What is Wannacry? How to detect and prevent it effectively

WannaCry is one of the most famous ransomware attacks in the history of cybersecurity, causing a massive attack in May 2017.

WannaCry is one of the most famous ransomware in the history of cyber security, causing a large-scale attack in May 2017. With the ability to spread quickly and encrypt user data, WannaCry has affected hundreds of thousands of computers worldwide, from individuals to large organizations. Let's learn more about this cyber attack with ***TipsMake in the article below.***

Basics of Worm

A computer worm, also known as a computer worm, is a type of malicious software that can replicate itself and spread to other computers without human intervention. They often exploit security vulnerabilities in systems or network protocols to penetrate and spread, causing serious damage to systems and networks.

Features of Computer Worm:

? Self-propagating: Worms have the ability to self-replicate and spread across a network without user interaction. This makes them very fast at spreading, especially within local area networks (LANs) or over the Internet.

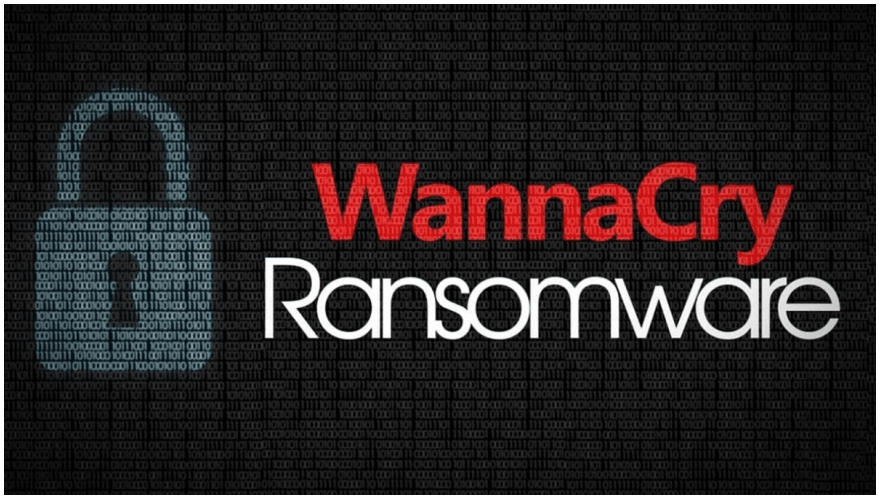
? Impact on system resources: When worms invade a computer, they often consume a lot of system resources, causing the computer to slow down or become unusable.

? Security risk: Worms can be disguised as harmless files or links to lure users into clicking, thereby infecting them with malware immediately.

So what is the Wannacry Ransomware attack?

WannaCry was a major ransomware attack that occurred in May 2017, affecting more than 200,000 computers in more than 150 countries. The cyberattack primarily targeted computers running unpatched versions of the Microsoft Windows operating system, exploiting a vulnerability known as EternalBlue, which was developed by the United States National Security Agency (NSA) and leaked by a hacker group known as The Shadow Brokers shortly before the attack.

The WannaCry attack had a far-reaching impact on many sectors, especially healthcare. The UK National Health Service (NHS) was particularly hard hit, with many services disrupted and ambulances diverted due to compromised systems. In total, the attack caused damage estimated to be in the hundreds of millions to billions of dollars globally.



What is Wannacry?

How Wannacry works

When WannaCry infects a computer, it encrypts all the data files on the hard drive using strong encryption algorithms such as AES-128 and RSA-2048. Each encrypted file will have the extension ".WCRY", and the victim cannot access these files without the decryption key. The malware will generate a pair of RSA-2048 keys, in which the public key is used to encrypt the AES-128 key, and the private key is kept by the hacker.

After successful encryption, WannaCry displays a message asking victims to pay a ransom in Bitcoin, typically around $300, with a countdown timer. If payment is not made within three days, the ransom will double, and after seven days, the data will be completely deleted.

WannaCry spreads mainly through two methods:

? Exploiting the EternalBlue vulnerability: WannaCry takes advantage of the MS17-010 security vulnerability in the Windows SMBv1 protocol, allowing remote code execution without user interaction. This vulnerability was discovered by the US National Security Agency (NSA) and later made public by the Shadow Brokers hacker

group.

? Spread via email: In addition to exploiting vulnerabilities, WannaCry can also spread through sending emails containing malicious attachments or through websites containing malicious code.

Who created Wannacry?

Up to now, there is still no exact information about who created Wannacry, however there are 2 groups of suspects considered to be the culprits who created Wannacry:

? Shadow Brokers hacker group: WannaCry was developed based on the security vulnerability MS17-010, also known as EternalBlue, discovered by the US National Security Agency (NSA). The Shadow Brokers hacker group leaked this exploit in April 2017.

