

CYBERSECURITY

Cybercriminals targeting MSPs as more attacks on supply chain expected in 2022



MSPs are having more of their own management tools used against them by cybercriminals, and thus increasingly vulnerable to supply chain attacks in 2022.

20 December 2021



Cream Cheese Is Latest Product Coming Up In Short Supply Due To Supply Chain Issues. (Photo by SPENCER PLATT / GETTY IMAGES NORTH AMERICA / Getty Images via AFP)

- **MSPs are having more of their own management tools used against them by cybercriminals**
- **The most attacked countries by malware in Q3 2021 were the US, Germany, and Canada**
- **Phishing actors have developed new tricks and even moved to messengers to launch get victims**

Supply chain attacks in 2022 are expected to continue to cause problems for organizations. While most were able to bounce back from such incidents after some time, the damage caused by supply chain attacks was extremely disruptive to everyone.

As 2022 approaches, organizations should be planning on ways to build their cyber resilience and **secure their supply chains from further attacks**. And this not only includes securing the enterprise itself, but making sure all processes in the company's operations that involve third-party operators are secured as well.

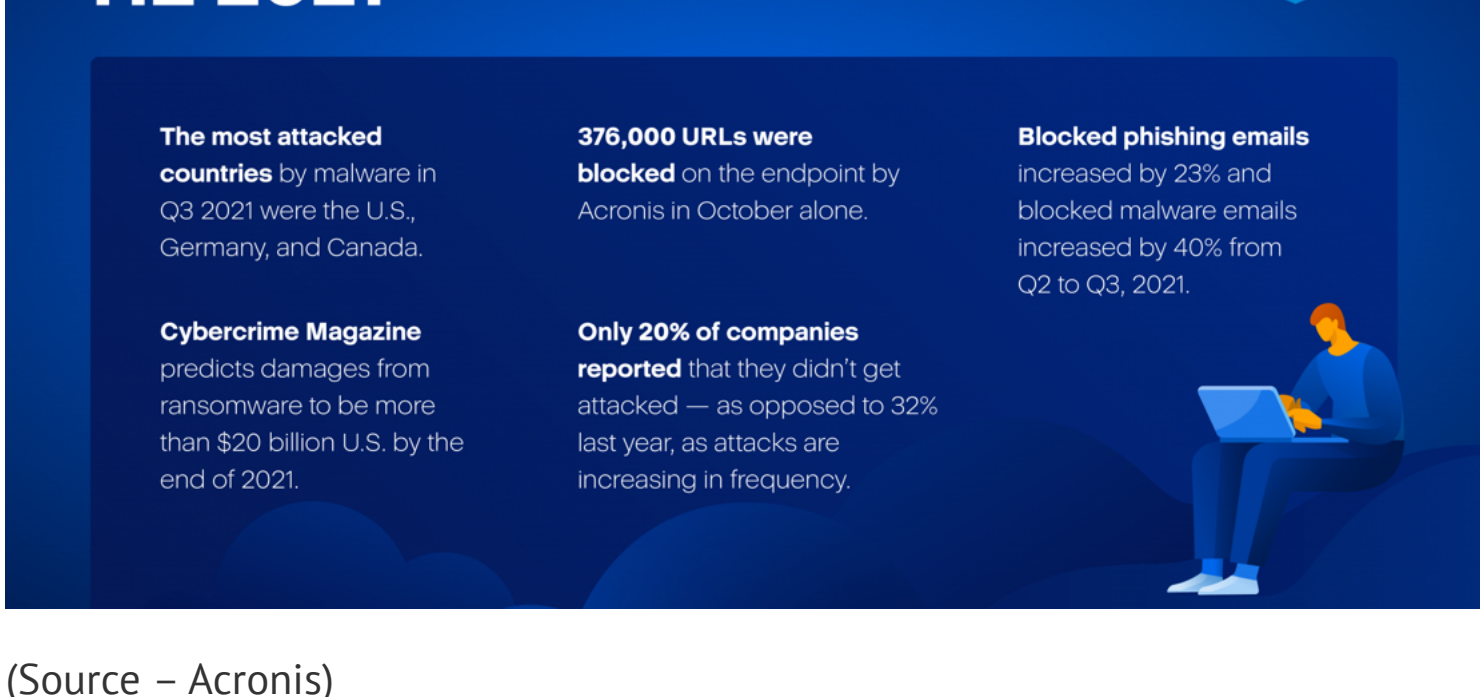
This includes **managed service providers** (MSP). The **Kaseya VSA ransomware attack** this year is an example of how badly a cyberattack on an MSP can severely disrupt the supply chain of its customers. A successful attack on an MSP can cripple hundreds or thousands of small and medium businesses. What's more concerning is that attackers gain access to both their business and clients, as seen in the **SolarWinds breach** last year.

