Cyberint
A Check Point Company

UK THREAT LANDSCAPE REPORT

Regional & Sectorial Expertise

May 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

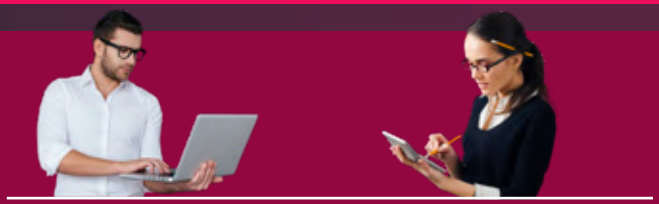
In 2024, cyber threats against UK organizations continued to grow in sophistication and impact across all major sectors. Ransomware remained the most disruptive threat to critical services, while phishing attacks persisted as the most common breach method. Early trends in Q1 2025 show threat actors leveraging new tools, from AI-driven phishing to deepfake scams, making attacks more convincing and harder to detect.

Every industry from healthcare to finance faced cyber incidents, with ransomware attacks on critical infrastructure causing service outages and supply chain breaches impacting multiple organizations via a single compromised vendor. Nation-state hackers (e.g. from Russia, China) intensified espionage and disruption efforts, while cyber criminal gangs expanded Ransomware-as-a-Service operations globally. Emerging threats such as AI-enhanced malware and deep-fake based fraud gained traction, pointing to an even more complex risk landscape in 2025.

To counter these threats, organizations are advised to strengthen basic cyber hygiene (patching, backups, multi-factor authentication) and invest in staff training to recognize attacks. Adopting a proactive security stance including incident response planning, supplier risk assessments, threat intelligence monitoring, and leveraging guidance like the UK's Cyber Essentials framework – will help build resilience. The report provides actionable steps for corporate leaders to mitigate risks and protect their operations.

Most Ransomware Attacked Countries in Europe

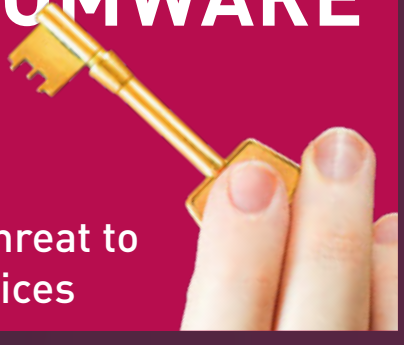
UK Germany France



Business Services Engineering Accounting

Most Ransomware Attacked Industries in the UK

RANSOMWARE



Is the most disruptive threat to critical services

Is the most common breach method

UK THREAT LANDSCAPE OVERVIEW BY INDUSTRY

FINANCIAL SERVICES

Banks, insurance companies and FinTech firms in the UK experienced persistent cyberattacks in 2024. Financial gain is a primary motive, cyber criminals used banking trojans, payment fraud schemes, and ransomware against financial institutions. At the same time, State-sponsored threat actors targeted the finance sector to steal funds or sensitive data: North Korea linked groups have been observed hacking cryptocurrency companies and international banks to bypass sanctions[1].

Although the finance sector's strong security measures have helped contain many threats, high-value targets like payment systems and customer databases remain at risk. In Q1 2025, the trend of sophisticated phishing attacks on banking customers and executives continues, increasingly using deep-fake voices or AI personalized E-mails to trick victims.

[1] NCSC Annual Review 2024

HEALTHCARE

Healthcare organizations continued to be prime targets due to the sensitivity of patient data and the critical nature of their operations. In 2024, ransomware attacks on healthcare providers had severe consequences, for example, an attack on a UK National Health Service (NHS) pathology supplier in June 2024 disrupted lab services and delayed patient critical care. Hospital networks and clinics also faced phishing and malware intrusions, seeking to steal medical records for extortion purposes. Early 2025 trends indicate continued targeting of this sector by both financially motivated criminal groups, and politically and ideologically driven nation-state actors. Considering the industry's lower tolerance for downtime and critical personal data exposure, it has a higher likelihood of paying ransoms, which makes it an attractive target for cyber criminals.

ENERGY AND UTILITIES

The Energy and Utilities sector plays a vital role in the United Kingdom's critical national infrastructure, supplying power to households, businesses, and essential services. Yet, its increasing dependence on digital technologies and interconnected systems has exposed it to heightened cyber risks. In 2023, cyber attacks on UK utility companies surged by an astonishing 568%, rising from 7 confirmed incidents in 2022 to 48 incidents. This trend continued in 2024, with ransomware attacks growing by 80% year-on-year. The integration of operational technology (OT) with information technology (IT), alongside geopolitical instability and aging infrastructure, has widened the sector's attack surface, creating significant vulnerabilities that threaten its operational integrity.

The National Cyber Security Centre (NCSC) has emphasized the "enduring and significant" nature of threats to critical infrastructure, noting that maximum-severity incidents tripled in 2024 compared to the previous year. With the Cyber Security and Resilience Bill expected in 2025, the sector is at a pivotal moment facing both pressing challenges and strategic opportunities to enhance its cyber resilience.

GOVERNMENT & PUBLIC SECTOR

The Governmental and public sectors are highly targeted in the UK - from state-sponsored threat actors (as will be elaborated in the following chapters) to financially motivated cyber crime. One study has found that a single county council of Lincolnshire has experienced 752,797 attempted attacks in 2024, or more than 1,200 per day, during the whole year. The British library, The British museum, NHS and many other public services also experienced cyber attacks in the past 12 months.

The financial impact of cyber attacks on government bodies can be staggering. In 2023, UK organizations spent an average of £1,100 per cyber attack, but for public institutions, the costs can be far greater. The 2025 National Audit Office (NAO) report on Government Cyber Resilience highlights how these attacks not only disrupt essential services but also lead to huge multifaceted costs including initial response, regulatory fines, recovery, litigation, and in some cases, ransom payments.

The financial impact isn't the only problem. Cyber attacks also erode public trust which can prove to also be costly, especially in today's volatile political climate. When government agencies fail to protect personal data or ensure services continue running smoothly, confidence in public institutions undoubtedly takes a hit. Rebuilding that trust can take years, and in the meantime, the British public may become wary of engaging with digital government services. This would ultimately make public services less efficient and more costly to run.

One of the other biggest challenges in tackling cyber threats in the UK is the cyber security skills shortage. The UK Government's Cyber Security Skills in the UK Labour Market 2024 report found that nearly half (44%) of businesses have skills gaps in basic technical areas. Public institutions, which often work within tight budgets, can struggle to attract and retain cyber security professionals, leaving them vulnerable to attacks.

