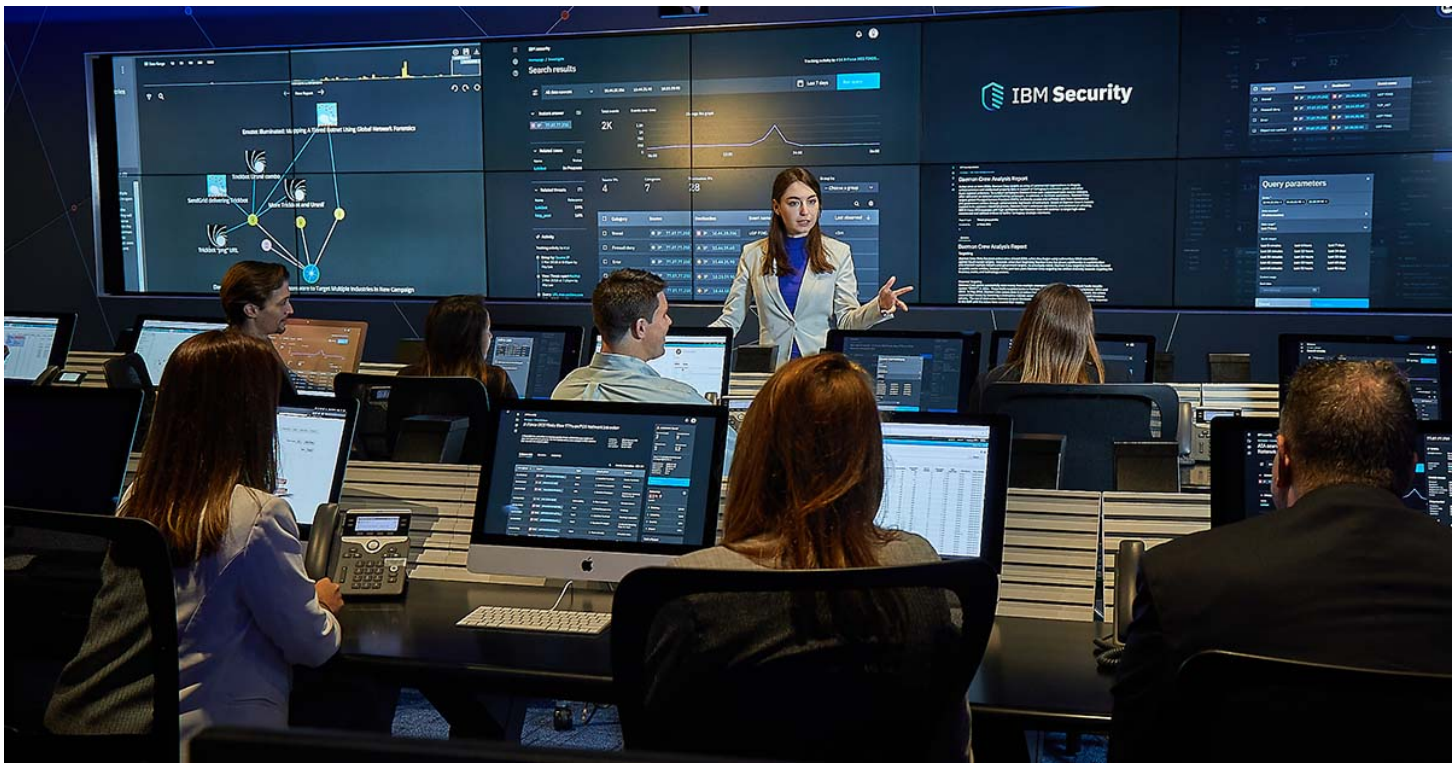
IBM UK Newsroom

IBM Report: Vulnerable UK energy system among top targets for cybercriminals as businesses face growing extortion threat

Data shows the UK was the most attacked country in Europe, with the energy and finance sectors each receiving 16% of cyberattacks in 2022.

Most common outcome of cyberattacks in the UK was extortion (57% of cases) – more than double the global average - primarily achieved through ransomware or business email compromise (BEC) attacks.

Globally, despite improved threat detection, the average time to complete a ransomware attack dropped last year from two months to less than four days.



ARMONK, N.Y. and LONDON, UK, FEBRUARY 22, 2023 – IBM Security (NYSE: IBM) today released its 2023 X-Force Threat Intelligence Index, which revealed that the UK's energy industry was among the primary targets for cyberattacks for the second consecutive year, seeing 16% of all attacks. The UK was the top-attacked country in Europe, accounting for 43% of the attacks X-Force observed, followed by Germany (14%), Portugal (9%), Italy (8%) and France (7%).

With rising energy bills a key factor in the squeeze on UK consumer finances, the report highlights the threat of further pressure on an already vulnerable energy sector and the potential for data breach costs to trickle down to consumers through price rises. As many UK businesses strive to carefully manage costs, there is heightened risk of cybersecurity investment falling and vulnerabilities proliferating.

