Security Vulnerabilities

Biggest Ransomware Attacks of 2021: A Look Back at the Chart Toppers

Ransomware threats have increased exponentially over the last year. Here we look back at the top ransomware attacks of 2021 and focus on the cautionary steps that organizations, governments, and individuals can take to prevent an attack.

Ojasvi Nath
Assistant Editor, Spiceworks Ziff Davis

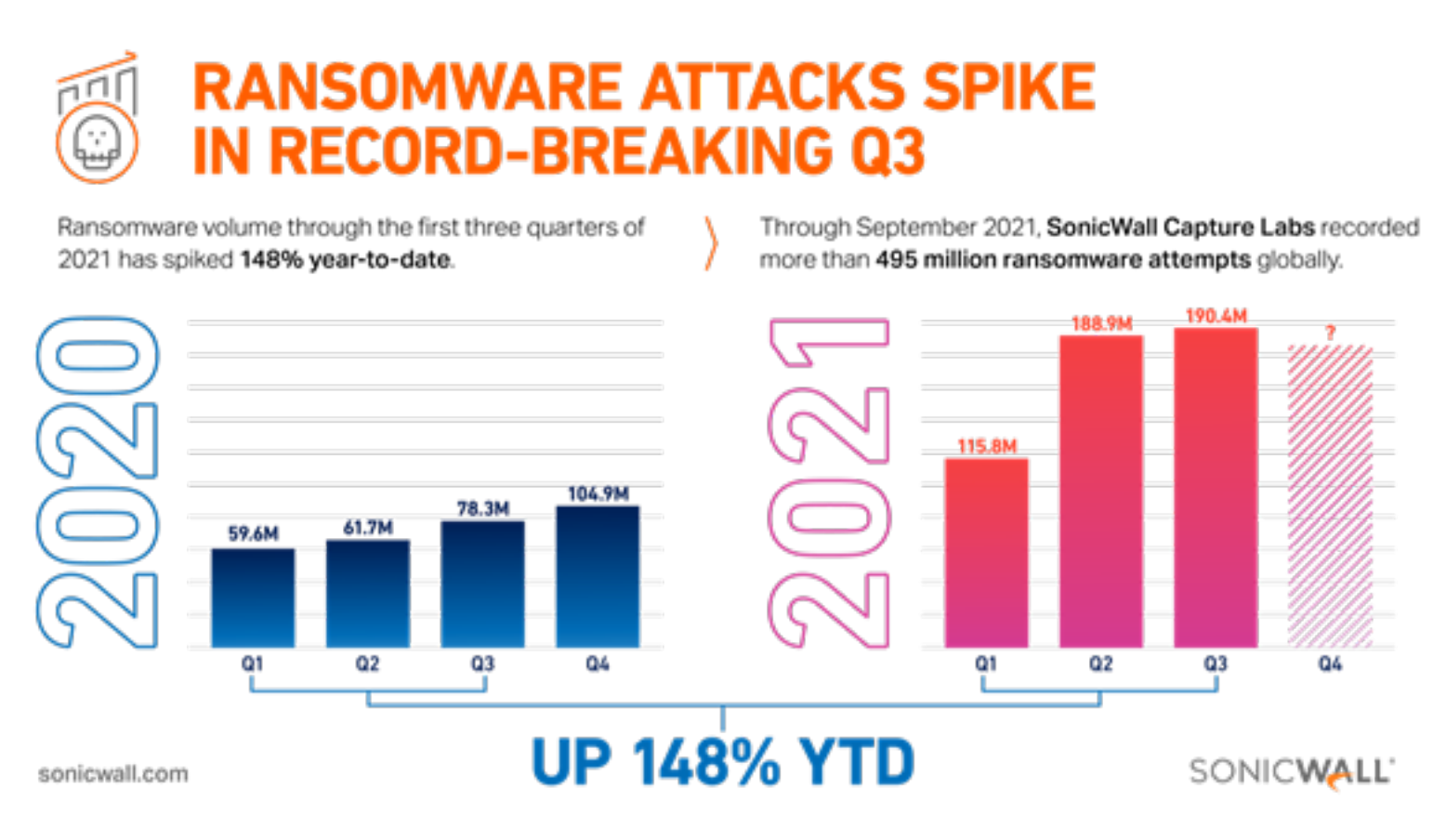
January 27, 2022

Popular
1 10 Cloud Security Trends That Will Shape 2022 and Beyond
2 Log4j Zero-Day Vulnerability: Everything You Need To Know About the Apache Flaw
3 Top 10 Cybersecurity Colleges in the U.S. in 2022

Last year was a watershed moment for the cybersecurity industry. According to a report by SonicWall, the number of ransomware attacks in the United States increased by 127% last year compared to 2020. Meanwhile, the U.K. identified a 233% surge in the attacks. The organizations and governments were unequivocally kept on their toes by several cyber threats originating from state actors and ransomware gangs. This article talks about the top ransomware attacks of 2021, what went wrong, and a few precautionary measures to be more prudent.

