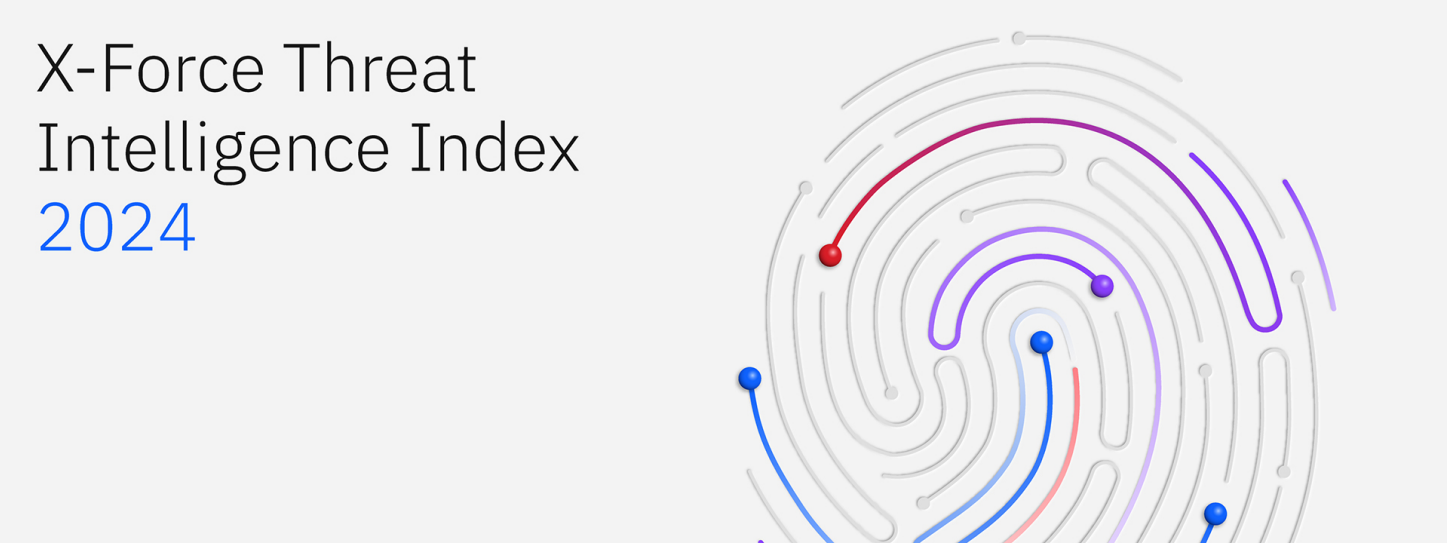
IBM UK Newsroom

IBM Report: Cybercriminals Intensify Attacks on User Identities in the UK, Complicating Recovery Efforts for Enterprises

• In 2023, 50% of UK cyberattacks used valid accounts as to gain initial entry

• Europe was the most targeted region globally in 2023, accounting for 32% of incidents reported, rising from second place in 2022

• The UK was the most targeted country in Europe, experiencing 27% of attacks



LONDON, UK, Feb 21, 2024 – IBM today released the 2024 X-Force Threat Intelligence Index highlighting an emerging global crisis as cybercriminals double down on exploiting user identities to compromise enterprises.

According to IBM X-Force, IBM Consulting's security services arm, cybercriminals last year generated more opportunities to "log in" to corporate networks through valid accounts, instead of hacking into them – making this tactic a preferred weapon of choice for threat actors.

The X-Force Threat Intelligence Index is based on insights and observations from monitoring over 150 billion security events per day in more than 130 countries. In addition, data is gathered and analysed from multiple sources within IBM, including IBM X-Force Threat Intelligence, Incident Response, X-Force Red, IBM Managed Security Services, and data provided from Red Hat Insights and Intezer , which contributed to the 2024 report.

An emerging identity crisis

The report data revealed that exploiting valid accounts has become the path of least resistance for cybercriminals, with billions of compromised credentials accessible on the Dark Web.

According to the report, 50% of cyberattacks in the UK involved the exploitation of valid accounts as the 'initial access vector' and a further 25% of cases involved the exploitation of public-facing applications. Across Europe, X-Force observed a 66% year-on-year rise in attacks caused by the use of valid accounts – contributing to

Europe's prevalence as the most targeted region of 2023 and the record number of attacks that X-Force has ever reported regionally.

The criminal ecosystem was also quick to adapt to the use of valid accounts by attackers. In 2023, X-Force observed a 266% increase in infostealing malware, which is designed to steal personal and enterprise credentials, personally identifiable information, and banking and crypto wallet information.

This "easy entry" for attackers is harder to detect, eliciting a costly response from enterprises. According to X-Force, worldwide, major incidents caused by attackers using valid accounts were linked to nearly 200% more complex response measures by security teams than the average incident – with defenders needing to distinguish between legitimate and malicious user activity on the network.

In fact, IBM's 2023 Cost of a Data Breach Report found that breaches caused by stolen or compromised credentials required roughly 11 months from detection to recovery – the longest response lifecycle among all infection vectors.

