Sodinokibi Ransomware to stop taking Bitcoin to hide money trail

bleepingcomputer.com/news/security/sodinokibi-ransomware-to-stop-taking-bitcoin-to-hide-money-trail/

Lawrence Abrams

By
Lawrence Abrams

- April 11, 2020
- 04:23 PM
- 0

The Sodinokibi Ransomware has started to accept the Monero cryptocurrency to make it harder for law enforcement to track ransom payments and plans to stop allowing bitcoin payments in the future.

In a 2019 webinar titled "The functionality of privacy coins", Europol stated that the use of both Tor and Monero made it impossible to trace the funds or the actors who received them.

“Since the suspect used a combination of TOR and privacy coins, we could not trace the funds. We could not trace the IP addresses. Which means, we hit the end of the road. Whatever happened on the Bitcoin blockchain was visible and that’s why we were able to get reasonably far. But with Monero blockchain, that was the point where the investigation has ended. So this is a classical example of one of several cases we had where the suspect decided to move funds from Bitcoin or Ethereum to Monero," Europol's Jerek Jakubcek said in a webinar.

Last month, the ransomware operators behind the Sodinokibi/REvil ransomware posted to a hacker and malware forum that they are starting to accept the Monero cryptocurrency to make it harder for law enforcement to trace them.

"This principle has led to allegations that Monero could be used for drug trafficking, the dissemination of child pornography and more. In this regard, Europol in 2017 expressed concern about the growing popularity of Monero. In 2020, Europol made an official statement - Monero is impossible to track.

Due to CryptoNote and the obfuscation added to the protocol, passive mixing is provided: all transactions in the system are anonymous, and all participants in the system can use plausible denial in case of capture.

The combination of an anonymous browser Tor and Monero can quite successfully make a person’s financial activity completely invisible to the police and government agencies. We are extremely worried about the anonymity and security of our adverts, so we began a “forced” transition from the BTC to Monero."

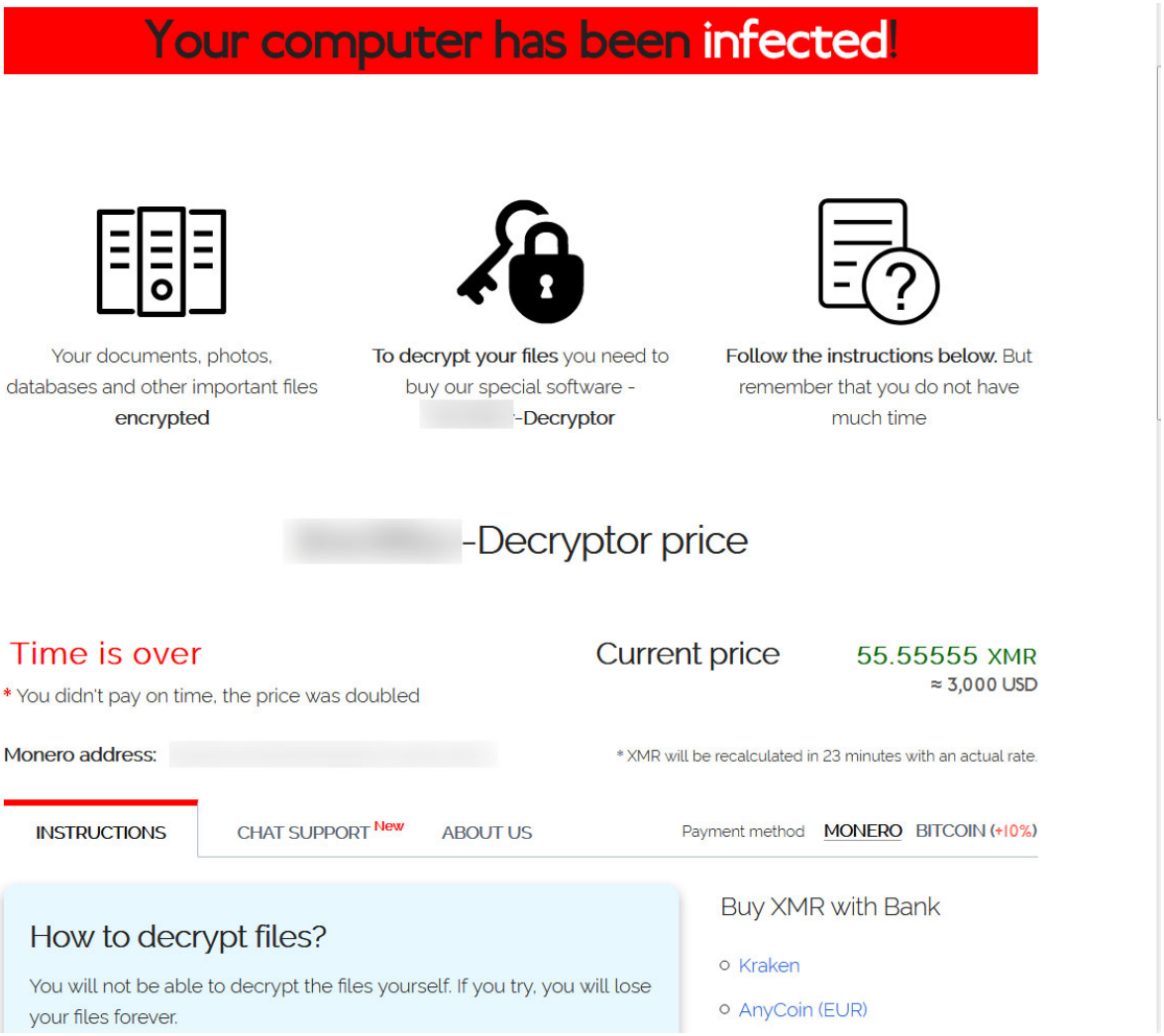
The operators go on to say that they will eventually remove bitcoins as a payment option and that victims need to start to learn more about Monero and how to acquire it.

"In this regard, we inform you that after a while the BTC will be removed as a payment method. Victims need to begin to understand the new cryptocurrency, as well as other interested parties who work with us," the threat actors warned.

Tor ransom payment site uses Monero by default

On the Sodinokibi Tor payment site, the ransomware operators have already started to move away from bitcoin by making Monero the default payment currency.

If a victim wants to use bitcoin to make a ransom payment, the amount is increased by 10%.



Tor payment site accepting Monero

The ransomware operators are also offering "partners" who help victims pay the ransom a discount that will make them "pleasantly surprised".

"Companies that assist our victims in acquiring the decryptor will be pleasantly surprised by the% discount on the amount of the ransom. In order to start working with us, it is enough to write in a chat and introduce yourself as a company of this type of activity. Our collaboration is completely anonymous. We do not disclose the data of our partners," the ransomware operators offered.

Many of these "data recovery" companies add a significant surcharge to victims they help, and with this additional discount, they stand to make a much larger profit by helping Sodinokibi switch to Monero.

Related Articles:

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

REvil ransomware returns: New malware sample confirms gang is back

REvil's TOR sites come alive to redirect to new ransomware operation

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.