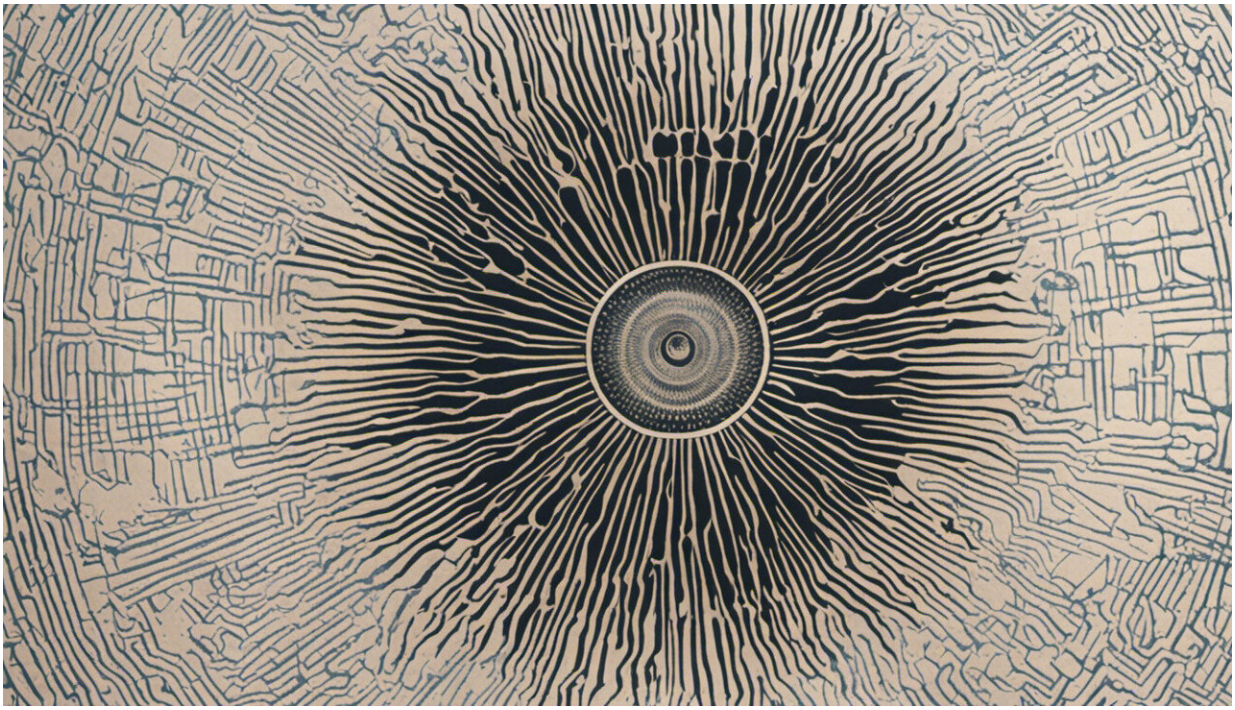
Are cryptocurrencies a dream come true for cyber-extortionists?

September 12 2017, by Nir Kshetri



Credit: AI-generated image (disclaimer)

When malicious software takes over computers around the world, encrypts their data and demands a ransom to decode the information, regular activities of governments, companies and hospitals slam to a halt. Sometimes security researchers release a fix that allows computer owners to decrypt their machines without paying, but many people are

forced to pony up to free their data.

In 2016, the FBI estimated that the ransomware industry took in US$1 billion – and that's only the cases officials know about. All that money isn't paid in cash. Before digital currencies existed, extortionists asked victims to send money by more formal transfer companies like Western Union or make deposits to bank accounts. Those were easily traced. Today, ransomware attacks demand payment in bitcoin and its ilk, systems praised by supporters for their transaction speed and protection of users' anonymity.

In researching cybercrime and cybersecurity for more than a decade, I have found that obtaining cybercrime proceeds is often the biggest challenge that cybercriminals face. In this regard, diffusion of cryptocurrencies is a major development that enables cybercriminals to achieve their goals. In fact, the escalation of ransomware attacks and the increasing prominence of cryptocurrencies may be connected. Some companies have invested in bitcoin and other cryptocurrencies specifically so they can pay extortionists if it ever becomes necessary. That helps contribute to the rapid growth in use and value of e-currencies. And as digital currencies become more common, ransomware attackers will have an easier time hiding their illicit transactions among the growing crowd of legitimate transfers.

Using cryptocurrencies in cyber extortion

The extortionists behind most ransomware attacks demand payments in bitcoin, the most popular cryptocurrency. The WannaCry attackers demanded between $300 and $600 per computer; the Petya ransomware wanted $300 in bitcoins before providing a code that would let victims decrypt their data. Not many people actually pay, though: WannaCry victims paid only about $241,000 in bitcoins to the extortionists. If everyone infected had paid, the criminals would have received at least

$60 million. It translated to a payout rate of 0.4 percent. Even fewer paid the Petya perpetrators: They got just 66 payments, totaling barely over 4 bitcoins, or about $18,200.

Other attacks are more successful: In June, a ransomware attack hit more than 150 servers owned by South Korean web hosting firm Nayana. More than 3,400 of the company's customers were affected – mostly small businesses running their websites on Nayana's equipment. Nayana itself stepped up, taking loans to cover a payment of more than $1 million in bitcoins to the attackers, saying it had to save its clients' sites.

The attackers don't always need to make much money to be effective. Many cybersecurity researchers believe that Petya attacks were carried out with political motives rather than for financial gains. But ransomware has a much higher payout rate than other common cybercrimes. One study found that for every 12.5 million spam emails sent promoting a fake online pharmacy, the scammers got only one response. That's a success rate of about 0.000008 percent. They make a lot of money – up to $3.5 million a year – only by sending out enormous numbers of messages.

Trusting cyberthieves?

One reason cybercrime success rates are low is that victims don't trust the extortionists to actually unlock their data once they get paid. In 2016, about a quarter of the organizations that paid ransoms were not able to recover their data.

The WannaCry attackers were particularly bad: Their system was labor-intensive, requiring the criminals to manually connect payments with encrypted files before letting victims decode them. In fact, a flaw in the WannaCry attack software made it almost impossible to decrypt a paying victim's data.

More sophisticated methods do exist, including those that incorporate what are called "smart contracts," another aspect of some cryptocurrency systems that runs a particular program as part of completing a transaction. In those ransomware attacks, making payment automatically releases the information a victim needs to decrypt and recover hijacked files.

Preparing for future ransomware

The fear of ransomware is growing. In mid-2016, a study found that one-third of British firms had bought bitcoins just in case they needed to pay off ransomware attackers. More than 35 percent of large firms, those with more than 2,000 employees, reported being willing to pay as much as $65,000 to unlock critical files. Even Cornell University was reported to be stockpiling bitcoins in case of a future ransomware attack.

At the same time, bitcoin and other similar systems are becoming much more popular. In 2016, the total value of all cryptocurrencies was 0.025 percent of the world's GDP. By August 2017, that number had increased more than eight-fold, to 0.21 percent of global GDP – about $162 billion . The World Economic Forum projects cryptocurrencies will hold 10 percent of global GDP by 2027.

These cycles are self-reinforcing: The more transactions there are involving cryptocurrencies, the harder it will be to trace where the money is going. As a result, cybercriminals will use cryptocurrencies more often – forcing their victims (and even potential targets) to invest in cryptocurrencies, too.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation