IBM Newsroom - Middle East & Africa

IBM Report: Ransomware Persisted Despite Improved Detection in 2022

Finance and Insurance Most-Targeted Industry in MEA; Email Thread Hijacking Attempts Spike; Time to Ransom Moves from Months to Days

Dubai, UAE, March 20, 2023 -- IBM Security released its annual **X-Force Threat Intelligence Index** finding that although ransomware's share of incidents in the Middle East and Africa (MEA) held steady at 18%, globally defenders were more successful detecting and preventing ransomware. Despite this, attackers continued to innovate, with the report showing that globally the average time to complete a ransomware attack dropped from two months down to less than 4 days.

According to the 2023 report, the deployment of backdoors, which allow remote access to systems, emerged as the top action by attackers in the MEA region last year. Backdoor deployments were detected in 27% of the cases X-Force responded to in this region in 2022. Ransomware and worms tied for the second-most common attack type in the region at 18% each. The uptick in backdoor deployments can be partially attributed to their high market value. 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.

As organizations across the MEA region try to address the ever-evolving cyber threats landscape, Frida Kleimert Knibbs, Security Leader at IBM MEA, stressed the critical role of threat intelligence in safeguarding against these threats. She commented: “Proactively managing security risks and evolving cybercrime tactics is a critical priority for organizations across MEA. The X-Force Threat Intelligence Index findings demonstrate the continued threat of ransomware and the increasing use of thread hijacking tactics.”

She added: “To safeguard against these threats, it's imperative that companies remain vigilant and focus on effective incident response planning. As the security landscape evolves, it is crucial to prioritize threat intelligence and strengthen defenses”.

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.

Some of the key findings in the 2023 report include:

- **Extortion: Threat Actors Go-to Method**. The most common impact from cyberattacks in 2022 was extortion, which was primarily achieved through ransomware or business email compromise attacks. Extortion and financial loss each accounted for half of identified impacts in incidents across the MEA region in 2021. Manufacturing was the most extorted industry globally in 2022, and it was again the most attacked industry for the second consecutive year. Manufacturing organizations are an attractive target for extortion, given the extremely low tolerance for down time.
- **Cybercriminals Weaponize 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% globally compared to 2021 data. Over the year, X-Force found that attackers used this tactic to deliver Emotet, Qakbot, and IcedID, malicious software that often results in ransomware infections.
- **Legacy Exploits Still Doing the Job.** The proportion of known exploits relative to vulnerabilities declined 10 percentage points globally from 2018 to 2022, due to the fact that the number of vulnerabilities hit another all-time high. The findings indicate that legacy exploits enabled older malware infections such as WannaCry and Conficker to continue to exist and spread.
- **Phishers “Give Up” on Credit Card Data.** The number of cybercriminals targeting credit card information in phishing kits dropped 52% globally in one year, indicating that attackers are prioritizing personally identifiable information such as names, emails, and home addresses, which can be sold for a higher price on the dark web or used to conduct further operations.
- **Finance and Insurance Remain Prime Targets for Cyberattacks in MEA** : In the Middle East and Africa, Finance and insurance was the most-targeted industry in 2022, accounting for 44% of incidents and down slightly from 2021 at 48%. Professional, business and consumer services accounted for 22% of

attacks, with manufacturing and energy tying for third place at 11%.

The report features data IBM collected globally in 2022 to deliver insightful information about the global threat landscape and inform the security community about the threats most relevant to their organizations.

You can download a copy of the 2023 IBM Security X-Force Threat Intelligence Report here.

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.

---

https://mea.newsroom.ibm.com/x-force-intelligence-index-launch-MEA