Malware digs virtual money over antivirus programs, forcing Windows to crash

Digging money for encryption is a new trend in the malware world, and recently, security company 360 Total Security has discovered a new malware that is extremely aggressive.

With the code name WinstarNssmMiner, this malware is said to take full advantage of the system resources to dig Monero cryptography, and it is also equipped with many protection techniques to bypass antivirus solutions and ensure users. It is not possible to close its processes.

First and foremost, when infecting the system, WinstarNssmMiner will try to avoid detection of antivirus programs by not starting the shady operations when the antivirus program is scanning. Instead, it will lie dormant and wait until the right time to begin the infection phase.

This malware then creates two different system processes called **svchost.exe** to hide its purpose. One of the two processes will start pre-coding digging, while the other will act as a "guard": if it detects that the antivirus programs scan the system, it will immediately stop running. move again.

But that's not the worst. Even if the user detects the malware and tries to close its progress from Task Manager, it will activate the BSOD - Windows "legendary" blue screen - causing the system to crash and forcing the user to boot. Leave the machine, thereby allowing itself to be restarted. So closing this malware process is impossible!

"This malware acts very cleverly in the face of different antivirus software. It will turn off the protection of weak antivirus programs, and find a way to retreat when meeting a stronger opponent. If not equipped with a good antivirus program will have to accept living with the slow and blue screen error on their computers " - 360 Total Security security company said.

As mentioned above, this malware uses the entire system resources to dig Monero encryption, and at the time of its discovery, it dug up about $ 28,000 worth of pre-encryption.

According to analysts, this malware is currently spreading strongly on computer systems around the world, and the easiest way to secure your data is to use fully updated antivirus programs, simultaneously. must scan new files since downloading. Finally, using reputable antivirus products can help you prevent any potential infections.

See more:

1. Many computers in Vietnam have been hijacked due to virus infection
2. Warning: new code of virtual money digging is available via Facebook Messenger
3. What to do when the computer is infected with a virus that fights virtual money?