IBM Newsroom

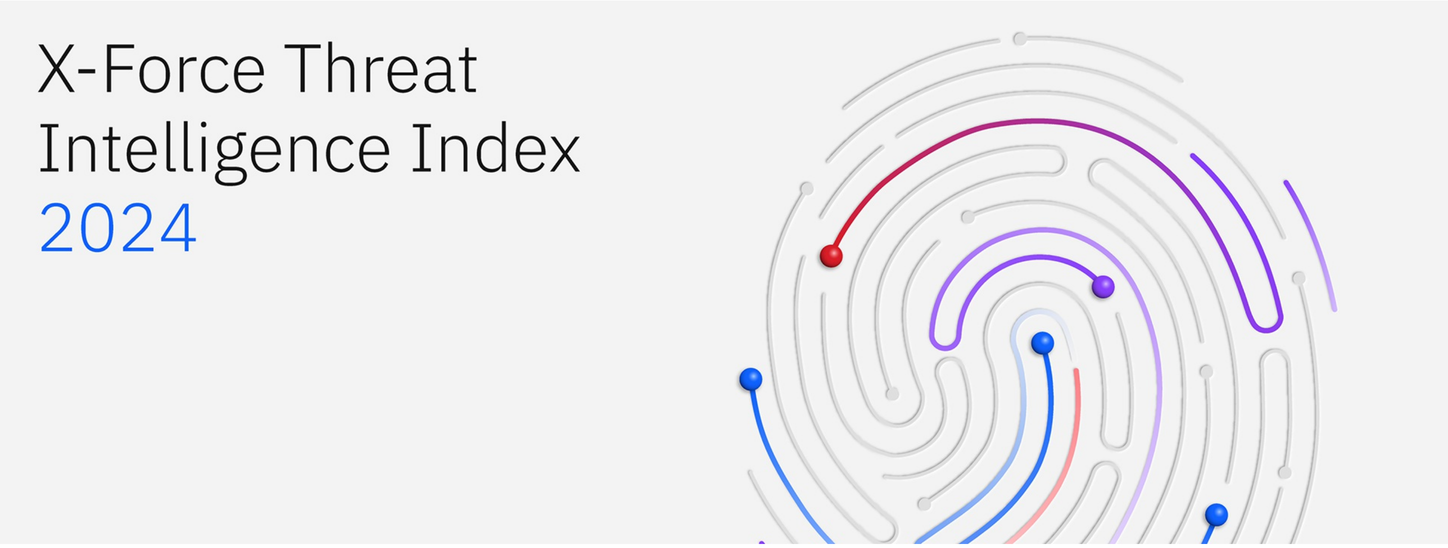
IBM Report: Identity Comes Under Attack, Straining Enterprises' Recovery Time from Breaches

-71% spike in cyberattacks caused by exploiting identity

- 50% AI market share milestone to trigger a cyber problem

- Nearly 70% of attacks globally targeted critical infrastructure in 2023

- Europe feels brunt of cyberattacks, making up 32% of global incidents



CAMBRIDGE, Mass., Feb. 21, 2024 /PRNewswire/ -- IBM (NYSE: IBM) today released the 2024 X-Force Threat Intelligence Index highlighting an emerging global identity crisis as cybercriminals double down on exploiting user identities to compromise enterprises worldwide. According to IBM X-Force, IBM Consulting's offensive and defensive security services arm, in 2023, cybercriminals saw more opportunities to "log in" versus hack into corporate networks through valid accounts – 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 analyzed 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.

Some of the key highlights include:

- **Attacks on critical infrastructure reveal industry "faux pas."** In nearly 85% of attacks on critical sectors, 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.
- **Ransomware groups pivot to leaner business model.** Ransomware attacks on enterprises saw a nearly 12% drop last year, as larger organizations opt against paying and decrypting, in favor of rebuilding

their infrastructure. With this growing pushback likely to impact adversaries' revenue expectations from encryption-based extortion, groups that previously specialized in ransomware were observed pivoting to infostealers.

- **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.

"While 'security fundamentals' doesn't get as many head turns as 'AI-engineered attacks,' it remains that enterprises' biggest security problem boils down to the basic and known – not the novel and unknown" said Charles Henderson, Global Managing Partner, IBM Consulting, and Head of IBM X-Force. "Identity is being used against enterprises time and time again, a problem that will worsen as adversaries invest in AI to optimize the tactic."