Organizations found themselves in a tangle last year as the number and severity of ransomware attacks soared significantly. 2021 is reckoned to be one of the costliest and most dangerous years for ransomware outbreaks, a recent report highlighted.

Approximately 500 million ransomware attacks were registered in nine months leading up to September 2021, with an average of 1,748 attempts per client. In the third quarter of 2021, 190.4 million ransomware attempts were reported, nearly surpassing the 195.7 million total ransomware attempts recorded in the first three quarters of 2020.



Ransomware attacks spike in Q3 2021; Source: SonicWall

"The techniques deployed by ransomware actors have evolved well beyond the smash-and-grab attacks from just a few years ago," said Dmitriy Ayrapetov, platform architecture vice president at security firm SonicWall. "Today's cybercriminals demonstrate deliberate reconnaissance, planning and execution to surgically deploy tool chains targeting enterprise and government infrastructure. This results in larger victims and leads to higher ransoms."

What is Ransomware?

Before we look at the top ransomware attacks of the previous year, let us quickly reiterate what ransomware is and how it operates.

Ransomware is a type of malware that encrypts the data of its victims. The intruder then demands a ransom from the victim, assuring that access to the data would be restored if the ransom is paid. Users are shown how to pay a charge to acquire the decryption key. The costs, which can vary from a few hundred dollars to thousands of dollars, are paid in Bitcoin to the hackers.

See More: A Midsize Company's Guide to Ransomware Protection

Top 5 Ransomware Attacks of 2021

Let us now look back at the biggest ransomware attacks of last year that caused significant damage to the prey organizations.

Colonial Pipeline

The ransomware onslaught on Colonial Pipeline in 2021 was set to be the most contentious of the year. Colonial Pipeline transports roughly half of the petroleum on the East Coast. The ransomware incident was the most significant hack on oil infrastructure in U.S. history. On May 7, 2021, the American pipeline company paid approximately $5 million to Eastern European hackers, defying rumors that the corporation had no obligation to pay a ransom price to facilitate the restoration of the country's major petroleum pipeline.

The company restored the pipeline to service by May 12, 2021, while the supply chain took a few days to function normally. The hackers, identified as DarkSide, infected the company's automated management equipment with ransomware. DarkSide hacked the password for an active VPN account that was no longer in use. Because Colonial Pipeline did not employ multi-factor authentication, hackers could access the firm's IT network and data more quickly.

JBS

Assuming May is the peak month for cybercriminals, JBS USA, a global meatpacker, also suffered a ransomware attack the same month. The company paid $11 million in Bitcoin to cybercriminals who used ransomware to lock corporate files and impair operations in the United States and Australia. The attack prompted the corporation to shut down its beef operations in the United States and reduce pork and poultry output. The hack wreaked havoc on the food supply chain, highlighting the manufacturing and agriculture industries' vulnerability to such disruptions.

Because of its cybersecurity policies, redundant systems, and encrypted backup servers, JBS stated it could promptly rectify the difficulties caused by the cyberattack. It claimed that it spends over $200 million on IT each year and employs over 850 IT specialists worldwide.

The attackers were revealed as the REvil ransomware-as-a-service operation by the FBI. The REvil gang is a ransomware (RaaS) company that sells encryption software to other criminal organizations.

Kaseya

Kaseya, a Florida-based software supplier that offers Remote Management Monitoring, issued a warning on July 2, 2021, about their product being used to install ransomware on end-customer systems. The attack was again carried out by the REvil ransomware gang that exploited two vulnerabilities in Kaseya software to hack into roughly 50 managed services providers (MSPs) that utilized the company's products.

Despite only 1% of Kaseya's clients being impacted, their MSP compromised an estimated 800 to 1500 small to mid-sized organizations. 800 Coop shops and a Swedish grocery chain were forced to close momentarily due to difficulty accessing their cash registers.

Ireland's HSE

The Health Services Executive (HSE), Ireland's state healthcare system, was struck by a ransomware attack in May 2021, which turned out to be exceedingly costly and impacted services for months. The hacker installed Conti ransomware on HSE systems on May 14, 2021. The organization activated its Critical Incident Process right away, shutting down all IT systems and isolating the National Healthcare Network from the internet.

The firm declined to pay the $20 million ransom in Bitcoin since the Conti ransomware gang provided the software decryption key for free. However, the early estimated costs were $600 million, including $120 million in recovery costs, replacement and upgrade fees for ransomware-affected systems, and charges to a third-party cybersecurity support team.

DC Police Department

The Metropolitan Police Department in Washington, D.C., released a statement in April. The Babuk gang, a Russian ransomware group, launched a ransomware attack on the department. The police unit declined to pay the group $4 million ransom in compensation for the agency's data not being leaked.

Internal information, including police officer disciplinary files and intelligence reports, was massively leaked due to the attack, resulting in a 250GB data breach. Experts claimed it was the most significant ransomware attack on a police agency in the United States.

See More: 3 Ways To Make Your Organization More Resilient to Ransomware Attacks

Precautionary Measures

Cybercrime, particularly ransomware, has been identified as a threat to the global economy by the World Economic Forum (WEF). The WEF has recommended a multi-stakeholder strategy in which organizations exchange information and conduct testing and training to avoid attacks. Following the Pipeline incident mentioned, the Cybersecurity and Infrastructure Security Agency (CISA) in the United States provided a set of ransomware-avoidance suggestions:

- Workers must log onto computers and networks using multi-factor authentication (MFA).
- Robust spam filters need to be in place to protect against phishing emails.
- Simulated phishing attempts to teach consumers about the dangers of ransomware.
- URL blocklists to filter internet traffic.
- All software is to be updated and patched regularly.
- Remote access to resources should be limited, and MFA should be required.
- Run antivirus and anti-malware checks regularly.
- Prevent illegal execution by limiting the apps and directories that can run programs and monitoring and blocking unexpected connections.

Conclusion

Ransomware attacks have become much more sophisticated and costly to enterprises. Cybercriminals now have access to additional tools, including the threat of exposing sensitive information. Many of them also provide tools to other criminals in exchange for a share of the ransom money. This kind of well-coordinated illegal behavior needs well-coordinated retaliation and vigilance. Organizations must become more conscientious about cybersecurity training, software patching and upgrades, and the implementation of proper cybersecurity technology to manage ransomware threats better in the years to come.

MORE ON RANSOMWARE:

- Ransomware: Is Your Sensitive Data Protected, or Will You Have To Pay Up?
- Why Immutable Backups Are Essential to Recovering from Ransomware Attacks
- What's Your Disaster Recovery Plan To Fight Ransomware Attack?
- How Have Ransomware Attacks Impacted Manufacturing Industry

Do you think that your organization is well-protected against ransomware attacks? Tell us what you think on LinkedIn, Twitter, or Facebook. We'd be thrilled to hear from you!

Bitcoin | Colonial Pipeline | Cyber Attacks | Ireland Hse | Jbs | Kaseya | Malware | Ransomware

Share This Article:

Ojasvi Nath
Assistant Editor, Spiceworks Ziff Davis

Ojasvi Nath is Assistant Editor for Toolbox and covers varied aspects of technology. With a demonstrated history of working as a business writer, she has now switched her interest to technology and handles a broad range of topics from cybersecurity, cloud, AI, emerging tech innovation to hardware. Being a philomath, Ojasvi thinks knowledge is like a Pierian spring. The more you dive in, the more you learn. You can reach out to her at ojasvi.nath@swzd.com

Join The Conversation

Recommended Reads

Security Vulnerabilities
Credential Stuffing: Five Key Strategies To Defend Against a Growing Threat

Security Vulnerabilities
An Ethical Hacker's Guide to External Attack Surface Management

Security Vulnerabilities
A Midsize Company's Guide to Ransomware Protection

Security Vulnerabilities
How Software Supply Chain Attacks Happen and How To Mitigate Them

Security Vulnerabilities
Why a Zero-Trust Model for Email Security Is Critical

Security Vulnerabilities
4 Reasons Why Multi-Factor Authentication Should Be Deployed Across the Enterprise