What is WannaCry, how to prevent Wanna cry for computers

The Wannacry virus has made waves and caused a lot of damage to computer users. If you still don't know what WannaCry is and how to prevent Wannacry on your computer, please follow the article below and Find the answer for yourself.

While Windows users have to face many types of viruses and Ransomware, those who are using smartphones, especially the Android operating system, are now facing the risk of being infected with CopyCat malware from applications of unknown source. Basically, because you do not download applications from Google Play, your device will easily be infected with CopyCat malware at any time. Once infected with CopyCat malware, you will lose control of your phone and all data. will be stolen and distributed.

The latest information that Taimienphi received is that there is a new malicious code called Petya Ransomware, threatening users' data, to know what Petya Ransomware is and how to detect it, how to prevent it. , readers can refer to the **Petya Ransomware** article here.

In recent days, not only the online press has reported information but even on television has warned computer users about a type of ransomware-like malicious code **with** the name **Wanna Crypt (also known as WannaCry or Wanna Cry). .** This is a type of spyware that accesses the user's computer and then re-encrypts the infected person's data. You will then be asked to spend a certain amount of money if you want to get these files back.

Most recently, CMC announced the release of a tool with the integration of artificial intelligence technology **that can prevent data encryption of all malicious code** , including WannaCry, a tool named **CryptoShield** by CMC . You can download it to try it out, hopefully it will be as useful as advertised. Of course, if you have some technical knowledge, protecting your computers will be the safest, let's see the necessary steps. Please do this to **prevent WannaCry** immediately.

Currently, the warning level of Wanna Crypt Ransomware is very high and users should pay attention when using the Internet to avoid being infected by Wanna Crypt because it can penetrate your system. First, you should check whether your computer is infected with WannaCry malware or not by checking WannaCry with two tools: BKAV CheckWanCry and VNIST Scanner.

Currently, there are some software that can do it to kill Ransomware, however, there is no such thing as Wanna Crypt, so readers should be careful with unfamiliar links or offers of any software that can kill Ransomware. ability to remove Wanna Crypt Ransomware and wait for updated information from TipsMake.

While everyone was still struggling with **WannaCry** , another form of malware was distributed around the world called EternalRocks - this is a form of malware that experts consider to be many times more dangerous than WannaCry, even From now on, please use measures to prevent **EternalRocks** right away. Below, we will learn about the WannaCry virus.

What is Wanna Cry ransomware?

To learn about Wanna Crypt Ransomware let's first talk about Ransomware

- **Ransomware** is a form of malicious software (malware) that encrypts multimedia files, documents and other files on the target computer and users only have access to these files when accepting the "ransom". " of the attacker. And for more details about Ransomware as well as its history, if readers are interested, please see the article about **what Ransomware is** that Taimienphi introduced.

- **Wanna Crypt** , also known as Wanna Cry, was recently released but the level of spread is very dangerous. 90 countries have been confirmed to be infected with this type of Wanna Crypt Ransomware, including Vietnam. Wanna Crypt has the ability to infiltrate all computers on the same network through a vulnerability called Internal Blue, without users even having to click on any links or attachments to be infected. With just one infected computer in the system, all are at risk of being infected.

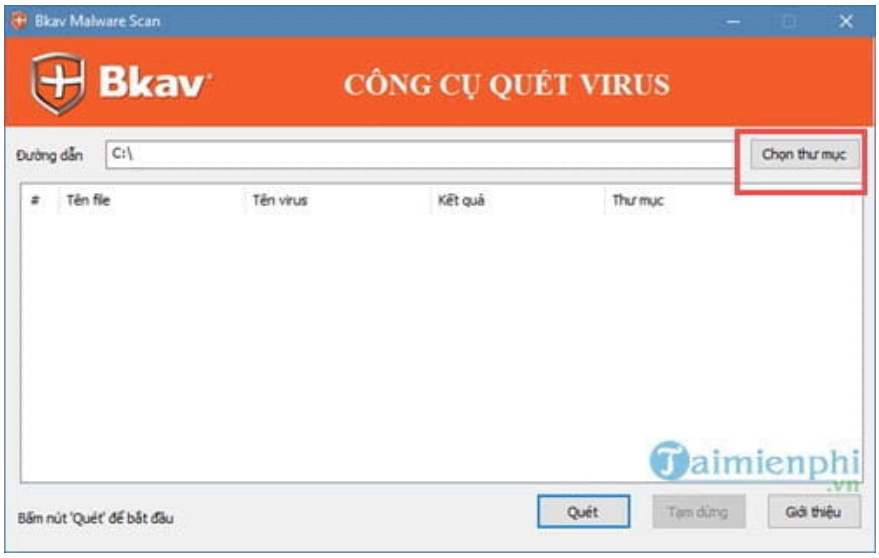
In addition, Wanna Crypt only allows you a few hours to pay the ransom if you do not want to lose all your data. The current way to delete Wannacry is available but not thorough, so if you refer to ways to delete Wannacry