A Global Identity Crisis Poised to Worsen

Exploiting valid accounts has become the path of least resistance for cybercriminals, with billions of compromised credentials accessible on the Dark Web today. In 2023, X-Force saw attackers increasingly invest in operations to obtain users' identities – with a 266% uptick in infostealing malware, designed to steal personal identifiable information like emails, social media and messaging app credentials, banking details, crypto wallet data and more.

This "easy entry" for attackers is one that's harder to detect, eliciting a costly response from enterprises. According to X-Force, major incidents caused by attackers using valid accounts were associated 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 to detect and recover from – the longest response lifecycle than any other infection vector.

This wide reach into users' online activity was evident in the FBI and European law enforcement's April 2023 takedown of a global cybercrime forum that collected the login details of more than 80 million user accounts. Identity-based threats will likely continue to grow as adversaries leverage generative AI to optimize their attacks. Already in 2023, X-Force observed over 800,000 posts on AI and GPT across Dark Web forums, reaffirming these innovations have caught cybercriminals attention and interest.

Adversaries "Log into" Critical Infrastructure Networks

Worldwide, nearly 70% of attacks that X-Force responded to were against critical infrastructure organizations, an alarming finding highlighting that cybercriminals are wagering on these high value targets' need for uptime to advance their objectives.

Nearly 85% of attacks that X-Force responded to on this sector were caused by exploiting public-facing applications, phishing emails, and the use of valid accounts. The latter poses an increased risk to the sector, with DHS CISA stating that the majority of successful attacks on government agencies, critical infrastructure organizations and state-level government bodies in 2022 involved the use of valid accounts. This highlights the need for these organizations to frequently stress test their environments for potential exposures and develop incident response plans.

Generative AI – The Next Big Frontier to Secure

For cybercriminals to see ROI from their campaigns, the technologies they target must be ubiquitous across most organizations worldwide. Just as past technological enablers fostered cybercriminal activities – as observed with ransomware and Windows Server's market dominance, BEC scams and Microsoft 365 dominance or cryptojacking and the Infrastructure-as-a-Service market consolidation – this pattern will most likely extend across AI.

X-Force assesses that once generative AI market dominance is established – where a single technology approaches 50% market share or when the market consolidates to three or less technologies – it could trigger the maturity of AI as an attack surface, mobilizing 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 recognize 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.

Additional findings:

- **Europe – adversaries' preferred target** -- Nearly one in three attacks observed worldwide targeted Europe, with the region also experiencing the most ransomware attacks globally (26%).
- **Where did all the phish go?** Despite remaining a top infection vector, phishing attacks saw a 44% decrease in volume from 2022. But with AI poised to optimize this attack and X-Force research indicating that AI can speed up attacks by nearly two days, the infection vector will remain a preferred choice for cybercriminals.
- **Everyone is vulnerable** – Red Hat Insights found that 92% of customers have at least one CVE with known exploits unaddressed in their environment at the time of scanning, while 80% of the top ten vulnerabilities detected across systems in 2023 were given a 'High' or 'Critical' CVSS base severity score.
- **"Kerberoasting" pays off** – X-Force observed a 100% increase in "kerberoasting" attacks, wherein attackers attempt to impersonate users to escalate privileges by abusing Microsoft Active Directory tickets.
- **Security misconfigurations –** X-Force Red penetration testing engagements indicate that security misconfigurations accounted for 30% of total exposures identified, observing more than 140 ways that attackers can exploit misconfigurations.

Additional Resources

- Download a copy of **the 2024 X-Force Threat Intelligence Index**.
- Read more about the report's top findings in this **IBM Security Intelligence** blog.
- Sign up for the **2024 IBM X-Force Threat Intelligence webinar** on Thursday, March 7th at 11:00 am ET.
- Connect with the **IBM X-Force team** for a personalized review of the findings.

Media Contact

Georgia Prassinos
IBM
gprassinos@ibm.com

SOURCE IBM

Additional assets available online: Photos (

https://newsroom.ibm.com/2024-02-21-IBM-Report-Identity-Comes-Under-Attack,-Straining-Enterprises-Recovery-Time-from-Breaches