How to destroy and prevent Conficker

Conficker is a new kind of computer worm that has been around since the beginning of this year but has quickly spread across a wide range of people, making many people 'stand out'. Below, please introduce to readers how to detect, prevent and destroy this dangerous computer worm.

Conficker is a new kind of computer worm that has been around since the beginning of this year but has quickly spread across a wide range of people, making many people 'stand out'. Below, please introduce to readers how to detect, prevent and destroy this dangerous computer worm.

What is Conficker?

In fact, this dangerous computer worm has been around since the end of last year shortly after Microsoft announced a fix with information about an extremely dangerous security bug that is present in almost every version of Windows. Conficker is a malicious code that takes advantage of this security bug to spread and infect users' PCs.

Microsoft itself, when it released the emergency update that fixed the above error, also warned about the malicious code that attacks Windows errors such as Conficker and recommends that users quickly download and

install the fix.

But it seems that the number of users who pay attention to Microsoft's warning is not much. Evidence clearly demonstrates this is the strong outbreak of Conficker in the first months of this year.

The Conficker worm is known by the following specific names: Worm: Win32 / Conficker.A - by the name of Microsoft, Crypt.AVL of AVG, Mal / Conficker-A (Sophos), Trojan.Win32.Pakes.lxf (F-Secure), Trojan.Win32.Pakes.lxf (Kaspersky), W32.Downadup (Symantec), Worm: Win32 / Conficker.B (Microsoft) and Trend Micro's WORM_DOWNAD.A.

The main mode of infection of this computer worm is through USB memory sticks or an infected PC in the network that will automatically infect other PCs on par. Conficker can break into PC because (1) users have downloaded software from unsafe websites on the Internet, (2) users use peer-to-peer file sharing applications and (3)) The user has access to a website used to spread Conficker worm.

The ultimate goal of the Conficker worm is that the hackers behind it have control of the user's PC. They can remotely tell the user's PC to distribute spam, attack websites, steal data or use phishing .

Conficker can infect any version of Windows Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, and Windows XP if users have not installed a Microsoft fix.

Identifying signs of infection with Conficker

There are many signs that PC infection is infected with Conficker. Here are some typical signs of PC infection not only the Conficker worm but also other malicious forms that are prevalent on the Internet.

First, users will see a PC pop up with various pop-up ads. Secondly, the web browser appears a lot of strange things that users have never seen and never downloaded the previous installation.

Thirdly, some settings on the system are changed and the user is unaware. For example, the homepage (homepage) of the browser has been changed to another page and cannot be changed again. Fourth, PC is suddenly running much slower than usual.

Secondly Conficker prevents users from accessing certain directories and does not allow access to websites of security companies such as www.symantec.com, www.mcafee.com . On the system. The system automatically appears several tasks to set a scheduled task schedule.

How to kill Conficker

Once the PC has infected the Conficker worm, it can be said that almost disabled antivirus software cannot completely destroy it. That's why security companies have developed standalone antivirus tools specifically for each type of malicious code. To destroy below please introduce readers Conficker removal tool of Symantec security firm - one of the simplest and easiest to use tools.

Step 1 : Please download this tool **here** . Right-click and select ' **Save Link As** ' with Firefox and ' **Save Target As** ' for Internet Explorer. Users should save this file in an easy-to-find location such as the Desktop screen.

Step 2 : Close all running programs, disconnect the Internet connection completely and disable the System

Restore feature of the system.

Step 3 : Run the downloaded program above.

Step 4 : After the program finishes running, restart the PC. Users should run the program again to make sure the system is clean.

Step 5 : Download and install MS08-067 security update of Microsoft **here** . The easiest is to use the Automatic Updates feature of Windows to update.

Self-protection

If you're lucky to not be infected with the Conficker worm, you should also take measures to protect yourself first, not just the Conficker worm, but also other malicious code.

For Conficker worm, users should quickly download and install **MS08-067** update soon or so. Ideally, users should turn on Automatic Updates auto-update feature so that Windows automatically downloads and installs all necessary updates.

Besides, users should also use anti-virus programs such as Kaspersky, Symantec Norton . to protect the system. Completely disable Windows AutoRun feature by following this **video tutorial** .

In addition, users should also apply safe Internet usage measures such as not opening attachments from unknown emails, so it is a habit to scan USB drives when connecting to the system, so use Windows password protection .