Strange ransomware detection only attacks the rich

Other ransomware often spread to all victims if possible, but the new ransomware is different, it selectively infects.

Recently, security researchers have discovered a new ransomware that works differently from other extortion malware software.

CrowdStrike and FireEye, two security companies that discovered the malware, said that since August 2018, it has earned more than $ 4 million in data encryption and extortion.

Other ransomware often spread to all victims if possible, but the new ransomware is different, it selectively infects. Specifically, Ryuk ransomware only infects large businesses, based on a security vulnerability created by another malicious software called Trickbot created earlier. Meanwhile, Ryuk does not attack small companies that are also infected with Trickbot.

CrowdStrike calls Ryuk's attack method 'big-game hunting', the target of attack is large companies and businesses.

Based on Trickbot, Ryuk will explore the system of objects to attack to understand their resources and ability to pay a huge ransom. In order for these companies to fail, the malware will not rush to attack immediately, but will conduct the most important system reconnaissance, then finally make a large-scale attack.

Currently, CrowdStrike and FireEye experts have found some evidence that Ryuk has some connection with Russia.

See more:

1. 14 games on the App Store contain malicious code, iPhone users be careful
2. 1.6 million computers in Vietnam were erased by the virus, losing nearly 15,000 billion in 2018
3. Warning: New extortion code GandCrab is attacking Vietnamese Internet users