** that likely corresponded to hacktivist claims, including the pro-Russian hacktivist group Z-PENTEST Alliance which claimed attacks against SCADA and human machine interfaces (HMIs) at multiple locations, including in the UK, U.S., France, Italy, and the Netherlands.*

What CSR will likely mean for affected UK entities?

Many large CNI providers within scope of the UK's NIS1 laws may be well-prepared for the CSR Bill. However, under the CSR's "delegated powers" framework, the Secretary of State could bring "new sectors and sub-sectors" in scope of CSR without passing new laws, and order regulated entities to "take action to address threats to and incidents affecting their systems where there is a significant threat to national security."

These changes imply a greater emphasis on proactive cyber risk management based on better insights into evolving digital threats.

The government's policy statement states it intends for cyber incident reporting to be "similar to, and no more onerous than, the equivalent requirements under the EU's NIS2 Directive." Affected entities, including specifically designated "critical suppliers," will need to inform the NCSC of a "significant incident" within 24 hours of discovering an incident, followed by an incident report within 72 hours.

Like NIS2, CSR aims to bring supply chain security and "technological and methodological security requirements" into greater focus for digital firms and operators of essential services (OESs).

NIS2 introduced fines of up to €10 million, or 2% of annual global turnover for essential entities. It also enabled regulators to temporarily ban a CEO or senior management of essential entities from exercising managerial functions. The government has not specified what fines may be issued for non-compliance.

What actions can entities take now?

1. **Help your SOC expedite investigations. Proactively manage and monitor your own and third-party external attack surfaces.**

The NCSC is encouraging an approach called external attack surface management (EASM) for organisations to identify their growing number of internet-facing assets. Vulnerabilities or misconfigurations affecting on-premises IT and in the cloud are routinely exploited by IABs, ransomware gangs, and nation-state actors.

Intel 471 customers rely on our continuous monitoring of third-party breaches and compromised credentials to rapidly and proactively isolate interconnected third-party systems when needed.

Organisations can deploy easy-to-use, pre-configured, CTI-enabled EASM to help prioritise patches with near-real-time alerts of assets affected by vulnerabilities discussed on cyber crime forums and crime-focused Telegram channels.

CTI-enabled EASM can also be used to monitor third-party attack surfaces. Combined with alerts for compromised credentials of third-parties, organisations can proactively mitigate risks when supplier breaches occur.

This proactive approach is critical given the challenge posed by digital asset sprawl following years of rapid digital transformation. This factor has made vulnerability management and patching incredibly difficult. Security operations centers (SOCs) facing 'alert fatigue' are under pressure to perform complex investigations, identify assets that are often not on the asset registry, and prioritise vulnerabilities at the greatest risk of exploitation.

2. **Third-party breach and supply chain visibility.**

Under CSR, organisations will need to be more cognizant of third-party cyber risk. The Software-as-a-Service (SaaS) model introduces further risk. The NCSC identified several risks in its 2024 breach survey, including third-party access to an organisation's systems, suppliers storing personal data or intellectual property, and phishing attacks and malware originating from compromised suppliers. Intel 471 customers rely on our continuous monitoring of third-party breaches and compromised credentials to rapidly and proactively isolate interconnected third-party systems when needed. The NCSC's survey suggests UK organisations are widely exposed to third-party risk. It found that only 11% of UK businesses review risks posed by their immediate suppliers, and 6% are looking at their wider supply chain.

The NHS's open letter to the CEOs of suppliers regarding its new "cybersecurity charter" is a laudable effort to encourage suppliers to lift cybersecurity standards before CSR arrives; and remind the suppliers of their existing legal obligations under UK GDPR. Contractual enforcement has some impact; however, organisations need a way to **"trust but verify"** third-party cybersecurity posture.

3. Strategic intelligence and behavioural threat hunting.

At a strategic level, the Intel 471 global team of CTI analysts help CTI teams, CISOs, and business leaders proactively identify emerging cyber threats and provide expert analysis of geopolitical events that may impact customers' cyber risk and assets in their regions of interest. Intel 471 specialises in cyber human intelligence (**HUMINT**) collection, providing unique insights and cybercrime data sets acquired through direct actor engagement and automated collection from highly-guarded cyber underground sources. The combination of HUMINT, Malware Intelligence, and Adversary Intelligence provides the tactics, techniques, and procedures (TTPs) Intel 471 threat hunters use to create HUNTER platform threat hunt packages. These packages enable threat hunting teams to identify behaviours and TTPs in their environment, such as the use of native operating system processes and tools that advanced threats use to evade traditional detection and avoid setting off alarms.

Conclusion

CISOs, boards, and business leaders assuming ownership of cyber risk as enterprise risk have an opportunity to redefine their relationship to their threat landscape. Cyber is no longer digital. CTI is no longer just about cyber threats. Leaders can use CTI planning frameworks such as the CTI-community-driven CTI Capability Maturity Model, which helps teams to assess their current maturity levels across data collection, analysis and dissemination to stakeholder engagement, and decision making. Organisations should take the time now to prepare for proactive cyber security risk management before the CSR comes into effect.

About Intel 471

Intel 471 equips enterprises and government agencies with intelligence-driven security offerings powered by real-time insights into cyber adversaries, threat patterns, and potential attacks relevant to their operations. By integrating human-sourced intelligence with advanced automation and curation, the company's platform enhances security measures and enables teams to bolster their security posture by prioritising controls and detections based on real-time cyber threats. Organisations are empowered to neutralise and mitigate digital risks across dozens of use cases across our solution portfolios: Cyber Threat Exposure, Cyber Threat Intelligence, and Cyber Threat Hunting. Learn more at www.intel471.com.

Our customers' eyes and ears outside the wire.