BIZCOMMUNITY

Cryptocurrency is fuelling cybercrime

By Doros Hadjizenonos

20 Jul 2021

Criminals have kept pace with changing technologies by no longer wanting their crimes to generate hard cash - Bitcoin has become the currency of choice. That's particularly true for cybercrime, where ransomware is booming as criminals infiltrate organisations' IT systems and threaten to publish or destroy crucial data unless a ransom is paid in Bitcoin.

Doros Hadjizenonos, regional sales manager at Fortinet | image supplied

How cypto encourages cybercrime

Ransomware payments have become so huge that attacks are mounting daily. A recent high-profile case was an attack on the US Colonial Pipeline, causing the system that carries 2.5 million barrels of oil a day to be shut off. It's become such a lucrative business that some syndicates now offer ransomware-as-a-service (Raas) where people can buy premade malicious software, which lowers the technical barrier to entry. One example is a group known as Sodinokibi, which runs a Raas business that earns them a cut of any successful attacks by other people.

Cryptocurrency is fuelling the activity because its anonymous and decentralised nature makes the transactions hard to trace and link to individuals. While the transactions take place on 'public ledgers' the parties in each transaction are anonymous and disguised with a random number.

Cryptocurrency target market is growing

While cryptocurrency has become the preferred method of payment, the companies and individuals dealing in it aren't immune from attack either. Hackers can penetrate bitcoin exchange platforms and take over by implanting corrupted programs. And as more and more ordinary people dabble in cryptocurrency trading, the target market is increasing every day.

Hackers recently targeted some cryptocurrency organisations via social media accounts of certain employees. The employees were sent phishing documents purporting to be recruiting for a blockchain company, but it led to malware being

introduced onto their networks.

Secure your cryptocurrency investments

Anyone investing in cryptocurrency must ensure that they put a comprehensive and multi-level security strategy in place to protect their investments. That needs to include end-user awareness and training about the latest social engineering attack methodologies so people know what to look for because ransomware makes its way onto devices and networks through infected emails, SMSs, websites or applications.

It is extremely important to always choose reputable cryptocurrency wallets, exchanges, brokerages and mobile applications when investing in cryptocurrencies. Applying core security principles like using strong passwords (changed frequently and never re-use the same password for other applications or websites) with two-factor authentication will minimise the risk of your cryptocurrency wallet being compromised. The responsibility of protecting your investment lies mainly with the end-user.

ABOUT THE AUTHOR

Doros Hadjizenonos is the regional sales manager at Fortinet.