Will banning cryptocurrency halt the scourge of ransomware?

By Brendon Kotze

19 Jul 2021

Ransomware attacks are on the rise. Recently, one criminal group staged a global attack that locked the systems of organisations in 17 countries, including South Africa.

Brendon Kotze, chief development officer, Performanta

Many people have been weighing in on the issue and talking about possible solutions. We've reached the stage where some suggestions are pretty radical. Ransomware locks your data with encryption and then extorts a cryptocurrency fee to get the unlock code. Cryptocurrencies primarily operate outside of financial systems and their paper trails, and are easier to launder into hard currency. Recently, publications such as the *Wall Street Journal* and *The Verge* mulled the idea of banning cryptocurrencies, as they are the payment of choice for ransom demands.

Symptom, not the cause

But that is too drastic an action, and I doubt it will make a real difference. If we step back, the problem isn't ransomware but weak security and the low risk associated with cybercrime. You can ban crypto, but criminals will find other techniques and payment systems to get their way. They can just do what cybercriminals are known for: steal your data and sell it to the highest bidder. Canning cryptocurrencies won't stop that.

The idea is also flawed because it tackles a symptom, not the causes. And there is one cause that few people talk about: the security poverty line. Analysts have coined this term to designate companies that cannot afford proper cybersecurity, and note that the vast majority of businesses fall under this threshold. The math is obvious: if the vast majority of companies (predominantly SMEs) cannot afford decent cybersecurity, a sharp jump in successful attacks is the outcome.

In the current market, you need to spend a lot to get genuinely robust security. JPMorgan Chase spends about $600m annually and employs 3,000 security staff. The cybersecurity market caters primarily for such customers. If you are a small or medium enterprise, or an individual, and with limited or no access to security skills, there isn't much out there to secure you. Yet, the answer doesn't start with buying technology. It starts with awareness.

Fixing this problem won't be easy, but we can start by talking about it. People should know more about their individual security risks. If we spend as much attention on security hygiene as we complain about our data on Facebook, it will be harder for cybercriminals to succeed.

We should also stop framing this problem as primarily one involving nation-states. Yes, they play a role, but most attacks are launched by unsophisticated criminal gangs. While security vendors develop a new impressive technology, cybercriminals dip into old attacks that we've forgotten about. Some of the most dangerous malware out there today first emerged over a decade ago.

Targeting small enterprises

Sensationalism and apathy are taking individuals off the hook and allowing the cybersecurity industry to focus on the big companies, not the little guy. Yet most attacks target small companies, and most attackers get through because an individual didn't scrutinise a phishing mail.

These are easy to solve problems. They require a change in attitude among people, security vendors, and the media. People need to understand they are the target, security vendors must help lower the security poverty line, and the media should look beyond sensationalism and treat cybercrime as a pandemic. If we could promote security hygiene the way we push masks and social distancing, the risk-reward ratio of cybercrime will diminish substantially.

Or we can ban cryptocurrencies and see what new trick the bad guys come up with next, which they will.

ABOUT THE AUTHOR

Brendan Kotze is the chief development officer at Performanta.

For more, visit: https://www.bizcommunity.com