from your computer, it will only partially delete it.

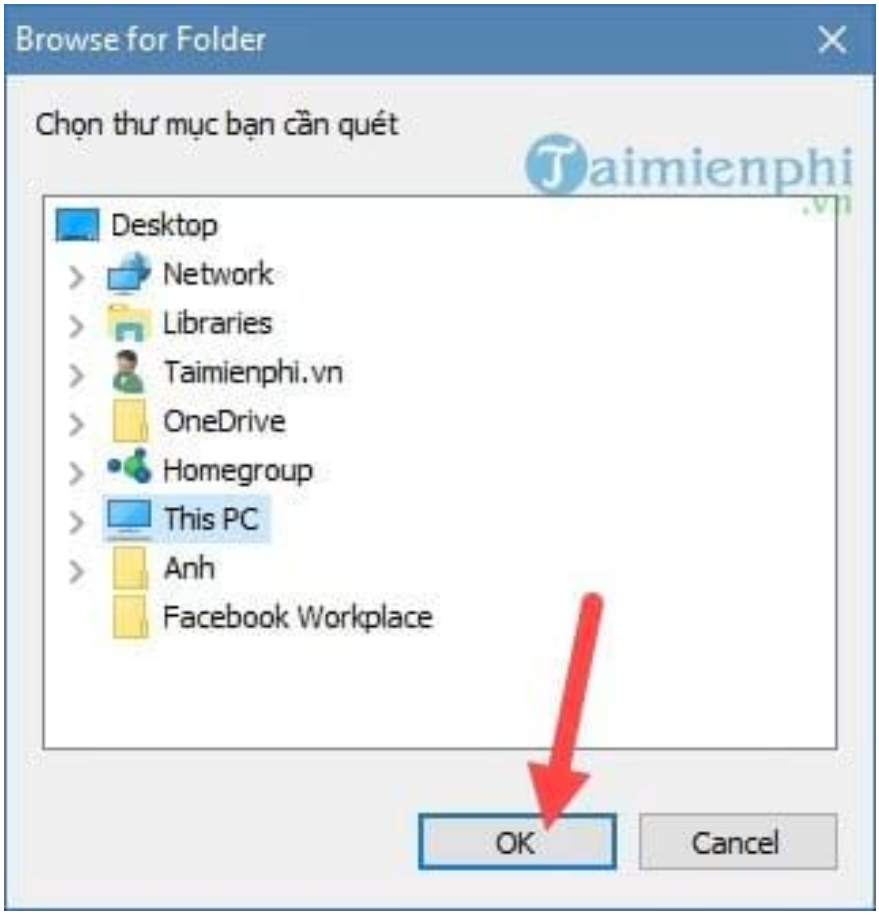
How to check WannaCry in computer

In fact, it is not possible to check whether Wanna Crypt is in your computer or not, but you can check if your computer has the Eternal Blue vulnerability and patch it to avoid being infected with Wanna Crypt Ransomware. Recently, BKAV has just released an application called Check WanCry that allows users to check computers for the Eternal Blue vulnerability. Readers can download **BKAV CheckWanCry** here.

