Windows SMB users should close some ports to prevent WannaCry

Will ransomware WannaCry come back to attack us? Try closing some of the ports below to prevent ransomware from attacking!

In early May 2017, terrorists who attacked Arianna Grande concert in Manchester and the world became victims of the WannaCry ransomware attack.

WannaCry has infected more than 230,000 computers in 150 countries. It made the British medical service deadlock, causing a blockage of telephone networks in Spain and loss of railroads in Germany. Overall, this is one of the worst cyber attacks the world has to go through.

Now, after 3 months, errors or holes still make ransomware easily spread.

Without super-high technology, WannaCry can easily infect using EternalBlue. It is an exploit developed by NSA of the SMB protocol (Windows Server Message Block).

Microsoft has created patches for millions of computers, including unsupported operating systems like Windows XP. Theoretically, these patches closed the EternalBlue SMB vulnerabilities.

1. Prevent WannaCry variants by turning off this Windows 10 installation
2. How to recover data encrypted by WannaCry malicious code

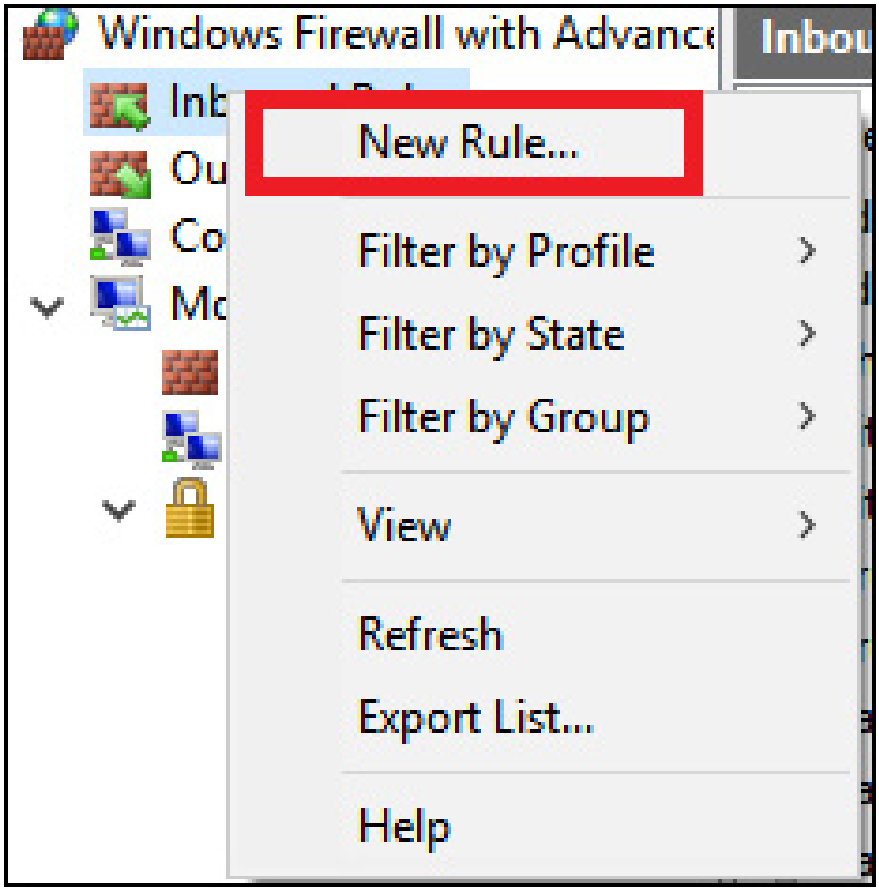
However, in reality, it seems they don't work very well. At the annual DEF CON conference last July, security researchers found another security hole. This vulnerability is called SMBLoris and is a remote denial of service attack. It can crash a computer or a server and only use no more than 20 lines of code.

Microsoft believes that this vulnerability should be automatically blocked by the firewall.

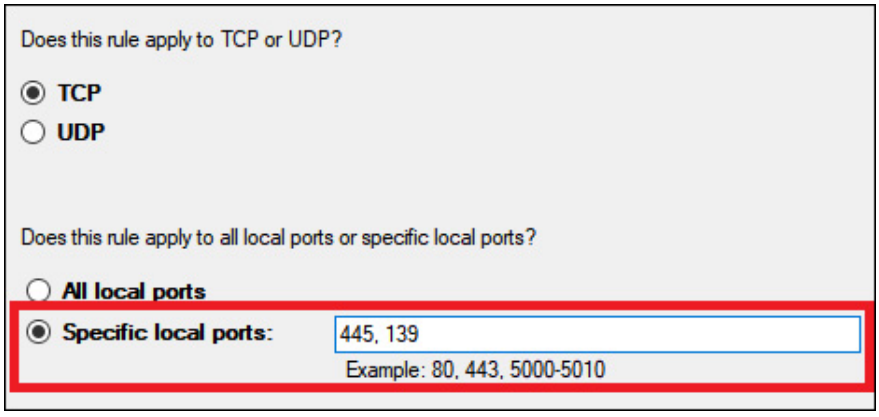
So how to protect yourself from ransomware?

SMBLoris affects all SMB types, meaning you must remove SMBv1 from the system completely. You need to block all incoming connections on ports 445 and 139.

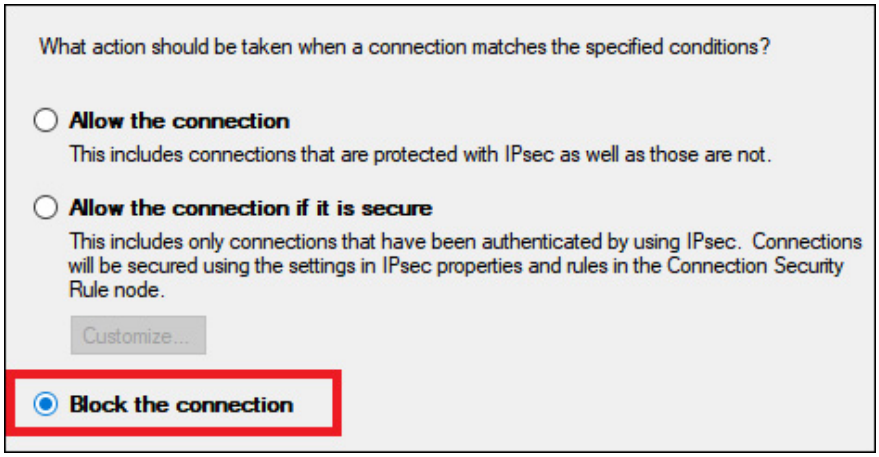
You can block ports on the router but there is an easier way - using the **Windows Firewall** tool. Visit the **Control Panel> Windows Firewall> Advanced Settings** , right-click on **Inbound Rules** and select **New Rule** .



On the next screen, select **Port,** then select **Next.** Now, you need to select **Specific Local Ports** . Enter 445, 139 in the box. Click **Next** again.



Finally, select **Block the Connection** , name the new rule and click **Finish.**



If you want to protect your computer from ransomware, follow the steps above!

You finished reading the article "**Windows SMB users should close some ports to prevent WannaCry**" 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.
