BIZCOMMUNITY

5 important lessons to learn from the REvil ransomware attack

By Anna Collard

13 Jul 2021

The recent ransomware attack carried out by REvil caused shockwaves around the world for a number of reasons: partly because of its scale the high ransom demanded, but also because it successfully breached a trusted IT solutions provider, using its network to impact thousands of customers around the world.

Anna Collard, SVP of content strategy & Evangelist for KnowBe4 Africa | image supplied

Kaseya's VSA remote network and endpoint monitoring solution for enterprises and managed service providers were used as a channel to both managed service providers (MSPs) and end customers.

This type of attack could not easily have been avoided, which is why the IT security industry and global organisations have reacted with heightened alarm. Where customers carry out due diligence and outsource to a service provider, there is a relationship of trust in place, and organisations typically expect proper supply chain risk management, patching and vulnerability management.

In the case of the Kaseya attack, which is thought to have been a Zero Day exploit, very little could have been done to prevent it. However, the incident has taught us five important lessons:

1. The world is increasingly interdependent

The REvil ransomware attack highlighted the interdependencies we all have: as an organisation, responsibility for security

isn’t just in the scope of our own environments, our vulnerabilities can impact the entire ecosystem.

The supply chain risk isn’t linear, as we saw from this attack – it can impact service providers, and through them, their customers in a complex web or ecosystem.

2. Security technologies aren’t always secure technologies

There is growing evidence that the very security technologies customers trust to protect them are increasingly being targeted by cybercriminals. How vulnerabilities should be disclosed may need to be revisited, and now more than ever before, it is vital to monitor and patch VPNs, firewalls, and any other security technologies we use.

3. Everyone is a target

No matter how big or small an organisation is, it is at risk. South Africa is not exempt, and in future could become more of a target as larger countries with more resources take a tougher stance on cybercrime.

Massive ransomware attack hits South African businesses

5 Jul 2021

4. CISO roles have changed

A chief information security officer's (CISO) role is no longer limited to risk management – now it also encompasses crisis management.

We have to plan for the worst; the threat of extortion isn’t going anywhere until underlying factors have been addressed. Among these factors are the deep-rooted security debt that has accumulated in our technology stacks over 30 years as we rushed towards an 'everything digital, everything online' society.

As well as governments investing in offensive security which doesn’t help anyone as their attack toolkits leak out into the underground and are used by malicious threat actors.

Orange Cyber Défense’s white paper Beating Ransomware notes that ransomware is a crime, not a technology problem, and therefore technology controls alone cannot resolve it. Cyber risk mitigation must include training and awareness and careful incident response planning.

5. We have to prioritise mitigation/prevention

Organisations must prepare for ‘when’ not ‘if’ they are attacked, and implement robust vulnerability management programmes, crisis management protocols, and a solid 3:2:1 backup strategy (which entails having at least three total copies of your data, two of which on different mediums (i.e., on different devices or hard-drives as well as the cloud), and at least one copy off-site).

Because there is a growing risk of double extortion – whereby attackers not only lock down data but also threaten to expose sensitive data, organisations should mitigate this risk by limiting the access service providers have to sensitive and mission-critical data.

Ongoing awareness and training remain one of the most important measures organisations can take to mitigate the risk of cyber-attacks, particularly since phishing remains the top method of launching ransomware attacks.

KnowBe4 report

The importance of training was highlighted in the recent *KnowBe4 2021 Phishing by Industry Benchmark* report, which measured organisations Phish-Prone percentage (PPP) – an indication of how many of their employees are likely to fall for phishing or social engineering scam.

The baseline phishing before any KnowBe4 security awareness training indicated a high level of risk, with an average initial baseline PPP of 31.4% across all industries and sizes. After 90 days of computer-based training and simulated phishing testing, the average PPP was reduced by approximately 50% to 16.4%, and after one year of monthly simulated phishing tests and regular training, the PPP further declined to just 4.8%.

For a great practical guide on how to mitigate ransom refer to Orange Cyber Defense “Beating Ransomware” Whitepaper

ABOUT ANNA COLLARD

Anna Collard is the senior vice president of content strategy and tech evangelist at KnowBe4 Africa
- #BizTrends2022: Discriminatory AI and disinformation powered by deep fakes - 10 Jan 2022
- 5 important lessons to learn from the REvil ransomware attack - 13 Jul 2021
- Here's how hackers break into the business environment and how it can be avoided - 11 Jun 2021
- PoPI Act readiness: 6 things to do - 12 Apr 2021
- Top IT security threats in 2021 - 20 Jan 2021

View my profile and articles...