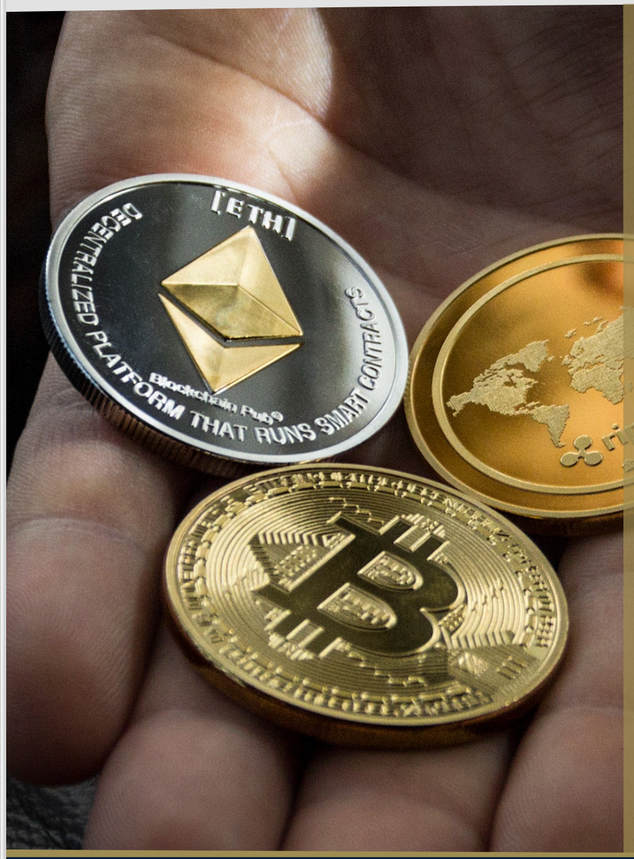


RANSOMWARE
A CRYPTOCURRENCY PROBLEM

Until relatively recently, when someone mentioned cybercrime, they were referring to cloned credit cards or illegal withdrawals from bank accounts, limited to the amount in a personal bank account. These days, though, it seems that all we are hearing about is one ransomware attack after another and the numbers are astronomical! Many people don't realise it, but we have really entered the world of cyber warfare where governments are backing attacks on big and small businesses.

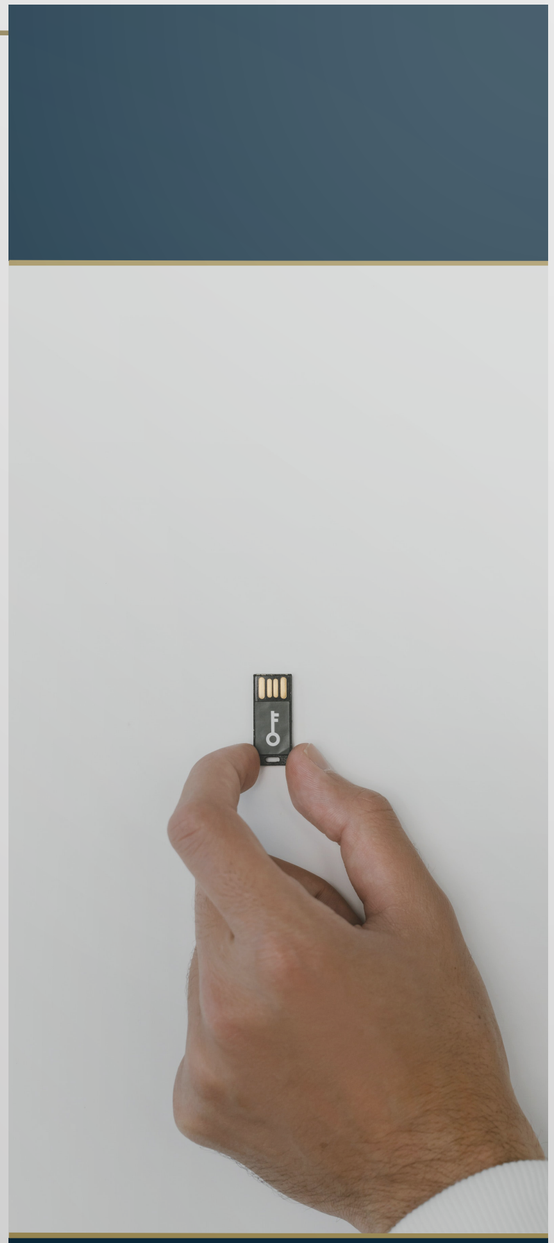
EXPECTED TO RISE TO $265 BILLION BY 2031

So far, ransomware has cost businesses around the world, $20 billion this year alone. That number is expected to rise to $265 billion by 2031. Research shows that 32% of ransomware victims pay the ransom, but they only get 65% percent of their data back. When you compare that to the 57% of businesses that are successful in recovering their data using a backup, it seems like there should be very little reason to give in and pay.

Unfortunately, most companies opt to pay the ransom because the interruption to their business caused by the ransomware ends up costing them more than the pay-out. In most cases, the cybercriminals demand an amount in the cryptocurrency of their choice, and when converted, this amount may not be negligible, but is far smaller than the cost of shutting down operations while data is being recovered and restored.

In fact, the growing success of cryptocurrencies can be said to be the impetus behind the increasing number of ransomware attacks being seen around the world. Cryptocurrencies like Bitcoin are fast and easy to get hold of, and most importantly, they are largely anonymous and hard to trace.

Cryptocurrencies are essentially the high-tech solution to the most common problem faced by thieves and criminals: how to transport and hide huge sums of ill-gotten gains without getting caught. Ransom demands in traditional currency require banks to be involved in the process, and they can intervene to stop payment. This was essentially what ended "screen lockers", which demanded a credit card payment to unlock the victim's computer. In addition, most cryptocurrency is decentralised, so it crosses borders without any controls taking place.



It’s not surprising that cryptocurrency’s role in the ransomware ecosystem has led some to call for banning cryptocurrency altogether. Others have suggested regulating cryptocurrency mining to make it more difficult to process ransom transactions. However, this would require a concerted international effort, and any outright ban would still leave the underlying blockchain technology available for criminals to start up their own cryptocurrencies on the dark web.

According to security experts, many of the ransomware attacks we are seeing at the moment are not specifically targeted. Rather, bots looking for vulnerabilities are running in regions where attacks have been successful, and those organisations that have security holes are becoming victims. These ransomware programmes can easily be purchased on the dark web, and don’t require specific hacking expertise to run.