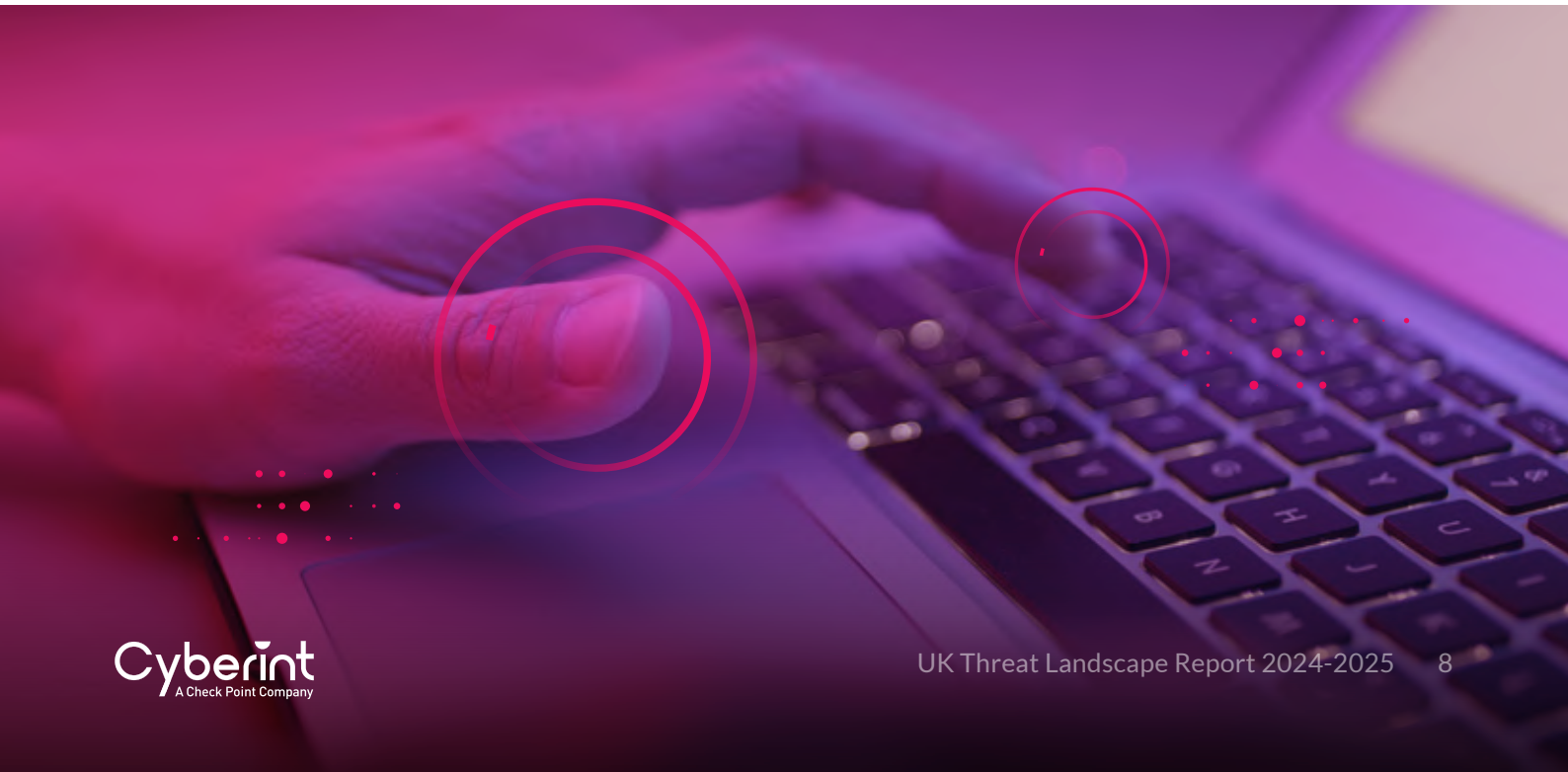
At the same time, many government bodies are still relying on outdated IT systems. The same 2025 NAO report found that 228 legacy systems that lack security patches are still in use across government agencies, with 53% (120 systems) having no fully funded plan for replacement or upgrades. Many of these systems operate on outdated software that no longer receive security updates, making them easy targets for hackers. While replacing these systems is costly and complex, failing to do so only increases the risk of future cyber incidents.

In 2025 the UK government proposed several legislative solutions to raise UK cyber resilience. The first aspect targets the most prevalent threat for UK governmental and public sectors – ransomware.

Councils, schools and NHS trusts are among the many UK victims of ransomware attacks, where attackers encrypt a victim's computer systems and extract data files. The assailants then demand a "ransom" payment, typically in cryptocurrency, to unlock the computers and return the data. Currently, paying ransomware gangs is discouraged by UK authorities but it is not illegal, depending on who is being paid. It is only illegal to pay a ransom if you know or suspect that the proceeds are going to a terrorist organization.

Schools, the NHS and local councils will be banned from making ransomware payments under the new government proposals to tackle hackers. The proposal's rationale is to make public sector and infrastructure organizations less appealing as targets for ransomware gangs. The ban will also apply to critical national infrastructure such as energy and transport networks. Government departments are already banned from paying ransomware gangs, who earned a record $1.1bn worldwide in 2023. Under the proposed ban, payouts by private companies will have to be reported to the government and could be blocked if they are made to sanctioned groups or foreign states. Reporting ransomware attacks will also be made mandatory if the proposals become law.

No major economy has taken steps toward banning ransom payments on quite the scale as that being described in some of the UK's proposals today. It would be a monumental moment for cyber policy should they be passed and implemented.



Another major legislation that will impact the governmental, public, and energy sectors is the proposed Cyber Security and Resilience (CSR) Bill. Slated to enter Parliament later this year, the CSR bill was teased in the King's Speech in July, shortly after the Labour administration came into power. The gist of it is to strengthen the existing NIS 2018 regulations, and future-proof the country's most critical services from cyber threats. The CSR bill comprises three key pillars: Expanding the regulations to bring more types of organization into scope; handing regulators greater enforcement powers; and ensuring the government can change the regulations quickly to adapt to evolving threats.

In addition to the possibility of the government stepping in to make ad-hoc demands in response to systemic events and the associated fines, the CSR bill may include provisions to bring datacenters into scope. Given that the CSR bill's purpose is to improve the cyber resilience of the UK's most critical sectors, it makes sense that datacenters would be treated similarly to hospitals and energy suppliers. Recent research suggests that of the 224 datacenter facilities in the UK, which are managed by 68 operators - 182 sites and 64 operators would be brought into scope of the CSR bill.

Illustrating the scale of the issue that necessitate the CSR bill, in the National Cyber Security Centre's (NCSC) annual review, published in December 2024, revealed that the number of nationally significant incidents it was called in to handle stood at 89 compared to 62 the previous reporting year. Twelve of these were Category 1 incidents – national cyber emergencies requiring Cabinet Office Briefing Rooms (COBR) meetings to be held.

Finally, the CSR bill will allow regulators to be given extra powers to ensure the industries they oversee can meet the requirements of the new legislation and guide in-scope entities on reaching compliance. A big part of this will involve introducing mandatory incident reporting to regulators and the National Cyber Security Centre (NCSC) and requiring more types of incidents (less severe ones) to be reported too, all within a 24-hour time frame. The initial early warning report of a significant breach will have to be made within a day, and a full incident report handed to regulators and the NCSC within 72 hours.

For reference, the EU's NIS2 and the US's CIRCIA enforce 72-hour windows for just the early reporting stage, making the UK's implementation of mandatory incident reporting more stringent than that of its geopolitical peers.

RETAIL INDUSTRY

The retail sector is particularly targeted by fraud due to the high volume of financial transactions processed, the vast amounts of sensitive customer data it stores, and the widespread use of online platforms that offer numerous opportunities for cyber criminals to exploit vulnerabilities for financial gain. These factors[5] make retailers prime targets for a variety of fraud schemes, including payment fraud, return/chargeback fraud, pricetag manipulation, and gift card fraud.

Also, according to a UK-based logistics firm, the UK retail sector has faced a significant surge in fraud, which presents a critical threat to both business continuity and consumer confidence. In 2023, the sector incurred £11.3 billion in losses due to fraudulent activities, with 35% of UK businesses being impacted by fraud. Additionally, a 2024 survey highlighted that 26% of UK consumers feel less secure shopping now compared to ten years ago, with concerns over data breaches and fraudulent transactions being the primary factors[2]. Indeed, when customers perceive a retailer as susceptible to fraud, they often turn to competitors, undermining brand loyalty.

Fraud groups generally remain less visible to the public due to the covert nature of their activities, which contrasts with other cyber criminal groups, such as ransomware operators. Indeed, ransomware groups are more easily identifiable because their attacks often leave clear markers, such as specific ransomware variants and ransom notes that explicitly claim responsibility for the attacks.

On the other hand, threat actors involved in fraud aim to minimize media attention around their operations, allowing them to continue operating their fraudulent activities for as long as possible until the victims become aware of the deception - if they ever do. This is why the most effective way to understand a fraudulent actor's TTPs is by engaging with identified fraud groups as part of HUMINT operations, as it may provide valuable insights into their tactics and help improve prevention efforts.

[2] UK Retailers Lost £11.3bn to Fraud in 2023 - Infosecurity Magazine

IDENTIFICATION OF TOP FRAUD GROUP IN UK / RETAIL

Cyberint, now a Check Point Company's External Risk Management Solution collects multiple sources linked to cyber criminals involved in fraud. Among all these threat actors, our team identified a recurrent group named "UK Fraud Department," which specializes in fraud operations targeting the UK. Analysis of the associated Telegram channel revealed that this group is primarily focused on targeting UK retailers.

Our team identified at least one post in which a group member advertised what seems to be payment fraud services targeting multiple entities.

In this specific post, the threat actor seems to be advertising for sale the Bank Identification Numbers (BINs) and the associated credit card details belonging to customers of the listed brands. The sale of such sensitive information indicates that attackers may have potentially gained unauthorized access to financial databases or systems belonging to the listed companies, enabling them to compromise customers' payment details. Another hypothesis is that the affected customers were initially infected with malware typically designed to steal their personal and financial information.

