ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202201_5(1).0019

Thoughts on Vulnerability Security by Ransomware Virus

Xin Zhang[1], Xiaoling Xiao[2, a]

[1]School of computer Science, Yangtze University, Jingzhou, 434023, China

[2]School of computer Science, Yangtze University, Jingzhou, 434023, China

[a]xxl@yangtzeu.edu.cn

Abstract

At the beginning of the online world was born, and successively with the virus was born. Recently called the eternal blue blackmail virus appears in people's field of vision, to give people a wake-up call, especially the intervention of the national security agency and the equation group, make the virus more damaging in this paper, starting from the worm was introduced in detail the characteristics of the eternal blue effects and preventive measures, and then from virus attack way to talk about the thinking about vulnerability safety as well as how to effectively prevent network virus invasion.

Keywords

Eternal Blue; Windows RPC; Firewall.

1. Introduction

In recent years, with the continuous development of information technology, network security risks and threats have become increasingly prominent. In the past, when companies faced risks and threats, it was common practice to devote more "energies" to the Internet security protection of enterprises with a higher degree of security risk, while ignoring the company's internal office network, research and production network, and industrial control systems (Collectively referred to as the "enterprise local area network"), in the traditional conception of the enterprise, it is considered that the enterprise local area network and the Internet are physically isolated and relatively secure. Therefore， in addition to the compliance content that complies with relevant national requirements, corporate LANs have not targeted security risk prevention and security hardening. However, in actual work, it was found that once a network attack hits, the security protection capabilities of corporate LAN computers will Worse than a business-connected computer. Coupled with the diversity of network security threats today, the target of attack is gradually shifting from the corporate Internet side to affect and destroy corporate LANs. Among them, the degree of harm of viruses and Trojans has increased geometrically in recent years.

Worm is a common form of computer virus, it can use the web and E-mail to large-scale worm to COPY and distribute first appeared in the DOS environment, virus attack, the screen will appear a thing, like a worm can eat the letters on the screen and its transformation properties, the whole process is similar to snake the worm can spread itself functions of COPY or part of itself to other computer systems recently, called WannaCry Worm spread more than 150 countries and regions in the world, the serious influence to the economy, health care, energy industry and so on industry in our country, the development of campus network users from infection, suffer severe, lab, a large amount of data is encrypted locking part enterprise database file is encrypted, cannot work normally, has had a huge impact.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202201_5(1).0019

2. Eternal Blue

2.1. What is the Eternal Blue Virus?(WannaCry)

In 2017, some of the cyber weapons used by the Formula Hacker group under the NSA (US National Security Agency) were made public. These include eternal blue, eternal king, eternal romance, emerald fiber, and weird gophers. Eternal Blue is one of the exploit tools, attacks against SMB services in computers. After being published, it has become a tool for many new viruses. The most typical one is WannaCry.

WannaCry is a worm that can infect itself and spread. It is fast and spreads widely. It is mainly targeted at Windows systems. Once a virus infects a computer, it will immediately use confidential technology and confidential files to prevent users from accessing it normally. For an infected computer, the user must pay a large amount of bitcoin to the account provided by the hacker within a specified time, otherwise the files on the computer will be destroyed immediately.

2.2. WannaCry Key Features

It is mainly aimed at the internal network environment, is highly contagious, has a fast outbreak speed, and uses port 445 to spread. When a computer is infected, other computers in the same network are also infected. This super-autonomous transmission ability can infect all computers in a system within a few hours. And without any user operation, all disk files can be encrypted and locked, and the suffix becomes .onion. Then, the hacker can remotely control the Trojan and extort "ransom" from users.

2.3. WannaCry's Attack Process

The speed of the virus outbreak was so wide and its impact was unprecedented. The virus has spread to more than 150 countries worldwide, causing computer poisoning in more than 200,000 institutions. The virus first appeared in the computer of a college student. The poisoned person thought the content was particularly funny and demanded that the ransom be paid as soon as possible, otherwise the file would be deleted, thinking it was only a small-scale mischief. Unexpectedly, within five hours, the ransomware virus broke out in a large area, and many colleges and universities recruited more and more. Public service networks including the United Kingdom, Russia, Europe as a whole, and some universities, local immigration, gas stations, and hospitals in China have been attacked. Large corporate intranets and government agencies' private networks have all been recruited, posing serious threats to important data.

