Ako ransomware is raging all over the world, what do you know about this ransomware?

Ako was first discovered when a victim posted information about an infection he encountered on the Bleeping Computer security forum.

Ransomware has been one of the top security threats for nearly three years, since the first ransomware strain - WannaCry - was discovered in May 2017. Recently national security researchers International has continued to find a new strain of ransomware that possesses a very special encryption method, called Ako.

Ako was first discovered when a victim posted information about an infection he encountered on the Bleeping Computer security forum. Bleeping Computer experts then analyzed the malware and discovered that it was a new ransomware strain, with extremely dangerous properties: Targeting the entire network instead of just individual workstations. as usual.

Some important characteristics of this malicious code have been summarized by Bleeping Computer as follows:

1. Ako mainly affects single computer systems running Windows 10 and servers running Windows SBS 2011.
2. Contains many similarities with another ransomware strain: MedusaLocker - but the two types of malicious code today are not products from the same unknown malicious source.
3. Target the entire network instead of just individual workstations like many other malicious code.

How Ako works

The mode of attack of this malicious code is relatively sophisticated:

1. After successful infection, Ako will immediately delete the file copies as well as recent backups on the system.
2. Next, the malicious code will disable the Windows recovery environment before starting to encrypt data.

3. While encrypting, Ako will add a randomly generated extension to the files, and add the 'CECAEFBE' marker string to the successfully encrypted files so that the ransomware can identify them.
4. During the encryption process, Ako will ignore files with the extension .exe, .sys, dll, .ini, .key, .lnk and .rdp.
5. Next, the malicious code checks other devices connected to the network to complete the encryption process.
6. Finally, a ransom note called ako-readme.txt will appear on the desktop.

Dangerous level

There are two factors that create the dangers of Ako malware:

1. Not limited to individual systems and can spread exponentially across networks.
2. Infecting the entire network, victim organizations and companies were forced to pay large ransom, which could amount to millions of dollars.

Security researchers are still unable to identify the exact distribution technique for this malware.