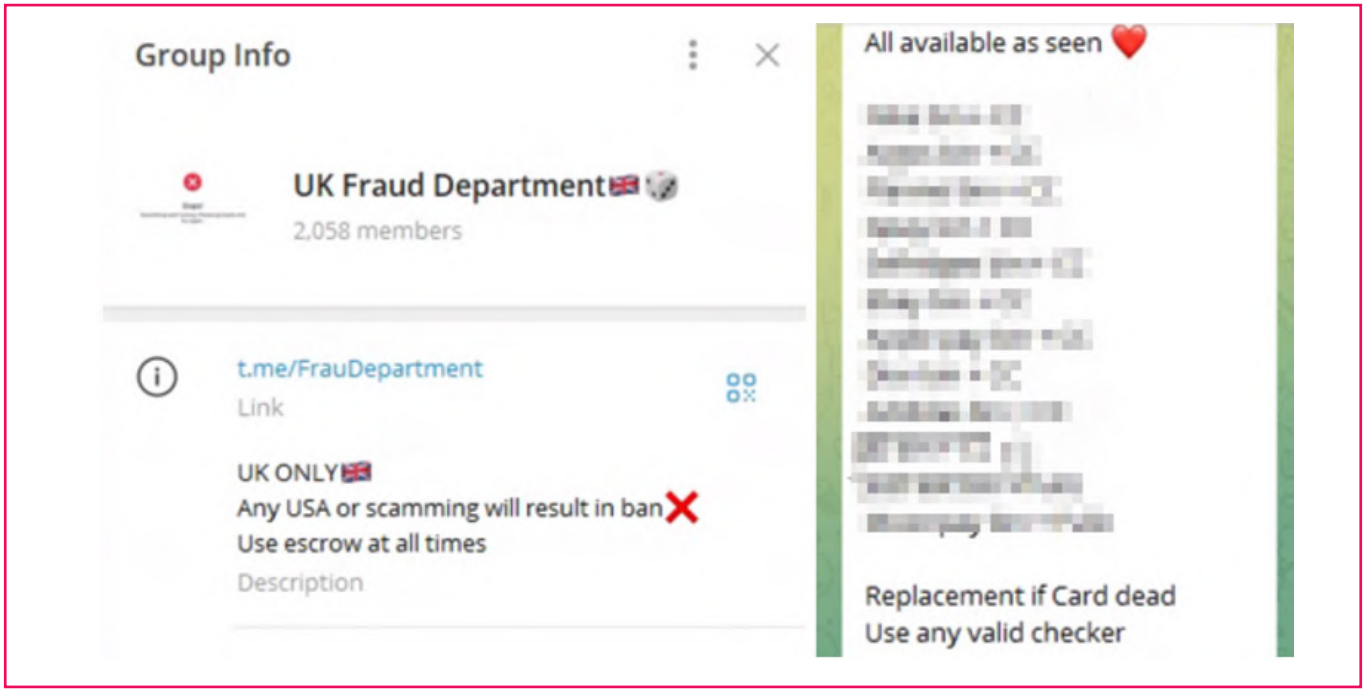


Figure 6: Screenshot of the UK Fraud Department's Telegram channel

COMMON TTPs

As noted earlier in this report, the TTPs used by the different existing fraud groups/actors are rarely disclosed publicly, and the threat actor who shared the message on Telegram did not specify how they obtained the customer details.

Indicators of Compromise (IoCs): When it comes to IoCs related with the "UK Fraud Department" group, there is currently no available information that we were able to track. Since IoC typically refers to an Indicator of Compromise, it is important to collect as much information as possible from the affected victims in order to identify recurring IoCs tied to a specific fraudulent operation. However, in many instances, victims may not realize they are being targeted by a threat actor engaging in fraudulent activity, which hampers the collection of these critical indicators.

In addition, threat actors engaged in fraud may actively and regularly change their attack infrastructure, such as rotating IP addresses, using domain name generation algorithms, AI tools, or employing fast-flux networks to avoid detection by traditional threat detection systems. This strategy can make it particularly challenging to track the group's activities and identify consistent IoCs.

With that in mind, the harvesting of retailers' customers' financial details suggests that these individuals may have been targeted by phishing emails. If this is the case, the phishing emails could involve malicious domains, which are considered IoCs. In these cases, the cooperation of the affected individuals — the retailers' customers — is essential for effectively gathering the necessary information. Their participation can help identify key details such as the malicious emails they received, the domains involved, and any suspicious activity linked to their accounts. This collaboration not only aids in pinpointing IoCs but also enables a faster response to mitigate further damage and prevent the spread of the fraudulent activity.

Furthermore, the theft of sensitive financial information often involves the deployment of malware which is specifically designed to capture personal data, including financial details, and transmit it to a Command and Control (C&C) server operated by the fraudster. Some of the most commonly used malware for this purpose and their related IoCs include Lumma and Redline.

MAJOR CYBER THREATS 2024 AND 2025

RANSOMWARE

Ransomware remains one of the most damaging cyber threats organizations are facing today, with threat actors continually evolving their tactics to maximize the impact and profit. In recent months, ransomware groups have demonstrated increased sophistication, leveraging double and even triple extortion methods, aiming at organizations, critical infrastructure and supply chains.

Cyberint research shows that the UK is the third most attacked country in the world just behind the United States and Canada. It remains the most threatened country in the European Union.

Most Ransomware Attacked Countries Worldwide by Attacks

USA	Canada	UK	Germany	France
#1	#2	#3	#4	#5
Brazil	Italy	India	Australia	Spain
#6	#7	#8	#9	#10

Figure 7: Most attacked countries worldwide

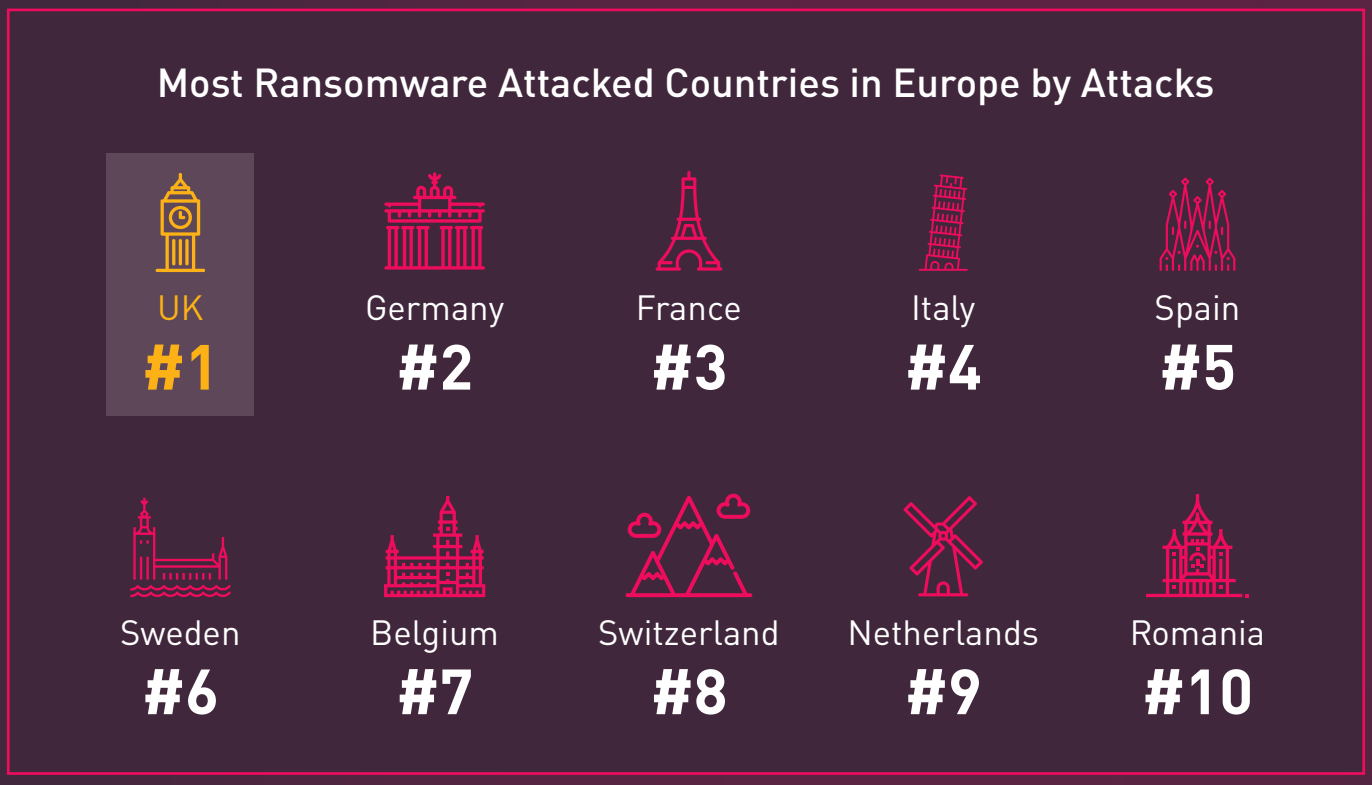


Figure 8: Most ransomware attacked countries in Europe.

