Kaseya ransomware attack: 80% of companies that pay are hit a second time

By Lior Div

6 Jul 2021

The global Kaseya ransomware attack is a reminder that the public and private sector need to change the way cyber-conflict is fought. The truth is that attackers still enjoy the advantage. The goal isn't to block and prevent all attacks - an operation like Kaseya and SolarWinds demonstrates that's not always possible - the goal is to quickly detect suspicious or malicious activity, and ensure you have the visibility, intelligence, and context to understand and remove the threat.

Lior Div, CEO and co-founder of Cybereason

Modern security companies have the technologies like Endpoint Detection and Response that can end these ransomware attacks. I believe it is our job to disrupt these operations. Technology, coupled with public and private partnerships is a step in the right direction to help in this fight against the REvil ransomware gangs and others like them.

We need to shift focus from dealing with ransomware after the fact to disrupting the earliest stages of attacks through behavioural detections - this is the operation centric approach to cybersecurity. We can’t just focus on the ransomware attack - by then it is too late. Look at the earlier stages of the attack when criminals are inserting malicious code into the supply chain for instance. The ransomware is the symptom of the larger disease we need to treat.

Massive ransomware attack hits South African businesses

5 Jul 2021

This newest attack will once again start the debate about whether it makes sense to rip and replace legacy computer networks used by public and private sector organisations. That simply isn't going to fix the problem. We have spent trillions of dollars on cybersecurity over the past 20 years. And in many ways, we're no safer today. We could spend another $250bn or $250tn and it will only incrementally help. What matters is how the money is spent.

In the coming days, we will learn the names of companies impacted by the Kaseya ransomware attack. We will also learn if companies are meeting the ransom demands of the REvil gang. In general, it doesn’t pay to pay ransoms. A recent Cybereason global research study found that 80% of companies that paid a ransom were hit a second time.

Overall, paying ransoms only emboldens threat actors and drives up ransom demands. Still, whether or not to pay a ransom is an individual choice each company needs to make. Consult with your legal team, insurer and law enforcement agencies before making any decision. In those rare life or death situations, paying a ransom could very well be the right decision.

ABOUT THE AUTHOR

Lior Div is the CEO and co-founder of Cybereason.