The actual impact is one-sided, and the psychological impact is even more terrifying. How many people dare not turn on the computer easily, especially the users who do not know the computer at all. How many users have closed port 445, don't worry, and open it again with the eternal blue immunity tool. Some people even use Eternal Blue to kill, close ports, patch systems, and use immune tools. Finally, the machine went into a blue screen and crashed. This situation is quite common.

3. WannaCry Precautions and Countermeasures

3.1. Update System Vulnerability Patches

Currently Microsoft has released patch MS17-010, which can effectively fix the system vulnerabilities of the Eternal Blue attack. You should download and install it as soon as possible.

3.2. Close the Vulnerable Port

If the user has not installed the vulnerability patch, according to the operating system used, close the vulnerability port or set the inbound and outbound rules through the command line window.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202201_5(1).0019

3.3. Enable Firewall

Windows operating system users can go into the firewall settings to enable the firewall, then enter the advanced settings and create a new user rule. Set port 445 to block the connection, and finally push it out.

3.4. Perfom Operations on Files

Users should immediately perform file backups of non-poisoned computers and strictly prohibit the use of devices such as U disks, mobile hard disks that can perform ferry attacks. At the same time, strengthening email security and effectively blocking phishing software can eliminate many hidden dangers.

4. Perform Exposed by the Virus this Time

4.1. Do Not Install Security Software

This is a common problem for many users. I think that installing anti-virus software will slow down the computer speed. Some have installed anti-virus software and do not update it in time. Especially intranet users and Internet users are better. Generally, the virus database is automatically updated. User anti-virus software virus libraries are old and can't do anything against new viruses.

4.2. Not Patched in Time

System vulnerabilities are defects in the specific implementation of hardware, software, protocols, or system security policies, and are inevitable. Since it is unavoidable, it may be used by hackers or viruses, and patches are used to fix operating system vulnerabilities. Generally, when the operating system is found to have security risks, the company that develops the system will release the patch (that is, the vulnerability is corrected) files in time. Generally, the existing vulnerable files will be replaced after installation to correct the system's operating problems. Or prevent certain people from exploiting vulnerabilities to create viruses or hacking software, spread, damage computer systems, or steal information. Except for non-professionals, a considerable number of users choose to never update their computer systems, which means that they will never patch.In the response to the Eternal Blue Virus, this situation was found. As a result, there was a system update, more than a hundred updates, and some even had 12 or 13 years of patches. Why does this happen? Because the system update is generally performed when the machine is turned on and off, the user feels that it is delayed, so he stops the update. Some simple settings are never updated and save trouble. This way, one day, your computer will also have “nothing” because of your “saving trouble”.

4.3. No Firewall

Quite a few users think that the system's built-in firewall is useless, which is a bad idea. Sometimes it also affects the use of certain functions of the computer, and directly closes the system's child wall. Reinstall the firewall that came with your security software. This kind of understanding is to be far away and even wrong. The firewall that comes with the system during development is definitely used to protect the operating system from being invaded, so whenever you install a new software, it will warn you that there is a risk. Some people think that this function is too cumbersome, so turn off the firewall directly. In fact, otherwise, the system firewall can prevent computer viruses from entering your computer. When you make certain connections, you will be asked. For unnecessary or deemed dangerous links, it will be blocked. You can also create a security log to record successful and unsuccessful connections. This log can be used as a tool for queuing failures. However, there are quite a few people who don't need the built-in firewall of Windows. Even if you search on Baidu, the system firewall,

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202201_5(1).0019

what you find is how to turn off the built-in firewall of the system. Nothing more than so many people do not turn on the system firewall.

4.4. Old Equipment

Many units still use the XP system. The XP system has been in use for a long time from 2001 to 2014. In 2014, Microsoft issued a statement that it would no longer update the XP system. However, many users still The XP system is not easy to use, and I feel used to it. It is easy to use. In addition, many application systems are also developed based on the XP system, and it is even more reluctant to replace the higher version of the operating system. In this way, the system cannot be updated at all. How can we not give the virus a chance? In fact, you can choose to download or install the update based on whether your time is free or not.

4.5. The Patch Time Is Not Set Properly

It is undeniable that after the system automatic update is turned on, the patch update is always performed every time the system is turned on or off, which is very troublesome and affects user use. So the user turns off the system update.

5. Virus Attack Methods

There are many types of computer viruses, including:

Harmless type: In addition to taking up disk space during the infection process, this type of virus has no other impact on the system itself and is easy to kill.

Non-Dangerous: This type of virus will reduce computer memory, change display images, computer sounds, and will not cause damage to system software and hardware.

