IBM Newsroom

IBM Security Report: Attacks on Industries Supporting COVID-19 Response Efforts Double

Ransomware Group Banks Millions; Cloudy Forecast Amid 40% Rise in Open-Source Malware in 2020; Social Distancing "Must Have" Tools Dominate Top Spoofed Brands

CAMBRIDGE, Mass., Feb. 24, 2021 /PRNewswire/ -- IBM (NYSE: IBM) Security today released the 2021 X-Force Threat Intelligence Index highlighting how cyberattacks evolved in 2020 as threat actors sought to profit from the unprecedented socioeconomic, business and political challenges brought on by the COVID-19 pandemic. In 2020, IBM Security X-Force observed attackers pivoting their attacks to businesses for which global COVID-19 response efforts heavily relied, such as hospitals, medical and pharmaceutical manufacturers, as well as energy companies powering the COVID-19 supply chain.

According to the new report, cyberattacks on healthcare, manufacturing, and energy doubled from the year prior, with threat actors targeting organizations that could not afford downtime due to risks of disrupting medical efforts or critical supply chains. In fact, manufacturing and energy were the most attacked industries in 2020, second only to the finance and insurance sector. Contributing to this was attackers taking advantage of the nearly 50% increase in vulnerabilities in industrial control systems (ICS), which manufacturing and energy both strongly depend on.

"In essence, the pandemic reshaped what is considered critical infrastructure today, and attackers took note. Many organizations were pushed to the front lines of response efforts for the first time – whether to support COVID-19 research, uphold vaccine and food supply chains, or produce personal protective equipment," said Nick Rossmann, Global Threat Intelligence Lead, IBM Security X-Force. "Attackers' victimology shifted as the COVID-19 timeline of events unfolded, indicating yet again, the adaptability, resourcefulness and persistence of cyber adversaries."

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 Security X-Force Threat Intelligence and Incident Response, X-Force Red, IBM Managed Security Services, and data provided by Quad9 and Intezer, both of which contributed to the 2021 report.

Some of the report's key highlights include:

- **Cybercriminals Accelerate Use of Linux Malware** – With a 40% increase in Linux-related malware families in the past year, according to Intezer, and a 500% increase in Go-written malware in the first six months of 2020, attackers are accelerating a migration to Linux malware, that can more easily run on various platforms, including cloud environments.

- **Pandemic Drives Top Spoofed Brands –** Amid a year of social distancing and remote work, brands offering collaboration tools such as Google, Dropbox and Microsoft, or online shopping brands such as Amazon and PayPal, made the top 10 spoofed brands in 2020. YouTube and Facebook, which consumers relied on more for news digestion last year, also topped the list. Surprisingly, making an inaugural debut as

the seventh most commonly impersonated brand in 2020 was Adidas, likely driven by demand for the Yeezy and Superstar sneaker lines.

- **Ransomware Groups Cash In On Profitable Business Model –** Ransomware was the cause of nearly one in four attacks that X-Force responded to in 2020, with attacks aggressively evolving to include double extortion tactics. Using this model, X-Force assesses Sodinokibi – the most commonly observed ransomware group in 2020 – had a very profitable year. X-Force estimates that the group made a conservative estimate of over $123 million in the past year, with approximately two-thirds of its victims paying a ransom, according to the report.

Investment in Open-Source Malware Threatens Cloud Environments

Amid the COVID-19 pandemic, many businesses sought to accelerate their cloud adoption. "In fact, a recent Gartner survey found that almost 70% of organizations using cloud services today plan to increase their cloud spending in the wake of the disruption caused by COVID-19." [1] But with Linux currently powering 90% of cloud workloads and the X-Force report detailing a 500% increase in Linux-related malware families in the past decade, cloud environments can become a prime attack vector for threat actors.

With the rise in open-source malware, IBM assesses that attackers may be looking for ways to improve their profit margins – possibly reducing costs, increasing effectiveness and creating opportunities to scale more profitable attacks. The report highlights various threat groups such as APT28, APT29 and Carbanak turning to open-source malware, indicating that this trend will be an accelerator for more cloud attacks in the coming year.

