Bitcoin proves double-edged sword for criminals

9 June 2021, by Joseph Sotinel

US authorities have said they were able to access the 'private key' to the hackers' bitcoin account of ransomware hackers Darkside.

Regulators have repeatedly criticised the growth of cryptocurrencies such as bitcoin because of their popularity with criminals but the technology's transparent transactions can also work against law breakers.

The lesson is one that has been learnt by cybercriminal hackers Darkside the hard way after the organisation extracted a $4.4 million ransom from oil company Colonial Pipeline in bitcoin.

Following the ransomware extortion, which forced the shutdown of a major fuel network in the eastern United States last month, the US Justice Department said it has clawed back $2.3 million of the funds by tracing financial transactions.

"Following the money remains one of the most basic, yet powerful, tools we have," US Deputy Attorney General Lisa Monaco said on Monday.

The financial forensics to track crypto transactions are more complex on the decentralised and anonymous networks.

For a traditional bank payment, police can turn to the bank that sent or received the money but for bitcoin, the registry that records these transactions—the blockchain—does not ask users to reveal their identity.

But the blockchain is also public and available to everyone to download and piece together who might own the anonymous addresses where the bitcoin arrives.

While some users keep their bitcoin safe in an offline wallet, for example on a USB stick or hard drive, Darkside's bitcoins were always linked to an online account.

Without specifying how they came by it—whether by hacking or through an informant—US authorities have said they were able to access the "private key" to the hackers' online account.

In 2019, analysis of the blockchain enabled British and American authorities to dismantle a child pornography ring and arrest more than 300 people in 38 countries.

The complex tracking of transactions has become an industry in its own right. Firms specialising in blockchain analysis have developed, such as Chainalysis in the United States and Elliptic in Britain.

The US Justice Department said it has clawed back $2.3 million of the funds Darkside received from Colonial Pipelines by tracing financial transactions.

Russian Hydra

According to a Chainalysis report released in February, cryptocurrency transactions for illegal purposes reached $10 billion in 2020, one percent of total cryptocurrency activity for the year. In 2019 criminal activity using the online currencies reached a record $21.4 billion.

The total cost of ransomware payments alone made in cryptocurrencies soared to nearly $350 million in 2020.

"Cryptocurrency remains appealing for criminals, primarily due to its pseudonymous nature and the ease with which it allows users to instantly send funds anywhere in the world, " Chainalysis said.

Elliptic analysts believe they have identified the bitcoin wallet that received the ransom payment from Colonial Pipeline to Darkside, and found that at least one other payment of $4.4 million.

More importantly, analysis of the transactions can identify the bitcoin sales platforms that received the wallet's ill-gotten funds.

"This information will provide law enforcement with critical leads to identify the perpetrators of these attacks," Elliptic researcher Tom Robinson wrote.

Market regulators have put pressure on cryptocurrency exchange platforms. Many, such as Coinbase, now require users to disclose their identity before making transactions. But other platforms are not following the same rules.

Both Elliptic and Chainalysis point to the growing role of Hydra, a sales site for Russian-speaking customers, which is accessible via the darknet, a version of the web not listed on search engines and where users can remain anonymous.

"Hydra offers cash-out services alongside narcotics, hacking tools and fake IDs," Robinson explained.

Using sites like Hydra in conjunction with cryptocurrencies, Darkside's hackers have reportedly already resold some of the ransomed bitcoins.

As the price of bitcoin has soared in recent months regulators are adapting their strategies.

The Bank of England said on Monday that payments in stablecoins, fixed-price cryptocurrencies, should be regulated to the same standards as bank payments.

APA citation: Bitcoin proves double-edged sword for criminals (2021, June 9) retrieved 24 October 2021 from https://techxplore.com/news/2021-06-bitcoin-double-edged-sword-criminals.html