Business Information Systems Project:

Review of Different Types of Software Attacks and

What Actions Shall Take to Defend

Zhan Qiu

COM-327-CA03

St. Leo University

Introduction

I conduct a good review of the different types of software attacks, which is commonly know as Malware, on the information assets of the organization I joined recently. According to the research, I will describe all the related information about these Malware included names, methods of transmission, modes of operation, and type of damage done by each type of the software attack. Also I will include all the actions my manager use to prepare and defend the organization against these types of attacks. The cost of enhancing and upgrading a company's network security after an attack has been increasing dramatically in recent years, since hackers, computer criminals and cyber criminals are both domestic and international, once you using internet you will suffer to face attacking. According to International Data Corporation, by 2020 more than 1.5 billion people will be affected by data breaches.

Background

I have recently joined a medium sized organization as an assistant manager. My manager is concerned about the number of security breaches that are reported almost on a daily basis in the press. My manager wants me to conduct a good review of software attacks that commonly occur on the information assets. As we know, internet users who browse malicious websites, or download games or other programs from unsecured sites, often bring the malicious programs with them to their computers without their knowledge. During that time, any sensitive information, such as bank account information and credit card passwords, could be stolen. According to the records, the earliest malware appeared in 1988. It can be said that compared with the malware technology at that time, the current malware technology is not very different, but due to the emergence of automated tools, the production and spread of malware has increased dramatically. In this case, the harm of malware has taken on a new era.

Types of Software Attacks

Spyware and Adware

Spyware is software that secretly gathers information about users while they browse the web. This information could be used for malicious purposes. Spyware allows users to install backdoors on their computers and collect information about them without their knowledge. It can weaken the user's ability to control their experience, privacy and system security. Adware is a form of spyware that collects information about the user that without the user's consent, to determine which advertisements to display in the user's web browser (Bidgoli, 2019).

Spyware does not necessarily spread in the same way as a virus or worm because infected systems generally do not attempt to transmit or copy the software to other computers. Instead, spyware installs itself on a system by deceiving the user or by exploiting software vulnerabilities. Spyware gets into your system by deception. Most commonly, spyware enters the computer when the computer user installs it. Of course, you wouldn't know that you are doing that. What happens is quite a bit more worrisome. You visit a website and find a piece of software that you would like to have. You download it. Or, you may have the spyware trick you into downloading it. In this case, you may be asked to perform an operation that is "required" to complete the download. When you do, you are actually downloading the spyware or adware onto your computer. Some of the newest versions of this software are even more devastating because they promise to protect your computer. In some cases, the spyware gets onto your computer by pretending to offer you a useful service or tool (Zhang, 2007).

Users' private data and important information will be captured by "backdoor programs" and sent to hackers, commercial companies and etc. These "backdoor programs" can even allow users to remotely manipulate their computers to form a huge "botnet", which is one of the

important risks of network security. For example, you may download a powerful app for free. All you have to do is contribute your name, address, phone number, email and some other personal information in exchange for having this incredible app completely free. Sounds great, doesn't it? But assume your personal information is still stored somewhere on your hard drive, in which case the routine passage over the Internet would send your personal data back to advertisers in exchange for more ads. Those companies offering free products that track users' browsing habits and then upload that information over the Internet in exchange for more advertising.

How to defend?

1. Manually or using software, place the URLs of the companies within the barriers.

2. Carefully install the plug-ins that come with the software.

3. For Windows system, it is necessary to update frequently and patch the vulnerability of Internet Explorer. Using non-internet explorer browsers, such as Firefox, Opera, etc., can avoid a lot of malicious web code. Use anti-spyware software to scan and clean the system, such as Windows Defender, AVG anti-spyware, CounterSpy, etc.

4. Use firewalls that can monitor program communication, such as ZoneAlarm firewalls in Windows to prevent unknown programs from accessing the network.

5. Check whether there are any remaining unknown programs in the system. You can use IceSword.

Ransomware

A type of malware designed to block access to a computer system until a sum of money is paid. According to Kaspersky Lab, the number of ransomware attacks targeting companies increased threefold from January 2016 through September 2016, affecting one in every five

businesses worldwide. The report indicates that there was one ransomware attack every 40 seconds against companies in September 2016 (Bidgoli, 2019).

The spread of ransomware is very similar to the common Trojan, mainly including the following: 1). Spread by web trojans, when users accidentally visit malicious websites, the ransomware will be automatically downloaded by the browser and run in the background. 2). Bundled with other malware. 3). Spread as email attachments. 4). Spread with removable storage media. Once a user is infected with ransomware, it usually takes the following forms, including:

1. Lock the computer or mobile terminal screen.
2. In the name of anti-virus software, falsely claimed that security threats were found in the user's system, which made the user panic and buy the so-called "anti-virus software".
3. A message similar to the one below pops up on the computer screen, saying that the user file is encrypted and demanding a ransom.

How to defend?

1) Provide user education; 2) Backup data all the time; 3) Be skeptical: Don't click on any suspicious email with an attachment; 4) Have a continuity plan in place; 5) Install the latest patches for all software; 6) Block popups.

Viruses

A type of malware and it is the most well-known computer and network threats. Computer viruses are man-made, destructive, contagious and latent programs that can damage computer information or systems. It does not exist independently, but is hidden in other executable programs. After the virus exists in the computer, light impact machine speed, heavy crash system damage; Therefore, the virus brings great loss to the computer users (Mata-Toledo, 2018).

