List of the 3 most dangerous and scary Ransomware viruses

While security solutions to protect us from threats, hackers are increasingly improving, while malicious programs (malware) are also becoming more and more 'cunning'. And one of the recent threats is how to extort money through ransomware.

If you have ever thought that **viruses** and **key-loggers** are deadly threats, don't reaffirm that because there is still a more dangerous threat.

While security solutions to protect us from threats, hackers are increasingly improving, while malicious programs (malware) are also becoming more and more " *cunning* ". And one of the recent threats is how to extort money through ransomware.

Ransomware virus is a type of malware, encrypting and locking all or some files on a user's computer, then asking the user to pay a ransom to unlock.

The severity of the attacks depends on the type of file that ransomware affects. In some cases, it only encrypts some software files that users download from the Internet, but the operating system does not have those features. In other cases, malware can affect the entire hard drive and make the user's computer unusable.

Here are the top 3 most **dangerous and scary Ransomware viruses** ever.

In addition, readers can get more detailed information about what Ransomware or Ransomware is here.

1. Locky Ransomware

Locky was first discovered in February 2016. This ransomware type is usually sent as an email attachment, titled ' *Invoice J-00* '. Email contains text documents that ' *programmed* ' macros in it.

This document states that if the recipient cannot see the invoice, they should allow the macro to run. And as soon as the user activates the macro, all of Locky's required executable files are downloaded and the system is compromised.

The latest version of Locky is quite clever, it can ' *hide* ' the system and can ' *protect itself* ' when users use traditional methods to check the system.

Recently, a new form of mail Locky was discovered that was ' *Receipt of Order - 00* ' instead of the form of invoices.

Read more steps to get rid of the virus * .OSIRIS - Ransomware Locky here.

2. Cerber Ransomware

Cerber is a smart and even malware type. The reason is because it is free software, available for users to download, install and accidentally be attacked by the software without knowing it.

This ransomware type uses two 'shipping' methods:

1. The first method is like Locky, Ceber is also sent as an attachment.When users open this file, it will attack the computer and the user system.

2. The second method is the link to unsubscribe from the phishing list, but 'provide' the user with attachments and ultimately attack the computer and the user system.

When Cerber "infects" and "attacks" your system, it will "hijack" more than 400 file types and encrypt them before requesting ransom. Ransom amounts can be as high as about $ 500 and if you don't pay, you won't be allowed to use your computer.

3. CryptoWall Ransomware

CryptoWall is a ransomware that has many ' *threats* ', threatening the most users. This ransomware does not use any tricks such as email attachments but it relies on vulnerabilities in Java and 'spreads' through malicious ads running on popular sites like Facebook and Disney.

This virus infiltrates the 'silently' computer primarily through the **% APPDATA%** folder and then starts scanning the hard drive to find the files it targets. Once you have a list of encrypted files, it will start your process.

The most notable point of CryptoWall lethal is its ability to run on both 32-bit and 64-bit operating system versions.

However, users can 'reduce' the impact of **CryptoWall** by temporarily replacing the hard drive backup files. Of course this is only a temporary solution, not a permanent solution, but it lasts longer for you to apply other security solutions.

4. Some solutions to protect you from Ransomware attacks

Ransomware virus is increasingly popular and scary. So to protect yourself from Ransomware attacks, you should make regular backups of your computer, update the latest and most important operating system versions, " *don't be fooled* " but click on the Files are sent from unknown sources on email attachments.

In addition, if you do not want to become a victim of Ransomware, readers can refer to some solutions here.

Refer to some of the following articles:

1. What to do to handle "No Internet After Malware Removal" error?

1. How to remove unwanted Toolbar on Chrome, Firefox, IE and Edge browsers?

1. The steps to clean up the virus 'Activate this edition of Windows' attack your Windows computer

Good luck!

You finished reading the article "**List of the 3 most dangerous and scary Ransomware viruses**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