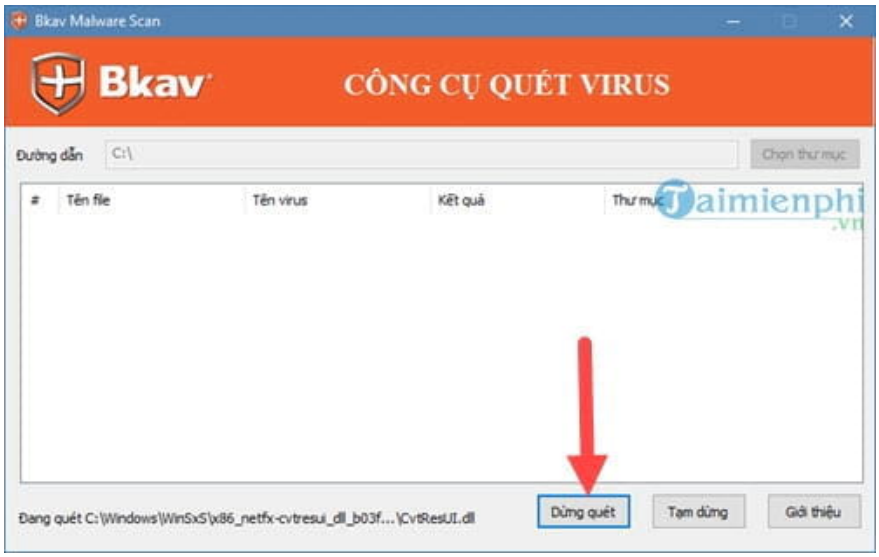
Step 1: After downloading Check WanCry to your computer, you just need to open it, select a folder for each drive and you can scan immediately.



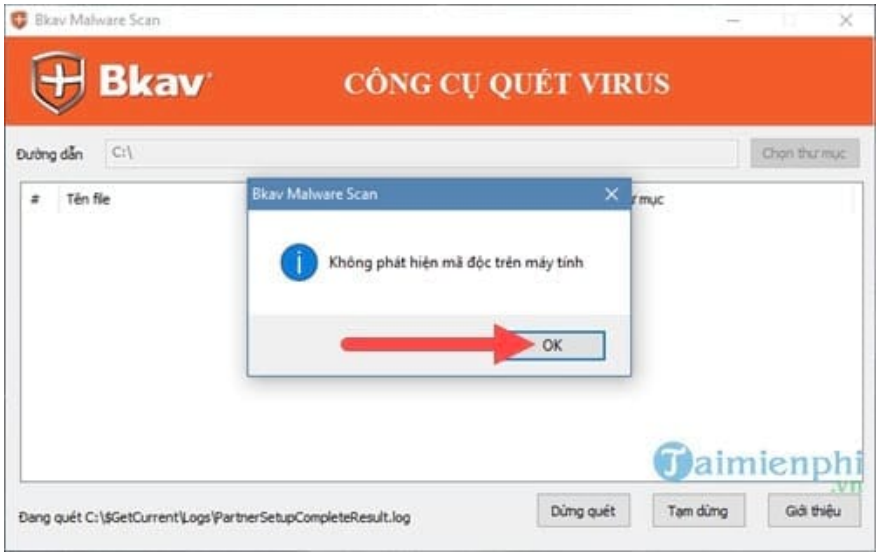
Step 2: Click **the drive option to check** the Wanna Crypt in the computer for the Eternal Blue error.



Step 3: Click **Scan** to let the software system start scanning.