Computer viruses have their own transmission mode and different transmission paths. The main function of the computer itself is its own replication and dissemination, which means that the spread of computer viruses is very easy, usually can exchange data in the environment for virus transmission. There are three main types of computer virus transmission:

1) virus transmission through mobile storage devices: U disk, CD, floppy disk, mobile hard disk, etc., can be the path of virus transmission, they are more likely to be favored by computer viruses and become carriers of computer viruses;

2) spread through the network: the network method described here is different, web pages, E-mail and so on can be the way of computer virus network spread, especially in recent years, with the development of network technology and the frequency of Internet operation, the speed of computer virus is faster and faster, the scope is also gradually expanding;

3) exploit the weakness of computer system and application software to spread: in recent years, more computer viruses exploit the weakness of application system and application software to spread out, so it becomes the basic transmission mode of computer virus.

How to defend?

Installing and updating an antivirus program is the best measure against viruses.

Worms

Worm virus is a common computer virus, is a computer user without intervention can be run independently of the program, it is through the network of computer holes in the acquisition of part or all of the control to spread. A group of computer instructions or program code that affects the use of a computer and can reproduce itself.

1) One of the most common ways for computer worms to spread is via email spam. Years ago, worms could hide in the main text of an email, but now email clients caught on and began

blocking direct embedding since 2010, the risk for this type of attack is fairly low. 2) Use of loopholes, this mode is the most important destruction mode of network worms, and it is also one of the most significant characteristics of network worm. Network worm attack, the first detection of the target computer vulnerability, then based on the detected vulnerability to establish a propagation path, and finally implement the attack. 3) Worms can take on similarly deceptive forms in instant messaging software and take advantage of users who are probably not on high alert when using such services.

How to defend?

1) Choose the right antivirus software. 2) Update virus library frequently. 3) Raise anti-virus consciousness. Do not easily click on strange site, there may be malicious code. 4) Do not casually check strange email, especially those with the attachment.

Trojan

Trojan contains code intended to disrupt a computer, network, or website and it is usually hidden inside a popular program. Users run the popular program, unaware that the malicious program is also running in the background. Disgruntled programmers possibly seeking revenge on an organization have created many Trojan programs. These programs can erase data and wreak havoc on computers and networks, but they do not replicate themselves, as viruses and worms do. The main transmission ways of Trojan virus (Bidgoli, 2019):

(1) spread by download, enter the program during the download, and implant the virus into the computer when the download is finished and the file is opened;

(2) spread by using system vulnerabilities, when there are vulnerabilities in the computer, it will become the target of Trojan virus attack;

(3) spread by email, many strange emails are adulterated with virus seeds. Once the email is opened, the virus is activated.

(4) use remote connection for transmission;

(5) spread through the web page, when browsing the web page often appear a lot of jump out of the page, this page is where the virus stationed;

(6) spread by worm virus, etc.

How to defend?

Always keep your software up to date; always keep a firewall up; install an antivirus software or Trojan remover.

Logic bomb

Logic bombs is a type of Trojan program, causes symptoms similar to those of some viruses and can cause collateral damage to network society. In contrast to viruses, it emphasizes the destruction itself, and the program is not contagious. A logic bomb is a program, or any part of a program, that is dormant until a specific piece of program logic is activated. When the bomb finally releases the code it can delete files, send confidential information to unauthorized parties, wipe out databases, and disable a network for a period of days.

How to defend?

A logic bomb can be rather difficult to detect, however you can take security measures such as constantly monitoring the network system for any suspicious activity, using antivirus applications and other scanning programs that can detect any new activity in the data on a network system. The scanning systems should also monitor the entire network and the individual computers connected to the network.

Backdoor

Backdoor programs are generally program methods that bypass security controls to gain access to programs or systems. During the development phase of software, programmers often create backdoors in the software so that they can modify bugs in the programming. However, if these backdoors are known to others or are not removed before the software is released, it becomes a security risk and can be easily attacked by hackers as a vulnerability.

How to defend?

1) Change your default passwords. 2) Monitor network activity. 3) Choose applications and plugins carefully. 4) Use a good cybersecurity solution.

Conclusion

The characteristics of malware make it easy to be popular, but it must also bring a lot of inconvenience to the user, causing speed and memory and space impact on the user's computer, as well as affecting the normal activities of people on the network. And it can also bring harm to the entire network and information security, especially in the company's operation process will cause significant losses and inconvenience. The tendency of malware is pervasive which makes people to prevent it more effectively, it is necessary to strengthen the security awareness in the process of using the computer, and use the computer knowledge to maximumly eliminate the system security risks, and strive to keep it out of the system. Usually, we can prevent from the following aspects: 1) strengthen the system security settings, timely update the system patch, minimize the system loopholes. At the same time, using strict account management, paying attention to the control of authority, trying safe login and login out. Companies use more secure Intranet. 2) develop good computer habits, do not open unknown sites. 3) timely supplement computer knowledge, the development of the computer is rapidly changing we need advance with times. 4) enhance the awareness of legal protection.

References

Bidgoli, H. (2019). *MIS9, Management of Information Systems.* Cengage. ISBN#978-1337-625982.

Mata-Toledo, R. A. (2018). Computer virus. *In AccessScience. McGraw-Hill Education.* .

Zhang, X. (2007). Spyware. *In AccessScience. McGraw-Hill Education.*