7 things to know to prevent Conficker worm

Conficker is an extremely dangerous 'infamous' computer worm as well as extremely powerful dispersal in recent times.

Conficker is an extremely dangerous 'infamous' computer worm as well as extremely powerful dispersal in recent times. It is forecasted that on April 1, this worm will be upgraded to use a new communication mechanism with the hacker control server to receive orders to launch a new attack aimed at users .

Here are seven things that security researchers recommend users should know to have an appropriate solution to protect themselves from infection with Conficker.

First , the Conficker worm attacks the PC through a security vulnerability that arises in Windows RPC. This error was closed by Microsoft by emergency patch with code **MS08-67** . If you have installed this patch, you can be assured. If not, it is best to install it as soon as possible.

It can be said that Conficker is a big problem for Windows XP. Windows Vista is technically also a Windows PRC error, but the exploit code is not capable of running on this Windows operating system version. Therefore, the risk of hacked Windows Vista users is not high.

Secondly , Conficker worm spread mainly through online sharing. In addition, the worm has a built-in password cracking technique called "Dictionary attack". This type of attack is based on the most commonly used password

list. These passwords are in turn tested with the system until the correct password is found.

That's why when you find a self-executing file appearing on the shared drive, it means that you were attacked by Conficker. If the system is equipped with a good malware removal software, it will definitely detect Conficker. In case you don't know how to handle it, it's best to call the technical support staff.

Thirdly , derived from the above number two factor, you will find a useful advice that always using a complex password that combines many characters has no obvious meaning. It is best to use a password that combines both letters, numbers and punctuation marks such as dots, commas, questions .

Fourth , the Conficker worm is able to spread through the USB removable drive path. When manually copying to a USB drive, the Conficker worm will automatically create an Autorun file to allow the drive to automatically run every time it is connected to the PC. In fact, it is the Autorun file that controls Conficker to automatically execute infections whenever the USB drive is connected to the PC.

In some cases Conficker is fake as an option to open a Windows Explorer window to view the entire USB drive contents in the standard Windows Autoplay window. But if your PC is equipped with a good anti-malware software, the risk of Conficker can break into the system will be greatly reduced.

Fifth , malicious software is not 100% perfect, but the ability to detect and kill Conficker is something that can be trusted. This is a notorious computer worm, so almost every anti-malware developer knows and understands it. As long as you regularly update malware removal software, the risk of Conficker being attacked will be greatly reduced.

Sixth , Conficker is able to intervene to prevent Windows operating systems and malware from being able to update the latest information and fixes. It's best to take the time to carefully check and update manually for these two core applications. Any important updates should not be left unfinished.

Seventh , a number of Conficker worm detection and killing tools are free.

These tools only work when running on PCs that are infected with Conficker. However, you should note that if you are infected with Conficker, your PC will not be able to access the website of security companies. Which of the following tools are mostly released by security vendors. Therefore, you should use a non-malicious PC to download these tools and run on a PC infected with Conficker. Note that you should disconnect your network when running these tools to prevent other PCs on your network from infecting your PC.

McAfee Stinger

ESet EConfickerRemover

Symantec W32.Downadup Removal Tool

F-Secure F-Downadup

BitDefender single PC & network removal tools

Kaspersky KKiller

Trend Micro

BitDefender

Symantec

CMC Conficker Removal Tool

After using the above tools to successfully find and kill Conficker worm, you should quickly download and install **MS08-67** update because PC infected with Conficker means that you have not installed the patch. this error.

You finished reading the article "**7 things to know to prevent Conficker worm**" 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.