An in-depth analysis of UK ransomware incidents reveals **an increase of 37%** in ransomware attacks from Q4 2024 to Q1 2025. While the most targeted industries in 2024 were Business Services, Engineering Accounting as for the Q1 2025 the trend shows also an increase in Educational Services and Wholesale Trade-Durable Goods.

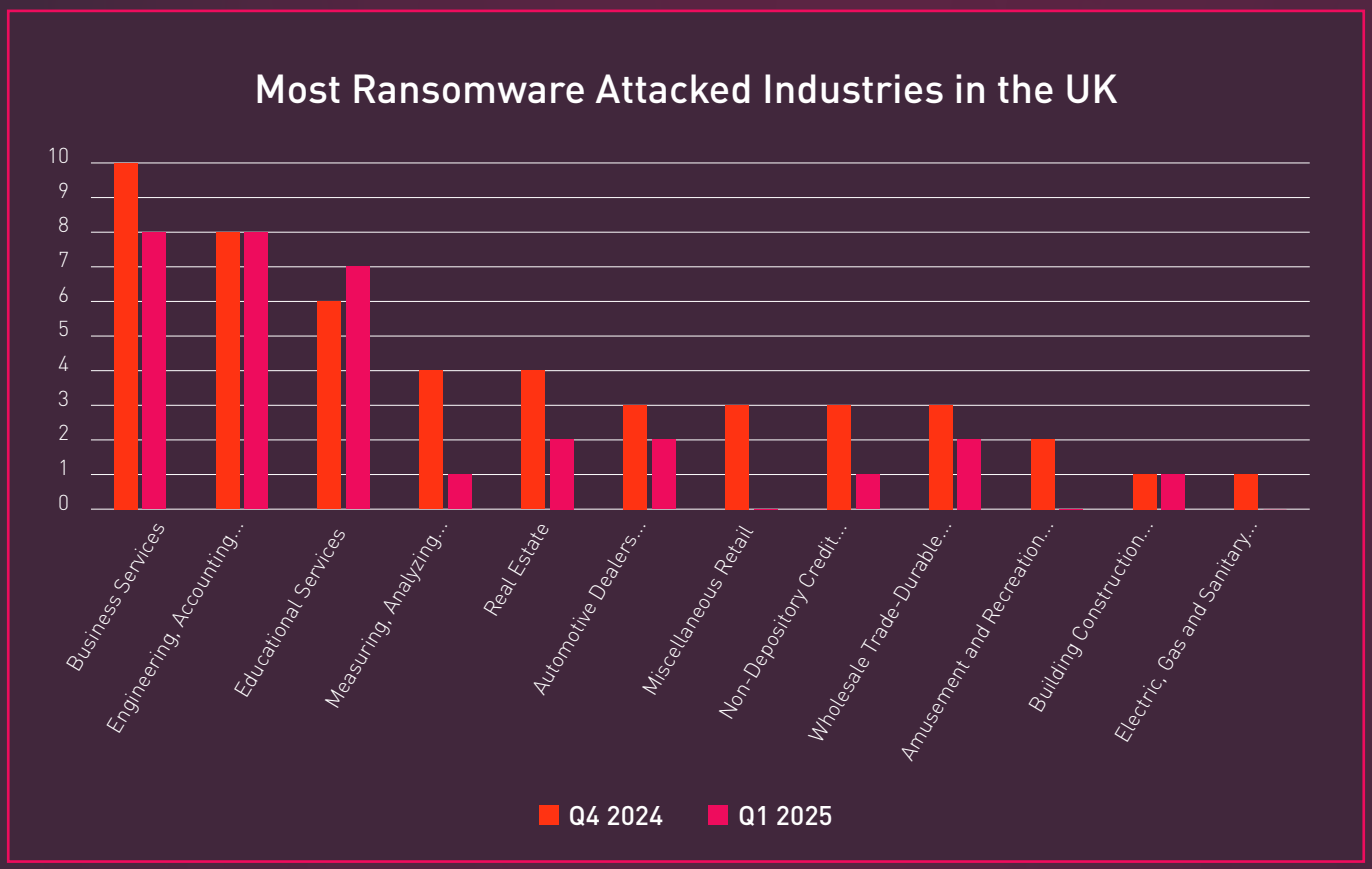


Figure 9: Most ransomware attacked industries in the UK: Q4 2024 - Q1 2025

For Ransomware groups, Cyberint's Q1 2025 analysis revealed a resurge of Medusa and Clop, while Ransomhub remains one of the key actors in the UK landscape:

Most active Ransomware Groups Q1 2025 in the UK

Medusa	RansomHub	Clop	Akira
12%	11%	10%	9%
Kairos	Sarcoma	Termite	DragonForce
6%	6%	6%	5%
Safepay	Babuk2	Inc Ransom	lynx
5%	4%	4%	4%

*Please note that the data provided is limited to observations from Cyberint's sources. While these are significant sources, they do not represent a complete picture of all threat activity

Figure 10: Most active Ransomware Groups Q1 2025 in the UK

INFO STEALER MALWARE

Information stealers, or stealer malware, are malicious programs specifically developed to harvest sensitive data, including financial details, login credentials, and personal information. In addition to credential theft, these threats often target browser cookies, which can enable threat actors to bypass multi-factor authentication (MFA) protections.

Stealer malware typically spreads through phishing campaigns, malicious downloads, and other vectors, underscoring the need for organizations to implement strong security controls to safeguard both customers and employee's data.

The relevance of stealer malware is expected to persist across all industries, driven by the effectiveness of the Malware as a Service (MaaS) model in lowering the barrier of entry for cyber criminals.

In 2024, the UK was among the top three most affected countries in Europe by info stealers, just behind Germany and Spain, with a significant surge in Q4. The first quarter of 2025 reveals an overall increase in infostealer attacks, with the biggest rise seen in Spain and France, placing the UK in 4th place among the most attacked countries in Europe.

Most attacked countries in Europe	Rank Q1 2025	Rank 2024
Spain	1	2
Germany	2	1
France	3	4
United Kingdom	**4**	**3**
Poland	5	5
Italy	6	6
Romania	7	8
Netherlands	8	7
Portugal	9	10
Hungary	10	9

The information-stealing industry is divided among various malware families, with Lumma and Redline remaining the most common stealers used in the UK. Racoon, however, is gaining relevance in the first part of 2025.

