All about WannaCry, Ransomware has been confusing for the past few days

The article will provide some knowledge about WannaCry and the most important security tips you should take and share with your acquaintances to prevent computers from ransomware WannaCry.

WannaCry Ransomware is probably not new to readers, because it has begun to spread from May 12, shocking the Internet world and attacking more than 200,000 Windows-based computers in just a few days. weekend.

After reading this article, you will be more cautious in using computers and can save yourself from WannaCry's attack, as well as other future network attacks.

Because the ransomware attack with this tremendous spread is not the first attack nor the last time that threatens users worldwide, so prevention is always the key to protect prevent threats from this malicious software.

In this article, we will provide some of the most important security tips you should take and share with your acquaintances.

1. How to close the port / Port 445 on Windows 2000 / XP / 2003 to Windows 10 to prevent ransomware WannaCry
2. Download the free WannaCry malware checker now
3. How to remove / fix ransomware WannaCry
4. How to identify WannaCry malicious code from Vietnam Computer Emergency Response Center (VNCERT)

What is Ransomware and why is WannaCry becoming more and more dangerous?

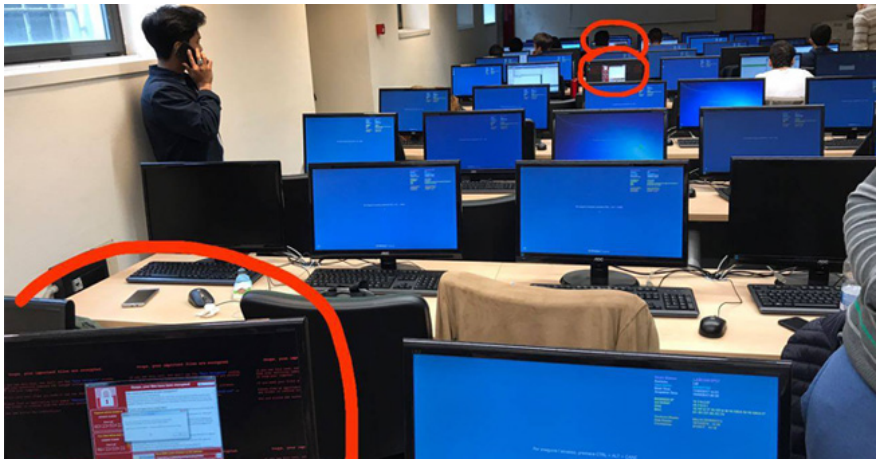
For those of you who don't know, Ransomware is a computer virus that often spreads through email spam mailboxes and malicious download links. Ransomware is specially designed to lock files on the computer until the victim pays the ransom as required, usually 300 to 500 USD in the form of Bitcoin (decentralized digital currency).

However, what makes WannaCry so special is its ability to spread itself without even needing a user to click on any link or file.

Ransomware WannaCry, also known as Wanna Decryptor, promotes the exploitation of the Windows SMB vulnerability, also known as EternalBlue, to allow hackers to attack computers running remote Microsoft Windows operating systems.

Once infected, WannaCry also scans for unpatched computers on the same LAN as well as scanning random servers on the wider Internet to spread the virus quickly.

So what happened?



From last Friday, we also talked about how this malware first appeared and attacked many computer systems in many hospitals around the world. Finally, these hospitals are forced to close their entire IT systems, refuse appointments with patients and cancel all other activities.

Shortly thereafter, this cyber attack also made many organizations powerless.

The following article will tell readers what has happened so far:

Day 1 : OutCry - WannaCry targets more than 90,000 computers in 99 countries.

Day 2 : Security researchers have succeeded in figuring out how to reduce the rate of infection of the virus, and at the same time, Microsoft has released an emergency patch update for unsupported versions of Windows. support.

Day 3 : New variants of WannaCry with remote control technology have been discovered and are said to be difficult to prevent, at least in the next few weeks. The more dangerous WannaCry version 2.0 has appeared

Didn't Cyber ??attack end?

Of course not.

That's just the beginning. Researchers have discovered this new version of ransomware, called WannaCry 2.0. There is currently no way to stop them.

Even worse, the WannaCry variants are created by someone other than the hacker behind the first ransomware.

People speculate that other organized hacker gangs, as well as kiddie scripts will take the momentum from this attack and create other similar malicious ransomware.

Who is behind WannaCry and why does this work?

Mr. Europol, the European police agency, said: "This attack is at an unprecedented level of danger and will require an international investigation to verify the culprit."

Why do they steal information from hundreds of thousands of computers around the world? It is simply to blackmail users infected with the virus.

By observing the infection rate, it seems that criminals responsible for this ridiculous attack have earned a lot of money up to the present time. The WannaCry attackers have received 1,71 payment accounts and collected 27,96968763 BTC (equivalent to 47,510.71 USD).

How to protect your computer from WannaCry Ransomware?

Here are some simple tips you should take, because most viruses that get into your computer are because users lack basic security measures:

1. Always install security updates

If you are using any version of Windows, except Windows 10, turn on the SMB protocol and make sure your computer is always updated automatically from Microsoft.

2. Fix the SMB vulnerability

When WannaCry started exploiting a critical vulnerability in SMB code (CVE-2017-0148), Microsoft distributed the patch (MS17-010) in March, making sure your system is installed with versions. patch it.

