New generation extortion trojan detection

The new generation of extortion trojans is much more dangerous because of the use of an anonymous TOR network and a stronger encryption method.

The new generation of extortion trojans is much more dangerous because of the use of an anonymous TOR network and a stronger encryption method.

Ransomware are the most annoying types of malware because they have the ability to encrypt user data and then demand ransom to decrypt. The preferred form of trading by bad guys is to use free currencies like *Bitcoin* . In most cases of infection, *ransomware* removal is not difficult, but this does not help users retrieve their valuable data.

Recently, the ransomware wave was even more dangerous when Kaspersky recently announced the discovery of a new threat called *CTB-Locker*, also known as *Critroni* or Onion, which is a ransomware type using an anonymous TOR system. *Trend Micro* also said it has discovered a new type of extortion Crytoblocker trojan that is seen as the next generation of CryptoLocker; and Synology customers are now the target of this new generation of ransomware.

Stu Sjouwerman, CEO of *KnowBe4* (*a company specializing in security awareness training*) added that the new generation of CTB-Locker extortion trojans probably originated from an Eastern European country like *Romania* or *Ukaraine* because of a The first number of cases were detected in Russia. Russian criminals never attacked their own countries because if they did, they would be immediately arrested by security agencies.

The reason for the new generation of extortion trojans is more dangerous because according to KnowBe4, CTB-Locker uses an anonymous TOR network to control attack servers (*C&C servers*), so it is difficult to intercept.

CTB-Locker also has the ability to compress data before encryption. In addition, the new generation extortion trojan also uses the *Elliptic Curve Diffie-Hellman* encryption method, which is rarely used but is a very powerful encryption method. In particular, *CTB-Locker* is built as a commercial software, so it can be widely traded in cybercrime world.

As I said before, the best way to protect users from ransomware is not to open suspicious attachments without checking the virus first. In addition, software should not be downloaded from unknown sites. And let's get to the habit of regularly backing up personal data in different locations (*online as well as offline*) to ensure there's always a backup copy even if *ransomware* wreaks havoc on your system.