IBM Newsroom

IBM Report: Manufacturing Felt Brunt of Cyberattacks in 2021 as Supply Chain Woes Grew

Other Findings: Asia Pacific Now Most Attacked Region; Average Lifespan of Ransomware Groups is 17 Months; Vishing Triples Phishing Click Rate

CAMBRIDGE, Mass., Feb. 23, 2022 /PRNewswire/ -- IBM (NYSE: IBM) Security today released its annual X-Force Threat Intelligence Index unveiling how ransomware and vulnerability exploitations together were able to "imprison" businesses in 2021 further burdening global supply chains, with manufacturing emerging as the most targeted industry. While phishing was the most common cause of cyberattacks in general in the past year, IBM Security X-Force observed a 33% increase in attacks caused by vulnerability exploitation of unpatched software, a point of entry that ransomware actors relied on more than any other to carry out their attacks in 2021, representing the cause of 44% of ransomware attacks.

The 2022 report details how in 2021 ransomware actors attempted to "fracture" the backbone of global supply chains with attacks on manufacturing, which became 2021's most attacked industry (23%), dethroning financial services and insurance after a long reign. Experiencing more ransomware attacks than any other industry, attackers wagered on the ripple effect that disruption on manufacturing organizations would cause their downstream supply chains to pressure them into paying the ransom. An alarming 47% of attacks on manufacturing were caused due to vulnerabilities that victim organizations had not yet or could not patch, highlighting the need for organizations to prioritize vulnerability management.

The 2022 IBM Security X-Force Threat Intelligence Index maps new trends and attack patterns IBM Security observed and analyzed from its data – drawing from billions of datapoints ranging from network and endpoint detection devices, incident response engagements, phishing kit tracking and more – including data provided by Intezer.

Your browser does not support the video tag.

Some of the top highlights in this year's report include:

- **Ransomware Gangs Defy Takedowns.** Ransomware persisted as the top attack method observed in 2021, with ransomware groups showing no sign of stopping, despite the uptick in ransomware takedowns. According to the 2022 report, the average lifespan of a ransomware group before shutting down or rebranding is 17 months.

- **Vulnerabilities Expose Businesses' Biggest "Vice".** X-Force reveals that for businesses in Europe, Asia and MEA, unpatched vulnerabilities caused approximately 50% of attacks in 2021, exposing businesses' biggest struggle– patching vulnerabilities.
- **Early Warning Signs of Cyber Crisis in the Cloud.** Cybercriminals are laying the groundwork to target cloud environments, with the 2022 report revealing a 146% increase in new Linux ransomware code and a shift to Docker-focused targeting, potentially making it easier for more threat actors to leverage cloud environments for malicious purposes.

"Cybercriminals usually chase the money. Now with ransomware they are chasing leverage," said Charles Henderson, Head of IBM X-Force. "Businesses should recognize that vulnerabilities are holding them in a deadlock – as ransomware actors use that to their advantage. This is a non-binary challenge. The attack surface is only growing larger, so instead of operating under the assumption that every vulnerability in their environment has been patched, businesses should operate under an assumption of compromise, and enhance their vulnerability management with a zero trust strategy."

The "Nine Lives" of Ransomware Groups

Responding to the recent acceleration of ransomware takedowns by law enforcement, ransomware groups may be activating their own disaster recovery plans. X-Force's analysis reveals that the average lifespan of a ransomware group before shutting down or rebranding is 17 months. For example, REvil which was responsible for 37% of all ransomware attacks in 2021, persisted for four years through rebranding, suggesting the likelihood it resurfaces again despite its takedown by a multi-government operation in mid 2021.

While law enforcement takedowns can slow down ransomware attackers, they are also burdening them with the expenses required to fund their rebranding or rebuild their infrastructure. As the playing field changes, it's important that organizations modernize their infrastructure to place their data in an environment that can help safeguard it – whether that be on-premises or in clouds. This can help businesses manage, control, and protect their workloads, and remove threat actors' leverage in the event of a compromise by making it harder to access critical data in hybrid cloud environments.

Vulnerabilities Become an Existential Crisis for Some

The X-Force report highlights the record high number of vulnerabilities disclosed in 2021, with vulnerabilities in Industrial Control Systems rising by 50% year-over-year. Although more than 146,000 vulnerabilities have been disclosed in the past decade, it's only been in recent years that organizations accelerated their digital journey, largely driven by the pandemic, suggesting that the vulnerability management challenge has yet to reach its peak.

At the same time, vulnerability exploitation as an attack method is growing more popular. X-Force observed a 33% increase since the previous year, with the two most exploited vulnerabilities observed in 2021 found in widely used enterprise applications (Microsoft Exchange, Apache Log4J Library). Enterprises' challenge to manage vulnerabilities may continue to exacerbate as digital infrastructures expand and businesses can grow overwhelmed with audit and upkeep requirements, highlighting the importance of operating on the assumption of compromise and applying a zero trust strategy to help protect their architecture.

Attackers Target Common Grounds Amongst Clouds

In 2021, X-Force observed more attackers shifting their targeting to containers like Docker – by far the most dominant container runtime engine according to RedHat. Attackers recognize that containers are common grounds amongst organizations so they are doubling down on ways to maximize their ROI with malware that can cross platforms and can be used as a jumping off point to other components of their victims' infrastructure.

The 2022 report also sounds caution on threat actors' continued investment into unique, previously unobserved, Linux malware, with data provided by Intezer revealing a 146% increase in Linux ransomware that has new code. As attackers remain steady in their pursuit of ways to scale operations through cloud environments, businesses must focus on extending visibility into their hybrid infrastructure. Hybrid cloud environments that are built on interoperability and open standards can help organizations detect blind spots and accelerate and automate security responses.

Additional findings from the 2022 report include:

- **Asia Leads Attacks –** Experiencing over 1 in 4 attacks that IBM observed globally in 2021,Asia saw more cyberattacks than any other region in the past year. Financial services and manufacturing organizations together experienced nearly 60% of attacks in Asia.
- **First Time Caller, Long Time Phisher –** Phishing was the most common cause of cyberattacks in 2021. In X-Force Red's penetration tests, the click rate in its phishing campaigns tripled when combined with phone calls.

The report features data IBM collected globally in 2021 to deliver insightful information about the global threat landscape and inform security professionals about the threats most relevant to their organizations. You can download a copy of the 2022 IBM Security X-Force Threat Intelligence Index here.

Additional Sources

- Sign up for the 2022 IBM Security X-Force Threat Intelligence Index webinar onThursday, March 3, 2022, at 11:00 a.m. ET here.
- Read a blog post from the report authors to learn more about three of the report's top findings, on the IBM Security Intelligence blog.

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force research, enables organizations to effectively manage risk and defend against emerging threats. 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. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Press Contact
Georgia Prassinos
IBM Security Media Relations
gprassinos@ibm.com

SOURCE IBM

Additional assets available online:

https://stage.mediaroom.com/ibmnewsroom/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew