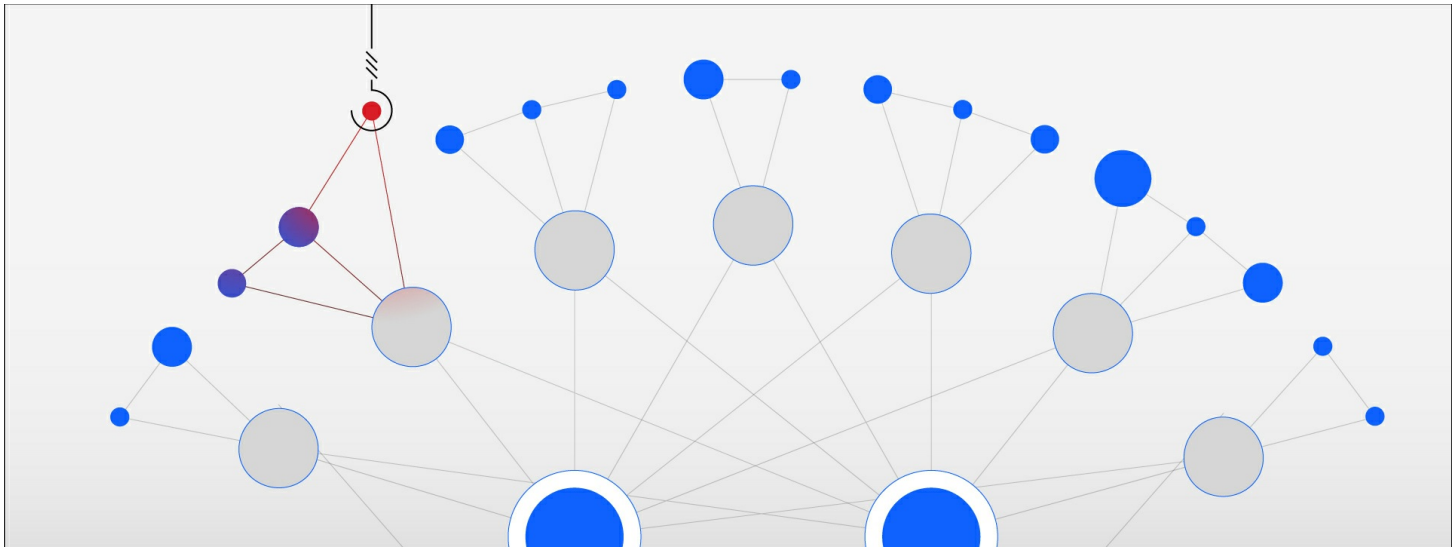
IBM Newsroom

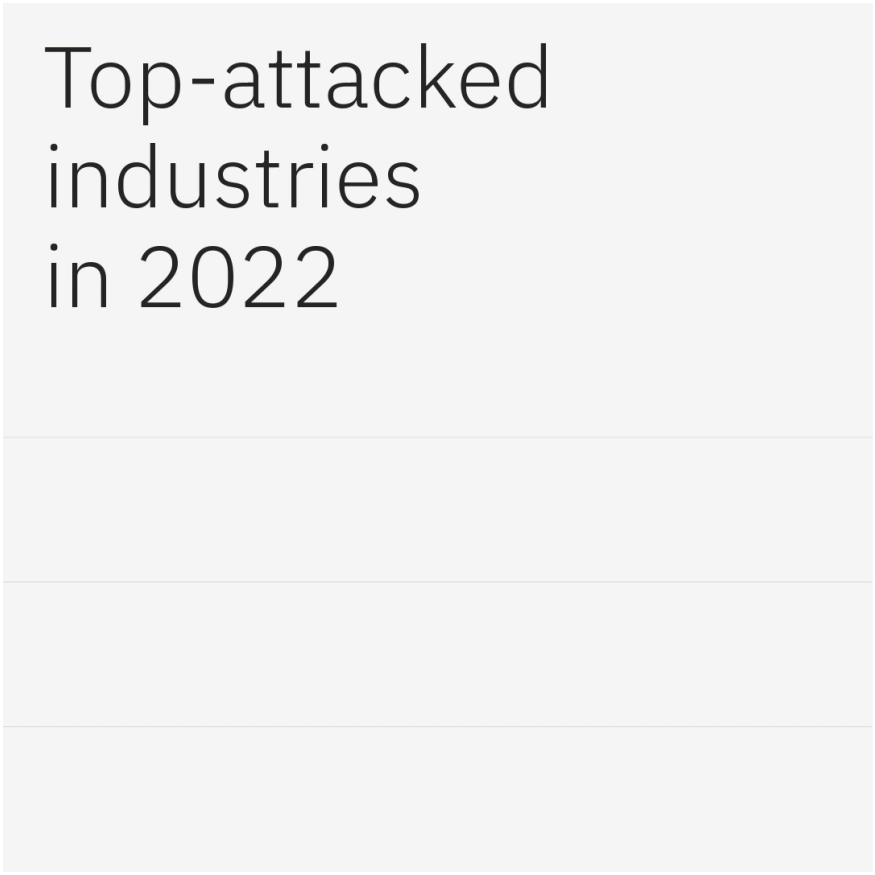
IBM Report: Ransomware Persisted Despite Improved Detection in 2022

