After WannaCry, Petya's 'extortion' malicious code is raging, this is a remedy to prevent

The 'blackmail' malicious code called Petya, which appeared under the new version of Petrraprap, is similar in effect to the WannaCry malicious code, causing the computer system of many multinational companies to be shattered. According to the initial record, these first countries infected with malicious code include Ukraine, Russia, Britain and India.

After WannaCry, a series of 'extortion' malicious codes constantly appear large-scale ransom claims happening globally. Recently, cyber-security agencies have discovered a "blackmail" malicious code called Petya that appears under the new "Petrwrap" version, which is similar in effect to the WannaCry malicious code that caused the computer system. a series of multinational companies were shattered.

"Petrwrap," the new virus of these attacks, is identified by experts as an improved version of Petya, malicious code is the culprit of attacking the global computer system in 2016.

Just as WannaCry used to "rain the wind" for a long time last month, many people suffered. This is a type of malicious code that easily spreads like a plague through malicious links and intentionally overwrites on the device's system startup management file (MBR) to block users. boot.

If infected with malicious code, users will be instructed to make ransom payments to hackers using Bitcoin virtual currency. [What is Bitcoin? Why is Bitcoin not "virtual money"?]

Initially recorded, these first malicious countries include Ukraine, Russia, Britain and India.

According to the Swiss technology agency, Petya malicious code also attacks the SMB service vulnerability on Windows-based computers. There are currently no Swiss companies affected by this malicious code, however, the computer system of the Ukrainian Government, together with some banks of Ukraine and Russia, supermarkets Auchan giant and Boryspol airport the largest of Ukraine; Nivea cosmetics company and chocolate maker Alpen Gold in Russia have been infected with malicious code in a new network attack.

Here are a few companies that have been "extorted" from Petya

Russia's Rosneft has switched to a redundant network for production processes, after being attacked by malicious code.

Danish shipping company Maersk, French industrial corporation Saint-Gobain is also among the major companies attacked. Its operations have been stalled at many locations.

WPP - Britain's largest advertising agency also said that the computer system at many of its agents was attacked and now network experts are evaluating the situation to make the most appropriate measures to overcome.

Petya affected operations at the Chernobyl nuclear power plant, forcing experts to switch to manual radiation monitoring. Small devices like cash registers or ATMs are also infected with new ransomware.

In the United States, ransomware Petya, the attacked companies including Merck Pharmaceuticals, a hospital in Pittsburgh and the US office of DLA Piper law firm, have also appeared.

As of the morning of June 28, 2017, according to Vietnam time, thousands of cases of Petya infection have been recorded, equivalent to the level of WannaCry coverage in the early hours.

How Petya Ransomware spread so fast?

Symantec confirmed that Petya exploited the EternalBlue vulnerability of SMBv1, like WannaCry, and took advantage of unpatched Windows machines.

"Petya succeeds in spreading because it combines both client-side attacks (CVE-2017-0199) and a network-based threat (MS17-010)", HackerFantastic security researcher (who has Turn the WannaCry solution) on Twitter.

EternalBlue is a Windows SMB vulnerability revealed by the infamous hacker group Shadow Brokers in the April data leak, which claimed to have stolen it from US intelligence agency NSA along with other Windows vulnerabilities.

Microsoft has patched vulnerabilities for all versions of the Windows operating system, but many users are still vulnerable to patching, and a series of malware variants are exploiting this vulnerability. to distribute ransomware and dig digital money. [Microsoft released emergency patch to prevent ransomware from attacking]

Just three days ago, we posted the latest WannaCry attack on Honda Motor Company and about 55 speed surveillance cameras and traffic lights in Japan and Australia. [WannaCry is not dead, it just attacked Honda and Australia's traffic camera system]

Well, quite surprisingly, even after learning about the WannaCry issue for a long time, large corporations and companies still haven't implemented appropriate security measures to protect against such threats. .

How to protect yourself from Ransomware attacks

What to do now? Again, make sure to install the EternalBlue patch (MS17-010) and disable the unsafe, 30-year-old SMBv1 file sharing protocol on Windows systems and servers.

How to do it: Type **Turn Windows features** into **Start Menu** and click on **Turn Windows features on or off** . Scroll down to **SMB 1.0 / CIFS File Sharing Support** and uncheck the box.

Since Petya Ransomware also takes advantage of WMIC and PSEXEC tools to infect fully patched Windows computers, you should also turn off WMIC (Windows Management Instrumentation Command-line).

Prevent infection and Kill-Switch Petya

The researchers discovered Petya encrypted the system after restarting the computer. So if the computer / system is infected with Petya and try to reboot, don't turn it on, turn off the power.

"If the machine restarts and you see this message, turn it off immediately! This is the encryption process, if you don't turn on the power, the files will be fine . " HackerFantastic wrote. *"Use a LiveCD disc or external device to recover files"* .

Picture 2 of After WannaCry, Petya's 'extortion' malicious code is raging, this is a remedy to prevent

PT Security, a network security company based in the UK and Amit Serper of Cybereason, discovered a Kill-Switch tool for Petya ransomware tool. According to a tweet, the company advised users to create a " *C: Windowsperfc* " file and set it to be a read-only file to prevent ransomware infection.

You can download the file here: *https://download.bleepingcomputer.com/bats/nopetyavac.bat*

If you want to do it manually, you can do it in the following simple way. For more knowledgeable users about computers can find better ways to protect themselves instead of just the following:

First, display the file extension. On Windows 7 go to **Folder Options> View>** uncheck the **Hide extensions for known file types** , from Windows 8 and above, open any folder> **View** > check the **File name extensions** .

Open **C: Windows** , scroll down until you find **notepad.exe** , copy this file and paste it directly into the open folder (ctrl + c, ctrl + v), click **Continue** in the window that appears, you will see appears **notepad** file - **Copy.exe,** select file, press F2 (to rename, click left mouse> Rename) and rename to **perfc** > **Enter** > **Yes** to

confirm rename.

To convert this perfc file to read-only, right-click on the file> **Properties** > tick to **Read-only** > **Apply** > **OK** .

The Properties window will close, and now your computer may be immune to Petya.

To protect yourself against any ransomware infection, you should be careful before unwanted files and documents are emailed and should not click inside links unless the source is verified to be secure. all.

To ensure your valuable data is secure, perform system backups and save them on an external storage device that is not normally connected to a computer.

Finally, make sure you are installing a reliable and effective set of antivirus software on your system and updating it regularly. Most importantly, always browse the Internet safely.

You finished reading the article "**After WannaCry, Petya's 'extortion' malicious code is raging, this is a remedy to prevent**" 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.