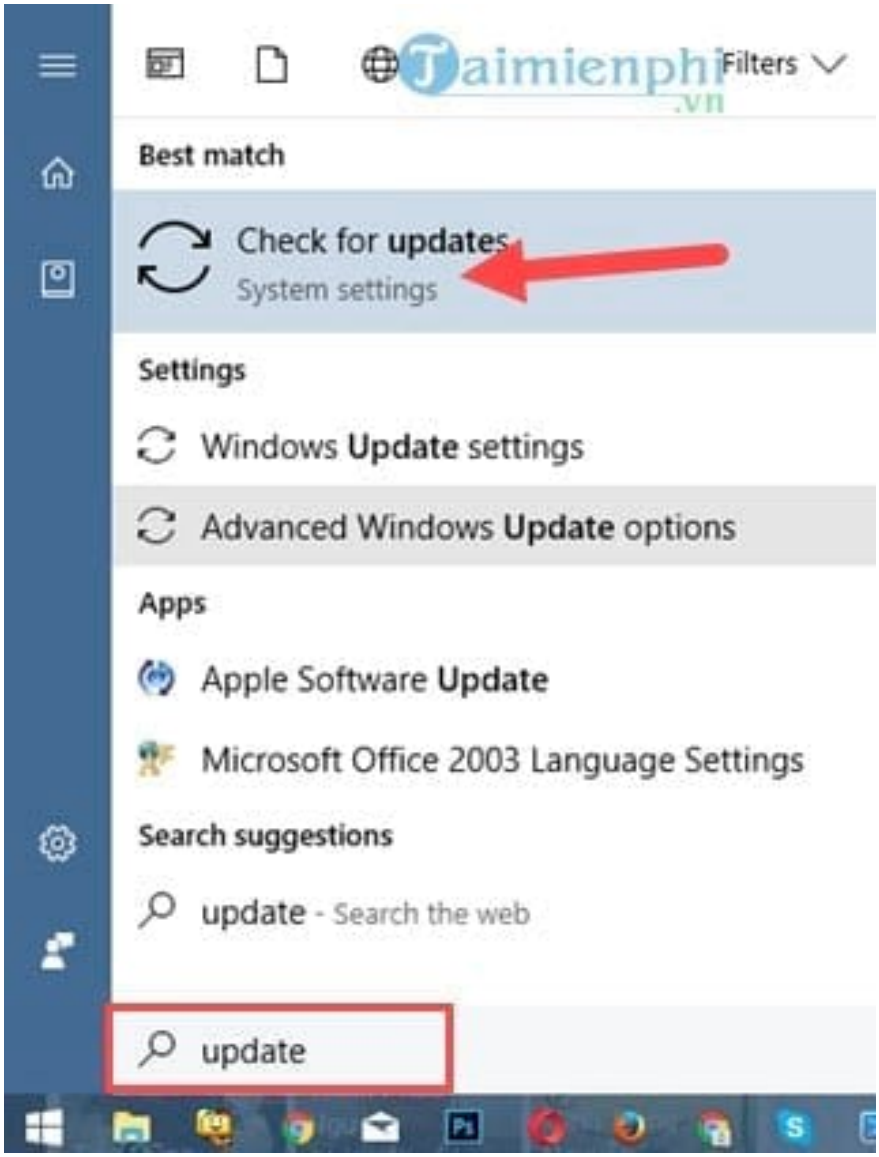


Step 4: If the computer has the message " **no malicious code detected on the computer** ", it means your computer is safe, in addition the computer has been updated with the Eternal blue patched version.



Step 5: But if you receive the following message, don't worry and turn it off and proceed to update Windows.

Step 6: Currently, Microsoft is also releasing the above patches. Now open **the Start Menu** , type " **update** " and go to **Check for update** to Windows Update.



Step 7: Next, wait for the system to check and then automatically download the update to your computer right away. This is a free update so anyone can upgrade.

How to avoid Wanna Cry on your computer

There have been many unfortunate cases that have happened. If you had previously prevented WannaCry with the world's leading anti-virus software such as BKAV, KIS. then your data would have been safe.

- Testing only helps you detect Eternal Blue errors and use Windows Updates to patch them.
- Currently there is no way to remove Ransomware Wanna Cry. Users should be careful not to click on any content related to removing Ransomware Wanna Crypt.
- Do not click on strange links, links sent on Facebook or any strange emails sent.
- Do not download strange files or email attachments if the source cannot be clearly identified.
- Do not access the dark web or poorly secured websites because it can cause you to be infected
- Remove the Tor browser used on the system computer, do not download files
- Back up important data a USB device, portable hard drive to prevent unfortunate cases.
- Regularly update the latest patches and upgrades from Windows.

Hopefully through the above article you will learn more about Wanna Crypt Ransomware as well as check Wanna Crypt in your computer, thereby finding preventive measures. This is an extremely dangerous type of malware. You should choose and install the best anti-virus software to better protect your computer. Refer to the list of anti-virus software for the best choice.