Manufacturing Most Extorted Industry; Email Thread Hijacking Attempts Spike; Time to Ransom Moves from Months to Days



ARMONK, N.Y., Feb. 22, 2023 /PRNewswire/ -- IBM (NYSE:IBM) Security today released its annual X-Force Threat Intelligence Index finding that although ransomware's share of incidents declined only slightly (4 percentage points) from 2021 to 2022, defenders were more successful detecting and preventing ransomware. Despite this, attackers continued to innovate with the report showing the average time to complete a ransomware attack dropped from 2 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 last year. About 67% of those backdoor cases related to ransomware attempts, where defenders were able to detect the backdoor before ransomware was deployed. 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, compared to stolen credit card data, which can sell for less than $10 today.



"The shift towards detection and response has allowed defenders to disrupt adversaries earlier in the attack chain - tempering ransomware's progression in the short term," said Charles Henderson, Head of IBM Security X-Force. "But it's only a matter of time before today's backdoor problem becomes tomorrow's ransomware crisis. Attackers always find new ways to evade detection. Good defense is no longer enough. To break free from the never-ending rat race with attackers, businesses must drive a proactive, threat-driven security strategy."

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. Europe was the most targeted region for this method, representing 44% of extortion cases observed, as threat actors sought to exploit geopolitical tensions.
- **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% 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 fact that the number of vulnerabilities hit 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.

Extortion Pressure Applied (Unevenly)
Cybercriminals often target the most vulnerable industries, businesses, and regions with extortion schemes, applying high

psychological pressure to force victims to pay. Manufacturing was the most extorted industry in 2022, and it was the most attacked industry for the second consecutive year. Manufacturing organizations are an attractive target for extortion, given their extremely low tolerance for down time.

Ransomware is a well-known method of extortion, but threat actors are always exploring new ways to extort victims. One of the latest tactics involves making stolen data more accessible to downstream victims. By bringing customers and business partners into the mix, operators increase pressure on the breached organization. Threat actors will continue experimenting with downstream victim notifications to increase the potential costs and psychological impact of an intrusion – making it critical that businesses have a customized incident response plan that also considers the impact of an attack on downstream victims.

Thread Hijacking on the Rise

Email thread hijacking activity surged last year, with monthly attempts by threat actors doubling 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.

With phishing being the leading cause of cyberattacks last year, and thread hijacking's sharp rise, it's clear that attackers are exploiting the trust placed in email. Businesses should make employees aware of thread hijacking to help reduce the risk of them falling victim.

Mind the Gap: Exploit "R&D" Lagging Vulnerabilities

The ratio of known exploits to vulnerabilities has been declining over the last few years, down 10 percentage points since 2018. Cybercriminals already have access to more than 78,000 known exploits, making it easier to exploit older, unpatched vulnerabilities. Even after 5 years, vulnerabilities leading to WannaCry infections remain a significant threat. X-Force recently reported an 800% increase in WannaCry ransomware traffic within MSS telemetry data sinceApril 2022. The continued use of older exploits highlights the need for organizations to refine and mature vulnerability management programs, including better understanding their attack surface and risk-based prioritization of patches.

Additional findings from the 2023 report include:

- **Phishers "Give Up" on Credit Card Data.** The number of cybercriminals targeting credit card information in phishing kits dropped 52% 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.
- **North America Felt Brunt of Energy Attacks.** Energy held its spot as the 4th most attacked industry last year, as global forces continue to affect an already tumultuous global energy trade. North American energy organizations accounted for 46% of all energy attacks observed last year, a 25% increase from 2021 levels.
- **Asia Tops the Target List.** Accounting for nearly one-third of all attacks that X-Force responded to in 2022,Asia saw more cyberattacks than any other region. Manufacturing accounted for nearly half of all cases observed in Asia last year.

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.

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.
- 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.

Press Contact:
IBM Security Communications
Michele Brancati
mbrancati@ibm.com

SOURCE IBM

Additional assets available online:

https://stage.mediaroom.com/ibmnewsroom/2023-02-22-IBM-Report-Ransomware-Persisted-Despite-Improved-Detection-in-2022