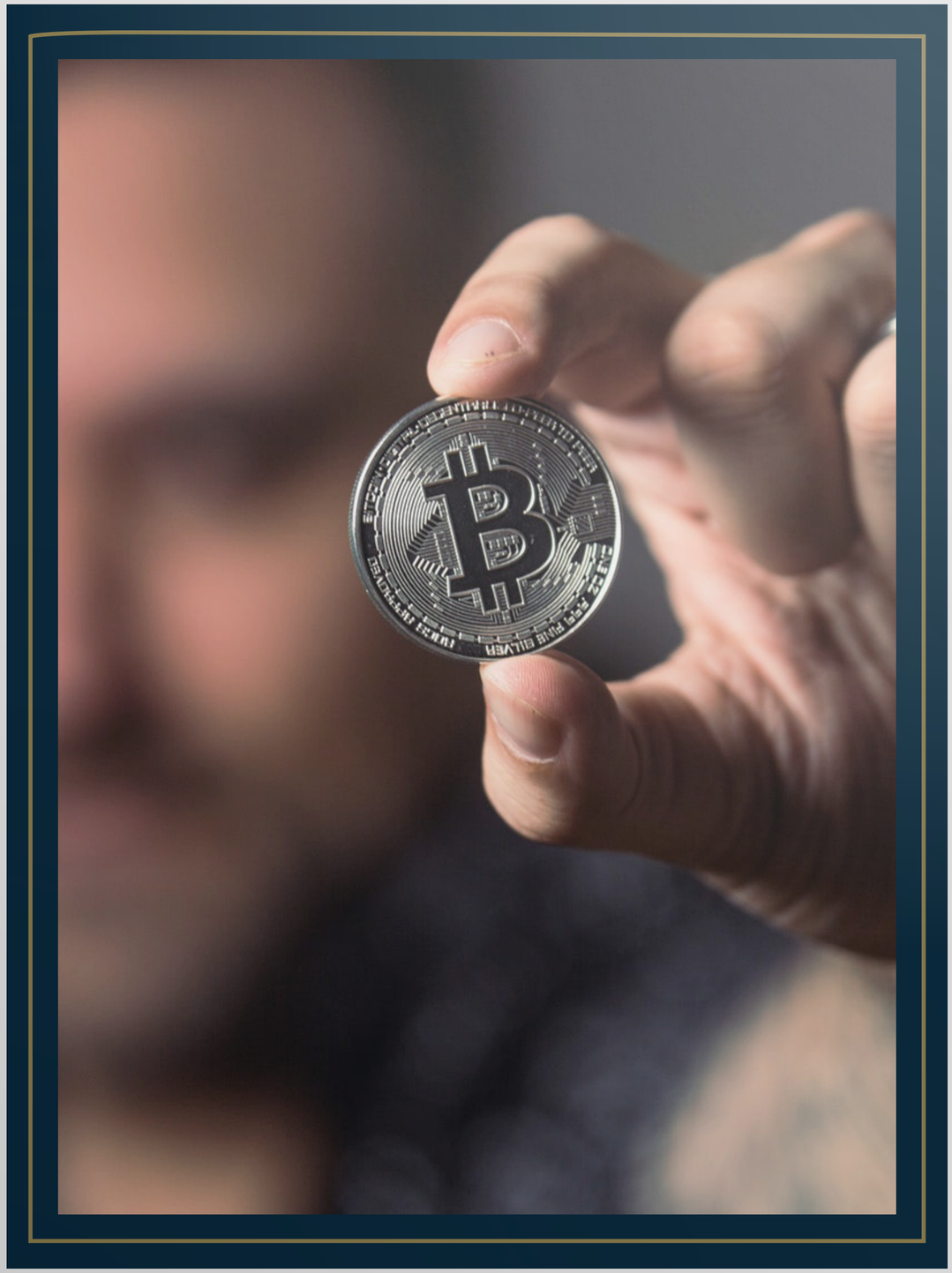
The silver lining to this situation is that all cryptocurrency transactions are recorded on the distributed blockchain ledger, allowing them to be traced. This is how the FBI was recently able to recover most of a ransomware payment.

Colonial Pipeline, which is responsible for fuel pipelines across the USA, was held to ransom, leading to the shutdown of gasoline supplies in the eastern US for the better part of a week. The FBI recovered more than half of the $4.4 million or R65.2m in ransom that Colonial paid to the hackers, who are known as DarkSide and believed to be based in Russia. This was the first time that a task force devoted to ransomware has been able to get some of the money back.

RANSOMEWARE PROGRAMMES CAN EASILY BE PURCHASED ON THE DARK WEB

According to court documents, the FBI worked its way through a maze of more than 20 cryptocurrency accounts to find the hackers. When it did locate the account, the bureau then sought a court order to seize the funds. However, even when the FBI located the computer, and had the court order, the bureau still needed the secret encryption key to unlock the account and capture the Bitcoin. The FBI hasn't said how it did this, but officially announced the recovery of the funds when it was successful.

The increase in ransomware attacks in both number and value is the latest unintended consequence of pushing for an unregulated financial market. Every government will tell you that it is not feasible, but many just don’t have the technical skill to design the antidote. The role of cryptocurrencies in enabling ransomware cannot be denied, and regulators must be forced to take this issue seriously. Government agencies worldwide, including Europol and the UK’s National Cyber Security Centre joined the US Department of Homeland Security and a host of private companies in supporting an international Ransomware Task Force, which published a report outlining possible methods of mitigating these attacks earlier this year. However, until we have complete international co-operation and effective regulations, ransomware will continue to be a cryptocurrency problem.



FOLLOWING FIRTH | SEPTEMBER 2021