According to **Acronis Cyberthreats Report 2022**, MSPs are particularly at-risk next year. The report highlights that MSPs are having more of their own management tools, such as PSA or RMM, used against them by cybercriminals, and thus are becoming increasingly vulnerable to supply chain attacks. The report also shows that during the second half of 2021, only 20% of companies reported not having been attacked, as opposed to 32% last year, indicating that attacks are increasing in frequency across the board.

Highlights from the report for the second half of 2021 showed:

- The most attacked countries by malware in Q3 2021 were the US, Germany, and Canada
- 376,000 URLs were blocked on the endpoint by Acronis in October alone
- Blocked phishing emails increased by 23% and blocked malware emails increased by 40% from Q2 to Q3, 2021
- Damages from ransomware are expected to top \$20 billion U.S. by the end of 2021

“The cybercrime industry is a well-oiled machine, using cloud and machine intelligence to scale and automate their operations. While the threat landscape continues to grow, we see that the main attack vectors stay the same, and they still work. While the attack surface is growing and 2022 will surely bring us surprises, cyber protection automation remains the only path to greater security, reduced risks, lower costs, and improved efficiency,” says Candid Wuest, Acronis VP of Cyber Protection Research.



(Source – Acronis)

Supply chain attacks are not the only problems predicted for 2022

Apart from MSPs being targeted for supply chain attacks, the report also highlighted several other threats that could potentially disrupt organizations in 2022. **Phishing attacks** remain a big problem.

As 94% of malware gets **delivered by email**, using **social engineering techniques** to trick users into opening malicious attachments or links, phishing has been topping the charts even before the pandemic. This year, Acronis reported blocking 23% more phishing emails and 40% more malware emails in Q3, as compared with Q2 of the same year.

At the same time, **phishing actors** have developed new tricks and even moved to messengers. Now targeting OAuth and **multifactor authentication tools** (MFA), these new tricks allow criminals to take over accounts. To bypass common anti-phishing tools, they will use text messages, Slack, Teams chats, and other tools for attacks such as business email compromise (BEC). One recent example of such an attack was the infamous hijacking of the FBI's own email service, which was compromised and started sending spam emails in November 2021.

As such, 2022 will still see **ransomware be the top threat** to big companies and SMBs alike. High-value targets include the public sector, healthcare, manufacturing, and other critical organizations. But despite some recent arrests, ransomware continues to be one of the most profitable cyber attacks these days. *Cybercrime Magazine* **predicts** ransomware damages will exceed \$20 billion by the end of 2021.

YOU MIGHT LIKE



LOGISTICS

Even Santa's reindeers can't solve holiday season supply chain agony

Lastly, **cryptocurrency** is among the attackers' favorite playing cards. Info stealers and malware that swaps **digital wallet** addresses are the reality today. More of such attacks waged directly against smart contracts may happen in 2022, attacking the programs at the heart of cryptocurrencies. Attacks against **Web 3.0 apps** will also occur more frequently, and new and increasingly sophisticated attacks, such as flash loan attacks, will allow attackers to drain millions of dollars from cryptocurrency pools.

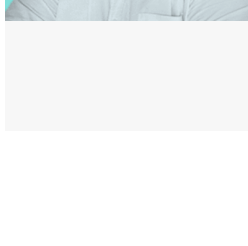
The reality is, every year, cybercriminals are finding more sophisticated ways to launch cyber attacks. With supply chain attacks a major concern for organizations, they need to ensure they are well secured and prepared not just to deal with the attacks but also recover from them fast enough to avoid more financial damages.

MSPs are key for running the IT operations of most SMBs. And cybercriminals know this. SMBs need to ensure they too have sufficient backup and recovery options should they ever be compromised in a cyber attack.

Ransomware

Supply Chain

SHARE



Aaron Raj

@norajar
aaron@hybrid.co

All stories

What does the US\$50b deal of AMD, Xilinx mean to the chip industry?

15 February 2022

Russian hackers profited the most from ransomware payments

15 February 2022

Chip shortages are still forcing the car industry to cut output

15 February 2022

T_HQ

Hybrid brands

Jobs @ Hybrid.co

About
Advertise with us
Contact

© 2022 Copyright TechHQ | All Rights Reserved

Terms of use
Privacy Policy