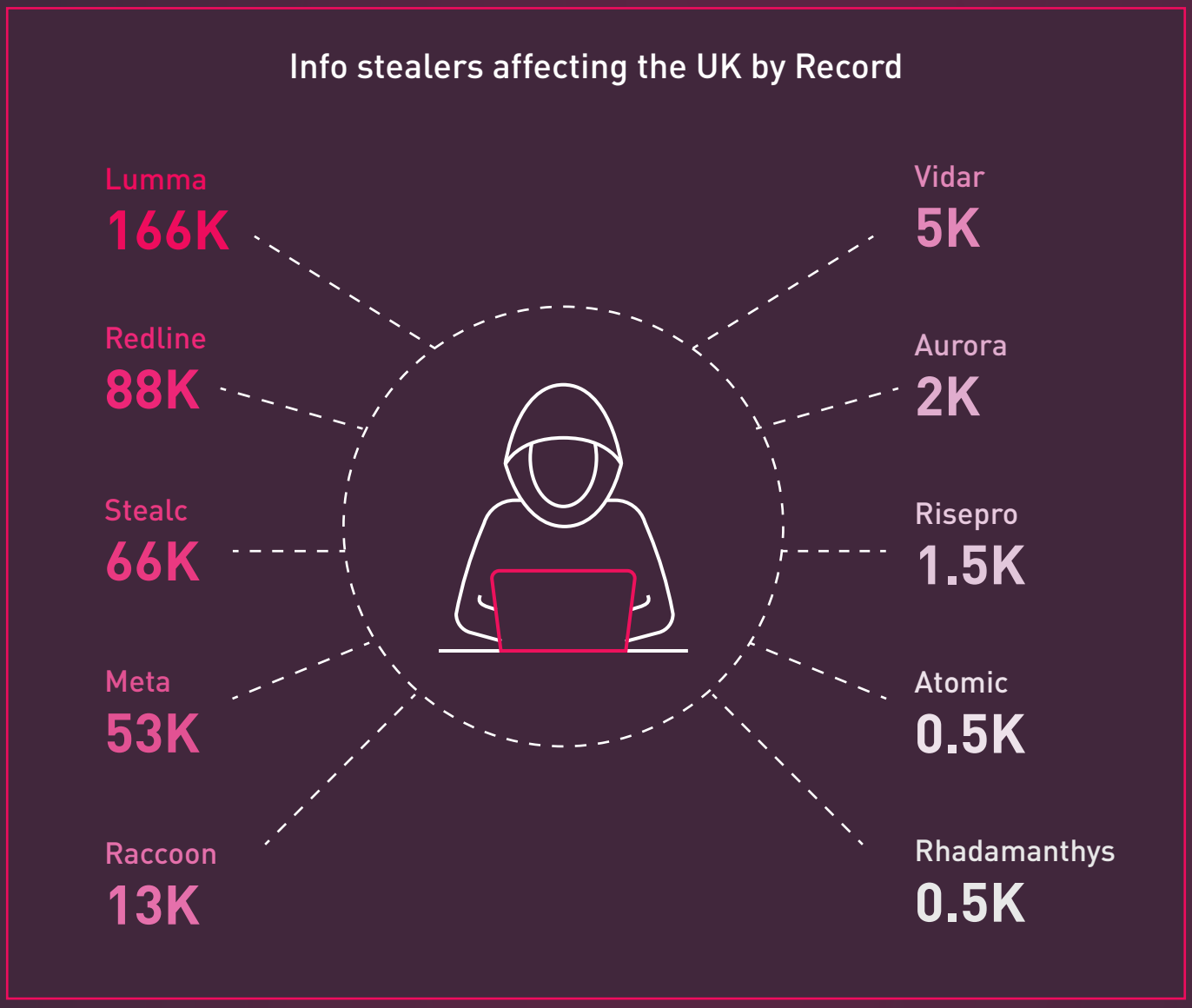


Figure 11: Most active info-stealers

PROMINENT THREAT ACTORS

NATION-STATE THREAT ACTORS

Nation-states continue to pose a fundamental and persistent threat to the UK by using advanced cyber capability against the most critical sectors, seeking to undermine UK. Highly sophisticated tools, techniques and procedures, including use of covert networks, help to obfuscate the activity of these states, increasing the overall impact of their activities and making it harder to attribute attacks.

The UK general election in July 2024 presented an attractive target for a range of threat actors. More generally, threats against UK officials and election candidates – particularly their personal devices and accounts – are seen as a softer target by adversaries and were highlighted in public attributions that included APT31 and threat actors 'Star Blizzard'.

"Our information space has become a geopolitical battleground," stated Kaja Kallas, the EU foreign policy chief, in the third report on foreign information manipulation and interference (FIMI)[3]. Between November 2023 and November 2024, 505 incidents of foreign information manipulation and interference (FIMI) were classified, involving 38,000 channels across 25 platforms. These incidents targeted 90 countries, and 322 organizations, and produced over 68,000 pieces of content. The infrastructure behind these incidents included official state media, covert networks, state-aligned proxies and unattributed channels.

[3] EEAS-3rd-ThreatReport-March-2025-05-Digital-HD.pdf

CYBER CRIMINAL GROUPS AND ECOSYSTEM

Cyberint, now a Check Point Company has assessed the top ransomware / data extortion groups targeting the UK. The following groups have been identified, along with their respective activities within the region and sector:

- **RansomHub**
- **LockBit**
- **BlackBasta**
- **Meow**
- **Scattered Spider**
- **Dragon Force**

RansomHub

RansomHub is a significant player in the ransomware landscape. They emerged after the FBI disrupted ALPHV's operation in December 2023. It is speculated to be a successor to ALPHV, formed with the help of former affiliates. The group made its first attack in February 2024, targeting Brazilian company YKP, and has since compromised over 50 organizations globally, with Business Services and Retail being primary targets.

RansomHub's ransomware, developed in Golang and C++, targets Windows, Linux, and ESXi systems, boasting fast encryption speeds. The group operates under a Ransomware-as-a-Service (RaaS) model, with affiliates receiving 90% of the ransom.

RansomHub's tactics, techniques, and procedures (TTPs) show similarities with ALPHV, and the group is also compared to Knight Ransomware, particularly in their use of Geo-based payloads and obfuscation techniques. RansomHub stands out for its affiliate model and its use of methods designed to disable or terminate endpoint detection and response (EDR) systems, integrating a tool called EDRKillShifter into its attack chain, which allows it to evade detection and maintain a foothold in compromised networks or systems.

```
Hello!

Visit our Blog:

Tor Browser Links:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Links for normal browser:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data
appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The
sooner you pay the ransom, the sooner your company will be safe.


>>> If you have an external or cloud backup; what happens if you don't agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree
with us, information pertaining to your companies and the data of your company's customers will be published on the
internet, and the respective country's personal data usage authority will be informed. Moreover, confidential data
related to your company will be shared with potential competitors through email and social media. You can be sure that
you will incur damages far exceeding the amount we are requesting from you should you decide not to agree with us.


>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because
the negotiations will make them look incompetent,After the incident report is handed over to the government
department, you will be fined <This will be a huge amount,Read more about the GDRP
legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward
them.And you will not get anything, and except you and your company, the rest of the people will forget what
happened!!!!!


>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://an2ce4pqpf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtly7bhid.onion/
- Log in using the Client ID: cf9e1200044391a8502dee45d4396844f4a14541bf76e5d2abd67ad772
```

Figure 12: Screenshot of RansomHub's ransom note

LockBit

Emerging as a dominant force in the ransomware landscape, LockBit ransomware began its wave of attacks in September 2019. Motivated by financial gain, the group boldly targets large, high-profile corporations and enterprises.

LockBit stands out due to its advanced technological sophistication, the use of triple extortion tactics, strong recruitment efforts for affiliates, and the execution of highly impactful cyber attacks. The group operates globally, with occasional pauses that align with the integration of advanced enhancements to their ransomware tools. Their attack strategies have solidified LockBit's position as a significant threat and a formidable player in the cyber world.

Since January 2020, affiliates using LockBit have targeted organizations of all sizes across various critical infrastructure sectors, including retail as a prime target industry. The group operates under the Ransomware-as-a-Service (RaaS) model, with numerous affiliates deploying their constantly updated encryptor across organizations worldwide.

In February 2024, law enforcement agencies charged two Russian nationals linked to the LockBit ransomware group and seized several websites associated with the crime organization, disrupting the group's ability to deploy the malware for file encryption and extortion activities. However, within days of the takedown, the LockBit gang managed to restore its infrastructure and resume operations, getting their malware back online.

In May 2025 the group experienced an attack on their own site leading to significant data leakage.

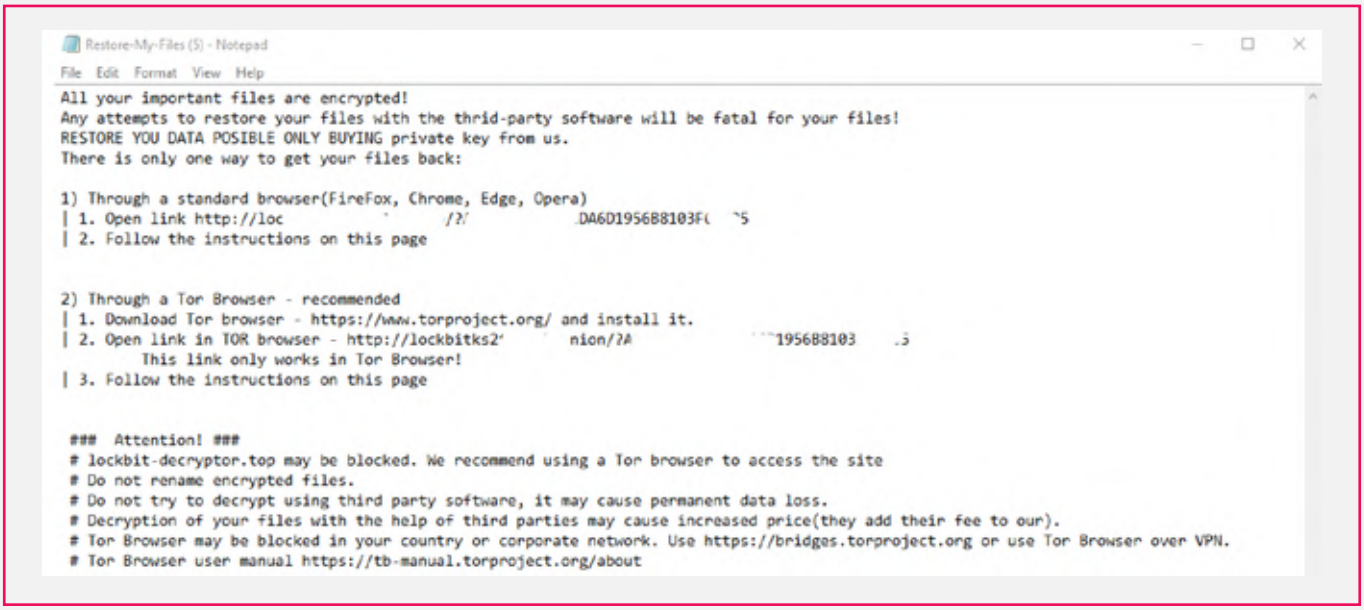


Figure 13: Screenshot of LockBit's ransom note

BlackBasta

BlackBasta is a highly active ransomware group that operates under the Ransomware-as-a-Service (RaaS) model, emerging in early 2022. The group quickly gained prominence for its targeted attacks on enterprises in the U.S., Canada, the UK, Australia, New Zealand, and Japan, employing a double extortion tactic that encrypts data and threatens to leak sensitive information.