? North Korea suspicions: Several cybersecurity experts, including companies like Kaspersky and Symantec, have pointed out that the malware bears similarities to previous attacks by the Lazarus hacker group, which is believed to be linked to North Korea. They say the use of similar source code suggests the group may be behind the WannaCry attack.

While there is a lot of evidence pointing to North Korea, some others have suggested that the accusation may simply be part of a Western propaganda campaign to cover up their own responsibility for exposing the security breach.

Consequences of computer infected with Ransomware Wannacry

The WannaCry ransomware attack has had devastating consequences across the globe, affecting hundreds of thousands of computers and many large organizations. Here are some of the main consequences of the attack:

Impact on organizations and infrastructure

Wannacry, when it penetrated computer systems, caused many consequences not only for the information technology industry but also negatively impacted the medical and transportation networks.

? Healthcare network: The National Health Service (NHS) system in the UK was paralyzed, leading to the refusal of treatment for many patients. About 48 organizations in this network were affected, causing major disruption in healthcare.

? Transport: In Germany, malware disrupted rail operations, affecting train schedules and ticket vending machines. Similarly, in Spain, telecommunications company Telefonica was also attacked, disrupting services.

? Businesses: Many large companies such as FedEx and Renault were also affected, leading to production and business shutdowns.

Economic damage

Organizations have to spend a large sum of money to restore their systems and data. The ransom demanded ranges from $300 to $600 per computer. If the ransom is not paid within the specified time, the data will be permanently deleted, resulting in the loss of important information for organizations.

Number of infected computers

As of May 15, 2017, approximately 230,000 computers in 150 countries were infected with this malware. Russia was the country that suffered the most damage, with more than 1,000 computers attacked. Vietnam was also on the list of affected countries, with more than 1,900 computers infected during the initial period of the attack.

How to detect computer infected with Wannacry

To detect a computer infected with WannaCry malware, users need to pay attention to some signs and perform the following checks:

? Ransom note: When a computer is infected with WannaCry, a ransom note will appear on the screen demanding payment to decrypt the data. This notice usually includes a countdown timer and specific instructions on how to pay in Bitcoin.

? File encryption: WannaCry will encrypt most of the files on your computer, especially text files. Encrypted files will have the extension ".WCRY" and users will not be able to open them without the decryption key.

? Slow computer performance: If your computer is running slower than usual or is behaving unusually, this could be a sign of a malware infection.

How to prevent Ransomware Wannacry?

To prevent WannaCry ransomware, users and organizations need to take some important security measures to minimize the risk of being attacked. Here are some preventive measures for individuals, businesses and organizations:

For individuals

? Update your Windows operating system: Make sure your operating system is updated with the latest patches, especially the patch for the EternalBlue vulnerability that WannaCry exploited.

? Use antivirus software: Install and maintain licensed antivirus software, such as Bkav Pro, to automatically detect and block malware.

? Back up data regularly: Make regular backups of important data on your computer so that it can be recovered if attacked.

? Be careful with emails and links: Don't open attachments or click on links from unknown sources, especially from emails or social media.

? Use a sandbox: Only open text files received from the Internet in a secure environment (sandbox) to avoid the risk of infection.

For businesses and organizations

? Check and block network ports: Temporarily block ports 445, 137, 138, 139 on the server to prevent the spread of malware.

? Implement security solutions: Use solutions such as Firewall, IDS/IPS, and SIEM to monitor and protect systems from threats.

? Create backups for virtual servers: Create snapshots for virtual servers so they can be restored quickly in case of an attack.

? Employee information security training: Provide training to employees on how to recognize and handle ransomware threats.

? Monitor updates from security vendors: Make sure all software and systems are updated with the latest patches from the vendor.

Is Wannacry still a concern?

According to security experts, many computers have not yet been patched for the EternalBlue vulnerability exploited by WannaCry. In Vietnam, about 52% of computers (equivalent to nearly 4 million computers) could still be attacked if hackers decide to expand their operations.

WannaCry mainly spreads via the SMB (Server Message Block) protocol on Windows operating systems that have not been updated. It can also be transmitted via phishing emails or malicious websites. If not fixed, the risk of spreading this malware is still very high.

While attention to WannaCry has decreased over time, the lack of updates and security across many systems could lead to new attacks in the future.

Conclude

WannaCry remains a significant concern without proper precautions. Maintaining security updates and raising information security awareness are important to minimize the risk of this malware.