The report also suggests that attackers are exploiting the expandable processing power that cloud environments provide, passing along heavy cloud usage charges on victim organizations, as Intezer observed more than 13% new, previously unobserved code in Linux cryptomining malware in 2020.

With attackers' sights set on clouds, X-Force recommends that organizations should consider a zero-trust approach to their security strategy. Businesses should also make confidential computing a core component of their security infrastructure to help protect their most sensitive data – by encrypting data in use, organizations can help reduce the risk of exploitability from a malicious actor, even if they're able to access their sensitive environments.

Cybercriminals Disguised as Celebrity Brand

The 2021 report highlights that cybercriminals opted to disguise themselves most often as brands that consumers trust. Considered one of the most influential brands in the world, Adidas appeared attractive to cybercriminals attempting to exploit consumer demand to drive those looking for coveted sneakers to malicious websites designed to look like legitimate sites. Once a user visited these legitimate-looking domains, cybercriminals would either seek to carry out online payment scams, steal users' financial information, harvest user credentials, or infect victims' devices with malware.

The report indicates that the majority of Adidas spoofing is associated with the Yeezy and Superstar sneaker lines. The Yeezy line alone reportedly pulled in $1.3 billion in 2019 and was one of the top selling sneakers for the sportswear manufacturing giant. It's likely that, with the hype for the next sneaker release in early 2020, attackers leveraged the demand of the money-making brand to make their own profit.

Ransomware Dominates 2020 as Most Common Attack

According to the report, in 2020 the world experienced more ransomware attacks compared to 2019, with nearly 60% of ransomware attacks that X-Force responded to using a double extortion strategy whereby attackers encrypted, stole and then threatened to leak data, if the ransom wasn't paid. In fact, in 2020, 36% of the data breaches that X-Force tracked came from ransomware attacks that also involved alleged data theft, suggesting that data breaches and ransomware attacks are beginning to collide.

The most active ransomware group reported in 2020 was Sodinokibi (also known as REvil), accounting for 22% of all ransomware incidents that X-Force observed. X-Force estimates that Sodinokibi stole approximately 21.6 terabytes of data from its victims, that nearly two-thirds of Sodinokibi victims paid ransom, and approximately 43% had their data leaked – which X-Force estimates resulted in the group making over $123 million in the past year.

Like Sodinokibi, the report found that the most successful ransomware groups in 2020 were focused on also stealing and leaking data, as well as creating ransomware-as-a-service cartels and outsourcing key aspects of their operations to cybercriminals that specialize in different aspects of an attack. In response to these more aggressive ransomware attacks, X-Force recommends that organizations limit access to sensitive data and protect highly privileged accounts with privileged access management (PAM) and identity and access management (IAM).

Additional key findings in the report include:

- **Vulnerabilities Surpass Phishing as Most Common Infection Vector** – The 2021 report reveals that the most successful way victim environments were accessed last year was scanning and exploiting for vulnerabilities (35%), surpassing phishing (31%) for the first time in years.
- **Europe Felt the Brunt of 2020 Attacks –** Accounting for 31% of attacks X-Force responded to in 2020, per the report, Europe experienced more attacks than any other region, with ransomware rising as the top culprit. In addition, Europe saw more insider threat attacks than any other region, seeing twice as many such attacks as North America and Asia combined.

The report features data IBM collected in 2020 to deliver insightful information about the global threat landscape and inform security professionals about the threats most relevant to their organizations. To download a copy of the X-Force Threat Intelligence Index 2021, please visit: https://www.ibm.biz/threatindex2021

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

[1] Gartner Press Release, *Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021*, 17 November 2020

SOURCE IBM

---

https://newsroom.ibm.com/2021-02-24-IBM-Security-Report-Attacks-on-Industries-Supporting-COVID-19-Response-Efforts-Double