Cyber extortion threat grows across Europe

The most common impact from cyberattacks in 2022 was extortion, which was primarily achieved through ransomware or

business email compromise attacks. With threat actors often seeking to exploit geopolitical tensions, the report found that Europe was the most targeted region for extortion in 2022. More than half of the cases X-Force observed in the UK involved extortion (57%) – twice the global average - followed by data theft (29%).

Backdoor deployments - malware that provides remote access - were the most common attacker action observed in the UK in 2022, comprising 18% of cases. Gaining backdoor access often precedes ransomware attacks, distributed denial of service (DDoS) attacks, and deployment of remote access tools, which were each involved in 14% of UK incidents.

Cybercriminals are overwhelmingly exploiting IT vulnerabilities in UK organisations to gain initial access. Last year, 50% of UK incidents — nearly twice the global average — were caused by the exploitation of vulnerabilities, highlighting the need for stronger vulnerability management programs, including better understanding of attack surfaces and risk-based prioritisation of patches.

Laurance Dine, Global Lead, IBM Security X-Force Incident Response said: “Extortion is a battle-tested technique that has grown even more pervasive than ransomware. It’s not only piling financial pressure on key UK sectors at a challenging time, but in many cases theburden is passed on to consumers in the form of price rises, exacerbating the cost of goods and utilities. Ultimately, attackers are always innovating and cyber-security strategies should be just as flexible and adaptable.”

Julian David, CEO, techUK said: “At a time of real economic uncertainty, this important report makes it clear that cyberattacks result in significant costs for organisations and citizens across the UK. The surge in extortion-based attacks is a real concern and it is critical that all UK organisations implement a flexible cyber strategy that encompasses people, process and technology. No out-of-the-box solution guards against these ever-changing and pervasive threats.”

James Sullivan, Director, Cyber Research, Royal United Services Institute (RUSI) said: “This report from IBM provides valuable evidence to show that cybercrime, in particular extortion from ransomware and BEC fraud, continues to impact the UK. If the UK’s aspiration for a ‘whole of society’ approach to cyber resilience is to be realised, how the country responds to cyber extortion over the coming years may be one way to bring the concept to life.”

The IBM Security X-Force Threat Intelligence Index tracks new and existing trends and attack patterns – pulling from billions of datapoints from network and endpoint devices, incident response engagements and other sources.

Globally, the 2023 IBM Security X-Force Threat Intelligence Index also found:

- Backdoor ‘profit equation’: A global uptick in backdoor deployments can be partially attributed to their high market value. Globally, X-Force observed threat actors selling existing backdoor access for as much as $10,000 – compare this to stolen credit card data, which sells for less than $10 per card today. This financial incentive has helped spur innovation from attackers.
- Cybercriminals Weaponise Email Conversations. Thread hijacking saw a significant rise in 2022, with attackers using compromised email accounts to reply within ongoing conversations posing as the original participant. X-Force observed the rate of monthly attempts increase by 100% compared to 2021 data.
- Legacy Exploits Still Doing the Job. The proportion of known exploits relative to vulnerabilities declined 10 percentage points from 2018 to 2022, due to the number of vulnerabilities hitting another record high in 2022. The findings indicate that legacy exploits enabled older malware infections such as WannaCry and Conficker to continue to exist and spread.

The report features data and insight IBM collected globally in 2022 about the global threat landscape, to inform the security community about the threats most relevant to their organisations. You can download a copy of the 2023 IBM Security X-Force Threat Intelligence Report here.

ENDS

Additional sources

- Read more about the report's top findings in this IBM Security Intelligence blog.
- Sign up for the 2023 IBM Security X-Force Threat Intelligence Index webinar on Thursday, March 2, 2022, at 11:00 a.m. ET here
- Learn more about how IBM's Threat Detection and Response Portfolio can help
- Schedule a consult with IBM Security X-Force

About IBM Security

IBM Security helps secure the world's largest enterprises and governments with an integrated portfolio of security products and services, infused with dynamic AI and automation capabilities. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to predict threats, protect data as it moves, and respond with speed and precision without holding back business innovation. worldwide security experts, IBM is trusted by thousands of organizations as their partner to assess, strategize, implement, and manage security transformations. IBM operates one of the world's broadest security research, development, and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide.

About IBM

IBM is a leading global hybrid cloud and AI, and business services provider. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. Nearly 3,000 government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and business services deliver open and flexible options to our clients. All of this is backed by IBM's legendary commitment to trust, transparency, responsibility, inclusivity and service.

Visit www.ibm.com for more information.

Media contact:
Gregor Hastings
External Relations, United Kingdom and Ireland, IBM

Email: gregor.hastings@ibm.com

---

https://uk.newsroom.ibm.com/2023-02-22-IBM-Report-Vulnerable-UK-energy-system-among-top-targets-for-cybercriminals-as-businesses-face-growing-extortion-threat