In addition, Microsoft has been very generous to users during this difficult time, which is to release SMB patches (downloaded from here) for unsupported versions of Windows, including Windows XP, Vista , 8, Server 2003 and 2008.

Note : If you are using Windows 10, your computer is very difficult to fail the SMB vulnerability.

3. Disable SMB

Even if you have installed the patches, you should disable the Server Message Block version 1 (SMBv1) - which is enabled by default on Windows, to prevent attacks from ransomware WannaCry.

Here are simple steps to turn off SMBv1:

1. Go to Windows **Control Panel** and open **Programs** .
2. Open **Features** in Programs and click **Turn Windows Features on and off** .
3. Scroll down to find **SMB 1.0 / CIFS File Sharing Support** and uncheck the box next to it.
4. Then click **OK** , close Control Panel and restart the computer.

4. Activate the Firewall feature and lock SMB ports

Always turn on the firewall. If you need to enable SMBv1, you only need to change the firewall configuration to block access to SMB ports over the Internet. The protocol works on TCP ports 137, 139 and 445 and through ports UDP 137 and 138.

5. Use an antivirus program

An never-out-of-date solution to combat such threats is to install good antivirus software from a reputable provider and the software must always be up-to-date.

Most antivirus program providers add detection capabilities to block WannaCry, as well as prevent secret installations from malicious applications on the computer screen.

6. Stay alert before emails, websites and apps

Unlike WannaCry, most ransomware spread through phishing emails, malicious advertisements on third-party websites and applications or programs.

Therefore, you should always be cautious when opening unwanted documents on email and clicking on the link within it, unless you verify the source to protect the computer and fight the infection of ransomware.

In addition, you may not download any application from third party sources and must read reviews before installing applications from official stores.

7. Regularly backup files

To store important documents and files, it is best to keep a habit of backing up files, saving extra copies outside your computer so that if ransomware infects a computer, it cannot encrypt the copies. Your backup.

8. Always update knowledge

Every day there are announcements about cyberattacks, vulnerabilities in popular software and services, such as Android, iOS, Windows, Linux and Mac computers.

Therefore, this is the time when users using domain names should keep track of the activities happening in the network world, which not only helps users always have up-to-date knowledge but also prevents sophisticated attack of news. hackers.

What to do if WannaCry infects your computer?

If ransomware WannaCry infects your computer, you cannot decrypt the file until you pay the ransom to the hacker and get the secret key to open your file.

Never pay a ransom:

Individuals and organizations infected with the virus will decide whether to pay the ransom, depending on the importance of the files locked by ransomware.

However, before making the final decision, remember: there is no guarantee that after paying the ransom, you will regain control of the files.

Moreover, paying a ransom will encourage cyber criminals to offer similar threats and blackmail larger objects.

Therefore, users should not pay for hackers.

Who is responsible for the WannaCry attack?

Is it because Microsoft has created an operating system that has many vulnerabilities?

Or by the NSA (US national security agency) - who discovered a serious SMB vulnerability, indirectly enabling WannaCry and other public attacks by not disclosing information to Microsoft?

Or by Shadow Broker hacker group - who have found a way to hack NSA server, instead of telling Microsoft they openly hack tool and zero-day vulnerabilities.

Or by Windows users themselves - who do not install patches on the system or are still using unsupported versions of Windows?

I myself do not know who is responsible for this attack, but in my opinion, they all have similar responsibilities.

Microsoft blames NSA / CIA for the attack on WannaCry

Microsoft has criticized the US government for creating power conditions for cyberattacks like WannaCry. They did not disclose software vulnerabilities to their respective providers and kept the information confidential for their benefit - such as global cyber espionage.

In a blog post posted on Sunday, Microsoft president Brad Smith condemned the US security agency's unethical practices, blaming WannaCry's extensive damage from the NSA, CIA and Other intelligence agencies did not disclose zero-day vulnerabilities and let hackers steal them.

Mr. Smith said: "This is an emerging model in 2017. We saw the vulnerability hosted by the CIA on WikiLeaks, and now, the vulnerability stolen from NSA has affected customers worldwide. . "

The statement also publicly confirmed that hacking tools and vulnerabilities were leaked by Shadow Broker of Equation Group - a famous hacker group of NSA.

You should thank the security experts

The explosion of ransomware WannaCry on Friday night infested at least 30,000 computers worldwide. At that time, no one knew what was going on and how those ransomware could spread so quickly.

Over the past three days, network security experts and companies are continuing to work hard all night to analyze malware patterns to find ways to prevent this massive attack.

Photo: Thanks from a Tweet account to experts

I would like to mention some experts here who need to be thankful because they saved millions of computers from being attacked:

MalwareTech - an experienced software hunter who is only 22 years old. He was the first to find a kill-switch to prevent attacks from ransomware.

Matthieu Suiche , a security researcher, discovered the second conversion domain in a WannaCry variant and prevented nearly 10,000 computers from being hacked.

Costin Raiu - Kaspersky Lab's security researcher, who first discovered many variants of WannaCry, was created by many different hacker groups and was unable to prevent it.

These are just typical experts, besides Benjamin Delpy, Mohamed Saher, x0rz, Malwarebytes, MalwareUnicorn and many others.

The damage that ransomware WannaCry caused was terrible even though the parties tried to stop it. Hope the article brings you useful information about WannaCry.