Dangerous: As the name suggests, this type of virus starts a series of serious operations once it infects a computer.

Very Dangerous: This type of virus can not only actively perform a series of operations, but also delete programs, destroy data, and clear system memory. The damage caused by this virus to the system is not the danger it manifests in the computer itself, but the serious damage to the entire network computer during the transmission process, which has a wide range and is extremely harmful, as mentioned above——ransomware.

6. Vulnerabolity Security

Virus attacks often start with computer vulnerabilities. What is a vulnerability? Security vulnerabilities refer to defects in the specific implementation of hardware, software, protocols, or system security policies, which can enable attackers to access or damage the system without authorization. We know that computer systems are very complex, and no piece of software is perfect, which means that all software may have vulnerabilities that can be exploited by hackers. When we read about new security holes that have been exploited by hackers, it usually has a lot to do with Microsoft. Internet Explorer and Windows have been attacked numerous times in the past decade. But Microsoft's programs are not necessarily more vulnerable than others-more importantly, popular programs are more attractive to hackers. The more widely a program is used, the more systems and data a hacker can use. All software can be exploited and attacked.

A security vulnerability is defined as "meeting three elements: system sensitivity or flaws, the ability of an attacker to obtain vulnerabilities, and the ability of an attacker to exploit vulnerabilities." Once a malicious hacker has discovered a weakness or a computer security risk, he will use it. Hackers now have the "ability to exploit vulnerabilities"-all they need to do is connect to your network. How can you effectively prevent your computer from being exploited by hackers? We know that hackers mainly implement attacks by discovering weaknesses in

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202201_5(1).0019

software and creating vulnerable code; hackers can only attack vulnerable software that is assigned to open ports; modern operating systems and browsers are connected to a large number of servers, and Hackers have been discovering new vulnerabilities; any practice from the discovery of a vulnerability to the application of a security patch can be attacked. So we need to do the following:

(1) Use firewalls to close ports you do n't need: Only open ports on a networked server with a security hole will be attacked by hackers. When talking about how hackers connect to your network to take advantage of security vulnerabilities, we often talk about "open ports". It is recommended to close all unused ports, which can effectively prevent hackers from invading your computer.

(2) Another effective method to prevent computer vulnerabilities is to classify passwords. When setting passwords, you should choose different passwords based on different occasions. In addition, passwords that have already been set must be changed regularly to prevent security risks caused by password leakage or deciphering.

(3) Update software to the latest version in a timely manner: Once a vulnerability is found in the software, developers usually release patches shortly after. Don't ignore it, fix the security hole as soon as possible.

(4) Replace software that developers have stopped supporting: When developers stop using security patches to support it, it is when the life of the program or operating system ends. Windows XP is a good example. It still has many vulnerabilities and is still used by millions of people, but it is no longer updated.

7. Conclusion

With the rapid development of the computer industry, network security has gradually become a hot topic in today's world. The system has been updated, various types of software have emerged endlessly, old vulnerabilities have been filled in, new vulnerabilities continue to be born, and people are enjoying the network. At the same time, it is also necessary to increase the emphasis on security precautions. Use scientific firewall technology, network vulnerability scanning technology, and set access permissions to effectively protect your computer and build an efficient, secure, and stable network operating environment, so that Sci-tech network information technology strengthens network self-inspection, self-examination, and self-reinforcement prevention capabilities.

References

[1] Chen P.-K. Sitting outside the network: Reassuring the stability of the Taiwan strait under the trump administration [Título en Castellano: Sentado fuera de la red: Reasegurando la estabilidad del Estrecho de Taiwan bajo la administración Trump][J] Revista UNISCI, 2018, 2018(46).

[2] Cooke Andrew A unique year for cyber security[J] Network Security, 2020, 2020(9).

[3] Still Andy Bot mitigation – how gapsin understanding and ownership are exposingbusinesses to greater threats[J] Network Security, 2020, 2020(11).

[4] Dongxi Li, Xiaowei Cui Dynamics of virus infection model with nonlytic immune response induced by stochastic noise[J] Chaos, Solitons and Fractals: the interdisciplinary journal of Nonlinear Science, and Nonequilibrium and Complex Phenomena, 2017, 99.

[5] Anitta Patience Namanya, Irfan U. Awan, Jules Pagna Disso et al. Similarity hash based scoring of portable executable files for efficient malware detection in IoT[J] Future Generation Computer Systems, 2020, 110(prepublish).