Martin Borrett, Technical Director, IBM Security, UK, and Ireland (UKI) commented:

"Our findings reveal that identity is increasingly being weaponised against enterprises, exploiting valid accounts and compromising credentials. It also shows us that the biggest security concern for enterprises stems not from novel or cryptic threats, but from well-known and existing ones.

"Addressing cybersecurity challenges requires a strategic approach, emphasising the reinforcement of foundational security measures. Streamlining identity management through a unified Identity and Access Management (IAM) provider and strengthening legacy applications with modern security protocols are crucial steps in mitigating risks. Additionally, subjecting your system to rigorous stress tests by skilled offensive security teams proves invaluable in uncovering potential weaknesses. This insight is pivotal for crafting a robust incident response plan that engages all teams, from IT professionals to C-suite executives."

Julian David, CEO of techUK, added:

"In an era marked by the growing sophistication of cybercriminals who exploit legitimate accounts to breach business defences, IBM's X-Force Threat Intelligence Index serves as a stark wake-up call.

"The report underscores a troubling pattern where half of the cyberattacks in the UK rely on legitimate accounts for initial access, presenting significant challenges to businesses' recovery endeavours. To effectively combat this threat, businesses must adopt a strategic approach, integrating modern security protocols to mitigate risks and strengthen their defences against the ever-evolving landscape of cyber threats."

Further key UK findings include:

Malware made up 30% of security incidents observed in the UK.

- Ransomware (30%) and cryptominers (20%) were the top malware types encountered in the country.

- The impact of attacks was evenly distributed with extortion, digital currency mining and data leaks each making up 25% of total impacts in the UK.
- This marks a shift from 2022, when half the cases X-Force observed in the UK involved extortion (57%) – twice the global average – followed by data theft (29%).

The professional, business and consumer services industry was the most targeted sector in the UK, representing 39% of cases.

- Energy (30%) and finance & insurance (17%) were the second and third most targeted industries in UK, respectively.
- Manufacturing was the most targeted industry in Europe, accounting for 28% of cases.
- Europe overall experienced the highest percentage of incidents within the energy sector at 43%, as well as finance and insurance at 37%.

Major takeaways from the global report included*:*

Attacks on critical infrastructure reveal industry "faux pas."

- Worldwide, an alarming 69.6% of attacks that X-Force responded to were against critical infrastructure organisations, an alarming finding highlighting that cybercriminals are wagering on these high value targets' need for uptime to advance their objectives.
- In 84% of attacks on critical sectors globally, compromise could have been mitigated with patching, multi-factor authentication, or least-privilege principals – indicating that what the security industry historically described as "basic security" may be harder to achieve than portrayed.
- Exploiting public-facing applications, phishing emails, and the use of valid accounts were top causes of attacks on this sector. The latter poses an increased risk to the sector, with DHS CISA stating that the majority of successful attacks on government agencies, critical infrastructure organisations and state-level government bodies in 2022 involved the use of valid accounts. This highlights the need for these organisations to frequently stress test their environments for potential exposures and develop incident response plans.

ROI from attacks on generative AI not there - yet.

- X-Force analysis projects that when a single generative AI technology approaches 50% market share or when the market consolidates to three or less technologies, it could trigger at-scale attacks against these platforms.
- X-Force assesses that once generative AI market dominance is established, the maturity of AI as an attack surface will be triggered, mobilising further investment in new tools from cybercriminals.
- Although generative AI is currently in its pre-mass market stage, it's paramount that enterprises secure their AI models before cybercriminals scale their activity.
- Enterprises should also recognise that their existing underlying infrastructure is a gateway to their AI models that doesn't require novel tactics from attackers to target – highlighting the need for a holistic approach to security in the age of generative AI, as outlined in the IBM Framework for Securing Generative AI.

Based on the research, IBM X-Force produced the following recommendations for enterprises:

- **Reduce blast radius** – Organisations should consider implementing solutions to reduce the damage that a data security incident could potentially cause by reducing the incident's blast radius - namely the potential impact of an incident given the compromise of particular users, devices or data. This could include implementing a least privileged framework, network segmentation and an identity fabric that extends modern security and detection and response capabilities to outdated applications and system.

- **Stress-test your environments and have a plan** – Hire hackers to stress test your environment and identify the existing cracks that cybercriminals could exploit to gain access to your network and carry out attacks. Also having incident response plans that are customised for your environment is key to reducing the time to respond, remediate and recover from an attack. Those plans should be regularly drilled and include a cross-organisational response, incorporate stakeholders outside of IT and test lines of communication between technical teams and senior leadership.

- **Adopt AI securely** – Organisations should focus on the following key tenets to secure their AI adoption: secure the AI underlying training data, secure the models and secure the use and inferencing of the models. It's paramount to also secure the broader infrastructure surrounding AI models. IBM recently introduced a comprehensive Framework for Securing Generative AI to help organisations prioritise defenses best on highest risk and potential impact.

Additional Resources

- Download a copy of **the 2024 X-Force Threat Intelligence Index**.
- Sign up for the **2024 IBM X-Force Threat Intelligence webinar** on Thursday, March 21st at 09:00 am ET.
- Connect with the **IBM X-Force team** for a personalised review of the findings.

Media Contact

Imtiaz Mufti
IBM External Communications
Imtiaz.mufti@ibm.com
Tele: +44 (0)772 1211 048
