Abduction Trojans extort money to re-export Gypsy

After a period of lulling, the hacker is returning to the treacherous trick: 'kidnapping' important data inside the computer for ransom from the user. The Trojan Gpcode-AI program silently encrypts data inside the computer's hard drive

After a period of lulling, the hacker is returning to the dangerous tricks: "kidnapping" important data inside the computer for ransom from the user.

The Gpcode-AI Trojan program silently encrypts data inside the infected computer's hard drive before officially requiring users to pay to have the decryption key. This destructive software even includes keyboard tracking, designed to steal victims' bank accounts and credit cards.

More cunning

" *Gpcode-AI belongs to the Synowal family, which is used by hackers to steal passwords and bank information. However, this variation not only successfully completed that job, but it also extorted the user.* " , said Luis Corrons, Technical Director of security firm PandaLabs.

Once installed on the system, Gpcode-AI will encrypt all documents stored on the computer's hard drive and create a file called " **read_me.txt** " (Read it).

Source: ***SecurityLabs*** The content of this file notifies the victim that their computer has been encrypted using

RSA-4096 algorithm. " *If you want to decode yourself, it will take you at least a few years. All your private information in the last 3 months will be gathered and sent back to me* ."

Of course, it is indispensable for hackers to request and bid. " *To decode the data, you need to buy our software. Its price is 300 USD* ".

Below is the email address for the victim to contact. In any case, the perpetrator always holds the hook because they provide the condition that "successful transactions will send the decryption tool" to the victim, and private information will be deleted from the hacker database.

Finally there was a grim line: " *If you do not contact before July 15, 2007, all your sensitive information will be spread widely and you will lose all data* ."

However, according to PandaLabs experts, these threats are just fake. In fact, Gpcode-AI lacks a mechanism to delete all encrypted files and the culprit only uses psychological attacks to force the victim to give them fast money.

Psychological post

However, the eloquent statements about their encryption algorithms were not exaggerated.

" *The algorithms they use are complex. The victim is hard to decipher without his or her software or the help of security experts. However, this Trojan uses a modified version of RC4, not RSA-4096 as they say,* " *said* another Kaspersky Labs expert.

According to experts, victims should not pay the perpetrator because it only encourages them to commit more crimes. Security firms are actively researching technologies that have just blocked the kidnapping software and recovered the locked data.

For example, Kaspersky Labs has developed a decoding algorithm and will soon add it to its antivirus database.

In fact, extortion software is not a new idea. Ransom-A once threatened to delete a file every 30 minutes if the victim refused to pay the hacker.

Another type of malware, Arhiveus-A, forces victims to buy drugs from a website that sells drugs online instead of asking for money directly.

Trong Cam