The group's attack methodology starts with spear-phishing to gain initial access, often through collaboration with Initial Access Brokers (IABs). Once inside, they use tools like QakBot, MimiKatz, and PsExec to acquire credentials and escalate privileges. They exploit known vulnerabilities such as ZeroLogon and PrintNightmare for lateral movement within networks. The group utilizes Cobalt Strike for remote access and Rclone for data exfiltration, followed by deploying a custom ransomware payload that uses ChaCha20 encryption and Elliptic Curve Cryptography (ECC) for key management.

BlackBasta's operations are believed to be based in Russia, with connections to the disbanded Conti group and possible affiliations with the FIN7 gang. The group has first gained notoriety for targeting critical infrastructure, and has consistently updated its tactics, techniques, and tools to evade detection.

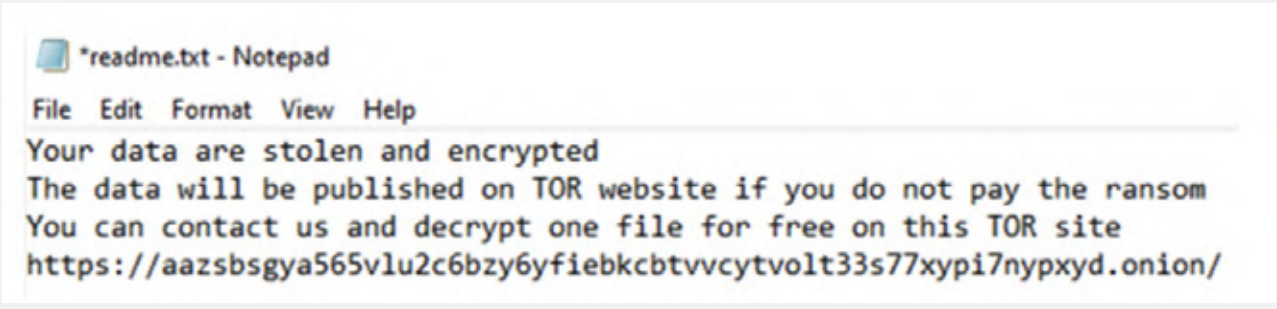


Figure 14: Screenshot of BlackBasta's ransom note

Meow

Meow ransomware is a significant cyber threat that operates with a modified version of the Conti ransomware, retaining much of its core functionality and encryption methods. First identified in late 2022, Meow emerged as one of four strains derived from Conti's leaked code, operating actively until February 2023. Initially relying on encryption to extort victims, Meow employed the ChaCha20 encryption algorithm and demanded payment through email or Telegram. Indeed, the group's ransom note, prominently featuring the repeated phrase "MEOW! MEOW! MEOW!", directs victims to reach out to the attackers through designated email addresses and Telegram channels for ransom negotiations and to recover their encrypted data.

In 2024, however, the group shifted tactics from traditional encryption to data theft and resale, making extortion more reliant on selling stolen data instead of decrypting files. The group now sells stolen data, with prices ranging from $2,999 to $60,000, profiting even when victims refuse to pay the ransom. Meow's victimology primarily targets the United States, with notable hits in several European countries as well, such as UK. Business services are the most frequent target, followed by retail, manufacturing, and government sectors.

The group's infection tactics include phishing emails, exploit kits, Remote Desktop Protocol (RDP) attacks, and malvertising. The ransomware was linked to the leaked Conti v2 source code, and while Meow is associated with an anti-Russian cyber extortion group, its origins remain unclear. The group also gained notoriety in 2024 by opening an account on the Russian hacking forum "Exploit.in", where they distanced themselves from traditional ransomware groups.

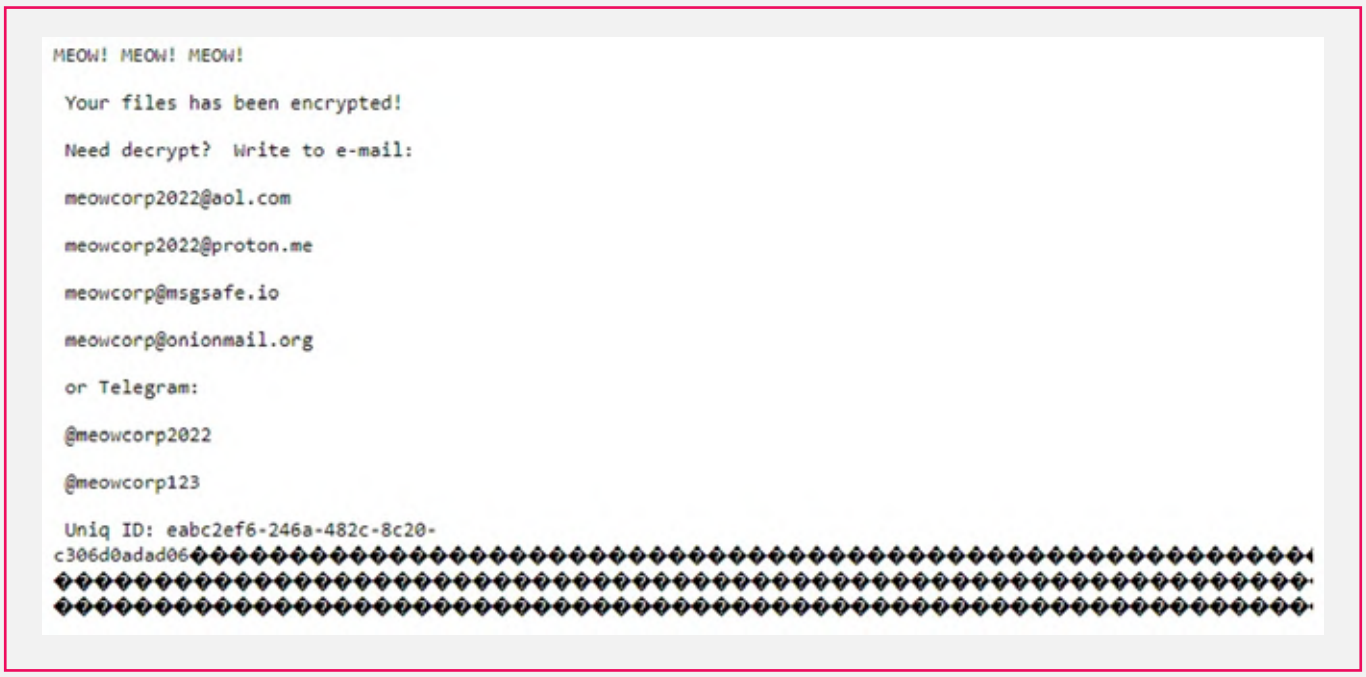


Figure 15: Screenshot of a Meow ransom note

Scattered Spider

Financially motivated Scattered Spider (aka 0ktapus, UNC3944, Octo Tempest) has evolved since May 2022 from targeting telecom and BPO to retail, SaaS, and critical infrastructure via sophisticated social engineering and cloud-native methods.

Their operations have progressed from account takeovers and data theft to ransomware deployment and encryption-optional extortion, employing advanced techniques like BYOVD and OAuth abuse. Affiliations with BlackCat (ALPHV) in 2023 marked a move to multi-platform ransomware, including VMware ESXi.

Recent targeting of UK retail and telco supply chains highlights a focus on high-leverage industries during peak seasons. Scattered Spider's combination of social engineering and cloud exploitation, emphasizing persistence and stealth, poses significant risks. This is particularly true for the UK retail industry due to third-party vendor dependencies and the group's adeptness at lateral movement. High helpdesk turnover and seasonal staff vulnerabilities to vishing during peak sales periods facilitates password resets and MFA attacks, while loyalty data and payment tokens remain valuable targets even without encryption.

The fact that the retail industry relies heavily on customer trust and receives a large amount of personal information from its customers makes it a particularly attractive target for cyber criminals.

DragonForce

DragonForce is a ransomware operation that began in December 2023. The group recently launched a white-label service, allowing other cyber crime teams to use their platform. It is now believed that some members of the Scattered Spider group act as affiliates of the DragonForce collective.

KEY CYBER SECURITY TRENDS AND EMERGING THREATS

AI DRIVEN THREATS & DEEPFAKES

Artificial Intelligence has emerged as a major catalyst for global innovation, driving change across a wide range of industries and reshaping the way people work. While its integration into business processes isn't entirely new, its impact is becoming increasingly evident in areas like medical diagnosis, fraud prevention, predictive equipment maintenance, and tailored shopping experiences in e-commerce. By streamlining routine tasks, enhancing the precision of decision-making, and unlocking deeper insights from data, AI has significantly boosted efficiency and fueled economic development. Its widespread adoption continues to grow as organizations recognize its potential to increase productivity and tackle complex challenges. Recent research shows that nearly 70% of companies around the world have implemented some form of AI, underscoring its growing role in today's business landscape [4].

The rapid rise of AI has also accelerated the emergence of its associated risks. Tools like Deepfakes, once confined to research environments, are now readily available to anyone, even those with minimal technical knowledge. This accessibility has enabled malicious actors to leverage AI for sophisticated scams, manipulate public perception, and breach organizational security. This section explores the major risks posed by AI, highlighting real-world examples and practical approaches to addressing these challenges. With this insight, organizations can better shield themselves from AI-related threats while maximizing the advantages that come with their growing adoption.

[4] Mckinsey: The state of AI in early 2024: Gen AI adoption spikes and starts to generate value. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

AI Powered Phishing and Social Engineering Attacks

Phishing and social engineering attacks, traditionally reliant on generic E-mails or calls, are evolving with AI's ability to analyze large dataset, including social media profiles and corporate communications. AI can craft personalized messages or deepfake audios that mimic trusted individuals, making these attacks highly convincing and extremely difficult to detect. For example, AI can generate E-mails replicating a colleague's writing style or audio impersonating a CEO, tricking employees into disclosing credentials or transferring funds.

These attacks affect all industries in the UK and worldwide as organizations become ever more reliant on digital communication and hybrid work environments. In finance, phishing can lead to unauthorized transactions; in retail, it can compromise costumer data and mislead customers with fake reviews; and in manufacturing, disrupt supply chains. 2025 data indicates that 40% of phishing E-mails targeting businesses are AI-generated, with 56% of organizations reporting social engineering as the most prevalent cyber attack[5].

By 2025, 93% of security leaders are anticipating AI-driven cyber attacks as much as on a daily basis, this underscores the need for a robust employee training and AI powered detections systems, as well as clear and comprehensive internal policies that might prevent unauthorized financial and operational actions.

[5] Top 40 AI Cybersecurity Statistics | Cobalt

Deepfake Enabled Fraud and Impersonation

Deepfakes, defined as synthetic media created using AI, produce realistic videos or audio that can impersonate key personnel. Cyber Criminals use deepfakes to bypass authentication, authorize fraudulent transactions, or gain unauthorized access.

This threat targets organizations for all industries as it might facilitate unauthorized fund transfers, damage brand reputation through fake endorsements, or compromise critical security systems with considerable business disruptions, as the global cost of Deepfake was estimated at $1 Trillion USD for 2024[9]. Moreover, deepfakes can also undermine trust, as stakeholders might question the authenticity of communications or professional endorsements.

The rapid spread of AI-generated fraudulent reviews poses a significant challenge for certain segments of the retail sector, undermining consumer confidence and distorting purchasing decisions. This issue has driven a notable surge in deceptive app reviews, with AI-crafted testimonials frequently appearing on major e-commerce platforms. In some instances, up to 50% of reviews may be inauthentic, characterized by uniform syntax, atypical formatting, and consistently polarized ratings that contradict genuine customer feedback trends. These fabricated reviews are strategically created to manipulate product ratings by overshadowing authentic consumer opinions. Given the scale and sophistication of AI-driven review generation, this issue has escalated into a critical cyber security and consumer protection concern.

The methods used to produce these fraudulent reviews leverage advanced AI language models designed to mimic human-authored content. Automated bots are deployed to inundate e-commerce platforms with favorable reviews for specific products or disparaging reviews targeting competitors. Moreover, generative AI tools can tailor reviews to appear more credible by incorporating personalized elements, such as purchase histories, user preferences, and common consumer concerns.

In the retail industry, where the integrity of consumer feedback is a cornerstone of e-commerce, the consequences of AI-generated fake reviews are profoundly significant. Eroded consumer trust may lead to diminished confidence in online shopping. Additionally, brands face reputational risks if consumers, misled by deceptive reviews, purchase substandard or unsafe products. Ultimately, these challenges expose businesses and consumers alike to substantial financial and reputational vulnerabilities.

A major concern about fraud cyber attacks is the use of AI enhanced bots to amplify the scams, where fake social media accounts often posing as satisfied customers, are deployed to interact with posts, shared fraudulent content, and respond to skeptical users with automated replies defending the legitimacy of the products; all this also aimed at increasing the reason to believe for potential victims.

---

[6] How a new wave of deepfake-driven cyber crime targets businesses | IBM

RANSOMWARE-AS-A-SERVICE AND THE CYBER CRIME ECONOMY

Ransomware as a Service (RaaS) is a cyber crime business model where professional hackers develop ransomware tools and lease them out to other criminals (Affiliates) for a share of the profits. Essentially it operates as a franchise model where creators maintain the malware and payment infrastructure, while affiliates conduct the attacks. This model has lowered the entry barrier for cyber criminal, when even those with limited technical skills can launch ransomware attacks by subscribing or partnering with a RaaS program. For a few hundred dollars, affiliates can buy network access from Initial Access Brokers (IABs), hackers who sell stolen credentials or system access, and then deploy the ransomware from a RaaS kit. The number of attackers using ransomware surged by over 50% in 2024, largely due to readily available and inexpensive RaaS kits advertised on cybercrime forums.

RaaS is part of a more complex ecosystem that includes various specialized roles. Some key components of this underground economy include:

- **Ransomware Developers (RaaS Operators):** Skilled groups that code the ransomware, run leak websites, and handle payments. They profit by taking a part typically 20-30% of ransom payments from affiliates.

- **Affiliates:** These are the attackers who break into targets and execute the ransomware. Affiliates may purchase initial access from brokers or obtain it by themselves, then choose a RaaS platform to deploy. They are the ones holding the operation together by assembling purchased access and malware into a full attack. The affiliate model has vastly scaled up ransomware operations just as a traditional franchise business model would by recruiting an increased number of affiliates.

- **Initial Access Brokers (IABs):** A specialized service where attackers infiltrate organizations (via phishing, hacked RDP/VPN credentials, etc.) and then sell that access to ransomware affiliates on dark web marketplaces. The rise of IABs in recent years has made launching ransomware attacks easier and faster, as access to an organization's network can be bought for just a few hundred dollars, creating a direct correlation between the spikes in IAB activity and ransomware attacks.

- **Money Laundering Networks:** After a ransom is paid, the cyber criminals must convert those funds, typically in cryptocurrency, to cash while hiding their tracks. RaaS leverage Tumbler services and shady cryptocurrency exchanges to launder the payments by breaking the trail into smaller transactions to evade tracing. In some cases, they convert Bitcoin into privacy coins like Monero to further anonymize their money.

Inside RaaS Operations – Affiliates, Brokers and Money Laundering:

1 Initial Access – The Break In

Affiliates acquire initial access, often via Initial Access Brokers offering compromised credentials or vulnerabilities

2 Persistence and Privilege Escalation

Attackers escalate privileges and disable security tools to maintain control and exfiltrate data

3 Deploying Ransomware – The Payload Drop

Affiliates acquire initial access, often via Initial Access Brokers offering compromised credentials or vulnerabilities

4 Extortion and Negotiation

Double extortion tactics are used, pressuring the victim to pay to prevent data release

5 Payment or Recovery

The victim either pays the ransom, whish is splited between affiliate and operator; or begins recovery

6 Cash-Out and Laundering

The ransom is laundered through mixers and exchanges to obscure the money trail

CISO TOP MITIGATION STRATEGIES AND RECOMMENDATIONS

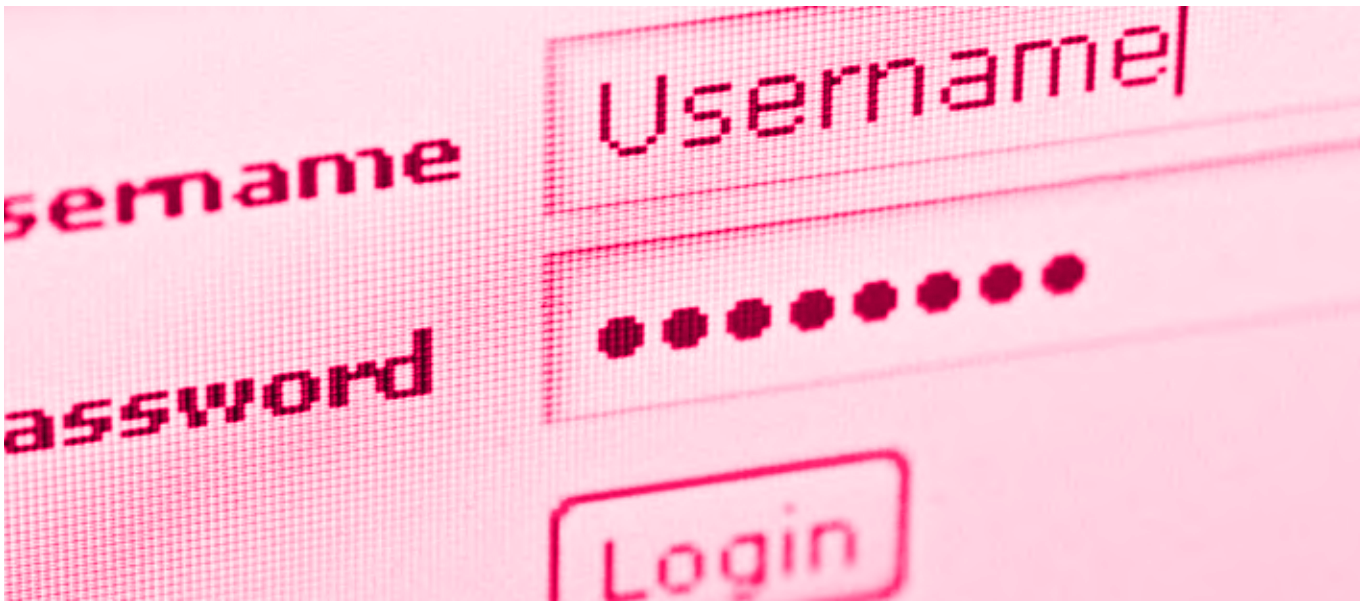
RANSOMWARE PREVENTION

- Maintain a robust patch management process to ensure that security updates and patches are applied in a timely fashion, securing the low-hanging fruit and preventing known vulnerabilities from being exploited.
- Continuously monitor endpoint security events as an early warning of suspicious behavior, for example, host-to-host communications indicating lateral movement or high-volume disk operations indicating mass file encryption or exfiltration.
- Consider monitoring for, and alerting on, the anomalous execution of legitimate Windows command line tools such as the use of net.exe, taskkill.exe and vssadmin.exe.
- Limit user permissions according to the principal of least privilege (POLP).
- Secure sensitive data, adhering to any legal or regulatory requirements, to prevent unauthorized access, be that internal or external in origin.
- Utilize application permits and deny lists to prevent the execution of unauthorized or unknown executables, such as those delivered as part of a broader attack.
- Ensure that disaster recovery plans and backup policies consider regular backups, verification of data integrity and offline storage to facilitate restoration in the event of a catastrophic incident.
- Make use of network segregation to limit communications between nodes, especially end-points, to provide damage limitation and limit the propagation of threats.
- Disable administrative tools and script interpreters to prevent misuse by malicious payloads or threat actors.

PHISHING DETECTION AND MITIGATION

Cyberint, now a Check Point Company recommends taking a proactive approach to ongoing phishing detection. Alongside the detection, we advise executing takedowns of websites based on copyright infringement. Upon request, Cyberint, now a Check Point Company can facilitate the takedown procedure on your behalf.

If the website is part of a broader phishing campaign, Cyberint recommends conducting an investigation. This would help to identify potential vulnerabilities and will enable the implementation of appropriate security measures.



ONGOING MONITORING OF UNDERGROUND PLATFORMS

Cyberint, now a Check Point Company strongly recommend implementing ongoing monitoring of the dark web, hacking forums, and relevant underground platforms frequented by threat actors. This proactive approach is crucial for detecting potential data breaches in a timely manner.

By staying vigilant and monitoring these channels regularly, you can swiftly identify any signs of compromise or unauthorized access to your sensitive information or to third-party vendors of your organization.

Early detection enables prompt response measures, minimizing the impact of potential breaches and safeguarding your organization's assets and reputation. The Cyberint, now a Check Point Company team can gladly support the setting up comprehensive monitoring strategies and implementing robust security measures to mitigate risks effectively.

Multilingual cyber professionals at Cyberint, now a Check Point Company are fully equipped to conduct analysis and investigations on prominent underground forums, encompassing languages such as Chinese, Russian, and others.

COMBATING PROMINENT THREAT ACTING GROUPS

It is essential to adopt a multi-layered security approach and implement best practices tailored to counteract their sophisticated tactics.

- Ensuring comprehensive network segmentation can limit lateral movement within your infrastructure, making it more difficult for Threat Actors to traverse and access sensitive data.
- Employing robust access controls and least privilege principles helps restrict unauthorized access to critical systems and data.
- Implementing regular security awareness training for employees is crucial to enhance their understanding of Threat Actors tactics, ensuring they remain vigilant against phishing attempts and social engineering tactics.
- Additionally, deploying advanced threat detection and response mechanisms, such as intrusion detection systems (IDS) and endpoint detection and response (EDR) solutions, can aid in early detection and swift response to Threat Actors activity.
- Maintaining up-to-date software patches and conducting regular vulnerability assessments can help close potential entry points for Threat Actors.

CONCLUSION

The UK cyber security landscape in 2024 and early 2025 is characterized by an evolving, complex, and increasingly aggressive threat environment. Across all sectors, including financial services, healthcare, energy, government and retail, organizations face increased risks coming both from sophisticated nation-state actors and thriving cyber criminal economy. The ongoing convergence of geopolitical tensions, rapid digital transformation, and the mainstream adoption of emerging technologies such as AI has significantly altered the threat dynamic, challenging traditional cyber security defense mechanisms.

Ransomware remains the most disruptive threat, with the rise of Ransomware as a Service (RaaS) boosting a more accessible cyber crime economy. Simultaneously, information stealer malware has proliferated, particularly impacting industries reliant on customer trust and regulatory compliance, such as financial services, healthcare and retail. Threat actors have increasingly turned to underground marketplaces and decentralized communication platforms, complicating detection and takedown efforts.

Notably, the rapid evolution of AI-driven threats has introduced new attack vectors that make attacks harder to detect and mitigate using traditional methods. As generative AI technologies become more accessible, threat actors are surging with highly targeted, credible attacks that exploit human trust and systemic vulnerabilities.

Nation-state actors continue to pose significant risks, especially to critical infrastructure sectors such as energy and government. Their activities are marked by a dual strategy of intelligence gathering and disruptive operations, often disguised as criminal activity to achieve plausible deniability. Meanwhile, cyber criminal groups have become more organized, resilient, and specialized, forming an underground ecosystem that supports everything from malware development to laundering stolen assets.

New and proactive security strategies are essential for organizational resilience. CISO's and executive leadership must prioritize comprehensive intelligence-driven defenses, strengthen ransomware prevention, enhance phishing detection, continuously monitoring of underground forums, and developing capabilities to disrupt threat actor operations. Collaboration between sectors, intelligence sharing, and investment in advanced threat detection technologies are critical to stay ahead of emerging risks.

Finally, the UK's cyber threat landscape requires an adaptive and proactive approach that balances robust technological defenses with heightened focus on human factors. Organizations must embrace cyber security as a core element of their business strategy to be better positioned to safeguard their operations, reputation, and stakeholders, in the face of an increasingly hostile digital world.

CONTACT US

ISRAEL

Tel: +972-37-286-777
17 Ha-Mefalsim St Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House,
14-18 Great Titchfield Street,
London, W1W 8BD

USA - TX

Tel: +1-646-568-7813
7250 Dallas Parkway STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
Level 42, Suntec Tower 3,
8 Temasek Boulevard. Singapore 038988

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road
Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm