Threats of Computer System and its Prevention

Virdyra Tasril[1], Meiliyani Br. Ginting[2], Mardiana[3], Andysah Putera Utama Siahaan[4]
[1,4]Faculty of Computer Science, Universitas Pembanguan Panca Budi, Medan, Indonesia
[2]Department of Informatics Management, Politeknik Poliprofesi Medan, Medan, Indonesia
[3]Department of Informatics, Sekolah Tinggi Teknik Harapan, Medan, Indonesia
[5]Ph.D. Student of School of Computer and Communication Engineering, Universiti Malaysia Perlis, Kangar, Malaysia

ABSTRACT

Computer viruses are a nightmare for the computer world. It is a threat to any user who uses a computer network. The computer will not be infected by a virus if the computer is not connected to the outside world. In this case, this is the internet. The Internet can be used as a medium for the spread of the virus to the fullest. There are many types of viruses that are spread through the internet. Some of them are aimed at making money, and there are only as a disrupt activity and computer performance. Some techniques are done to prevent the spread of the virus. Here will be explained how to tackle the virus optimally. The benefit is that the computer used will be free from virus attacks and safe to exchange data publicly. Techniques used include the prevention and prevention of viruses against computer networks are to know the characteristics and workings of the virus.

Keywords: Virus, Threat, Worm, Trojan, Adware, Malware

I. INTRODUCTION

The world of technology is growing rapidly from age to age. This development was created because of the technology of Internet technology. It is the main medium for exchanging information. This information is in the form of text, image, sound, video and so on. Not all information on the Internet is open, while the internet is a network of computers that can connect freely [8]. Thus it is necessary to ensure the security of information to computers connected to the Internet network. In the Internet network, there is a security gap that is always targeted by people who are not responsible. Many attempts have been made to improve the security of a site from malicious threats while there are parties with a specific intention seeking to exploit the security system.

This is an attack on the security of information systems. This form of attack can be grouped from easy and difficult. The form of exploitation of information system security is a digital infection. Viruses, Worms, Trojan Horse, are part of a digital infection which is a threat to computer users, especially those connected to the Internet [1][2]. This activity is caused by software that is personally created by a person to carry out criminal acts that would harm the owner he attacks. It aims to steal data and know the secrets that exist on the system and then sell it to the opposing party. Malicious software is one of the programs that commit this crime. This research tries to discuss how to overcome the threat problem on the computer network.

II. THEORIES

2.1 Virus

Virus firstly appeared in 1981 in Texas. The virus name is Elk Cloner. It is spread through Apple II floppy disks. This virus displays a message on the screen. The message from the virus was

It will get on all your disks
It will infiltrate your chips
Yes, it's Cloner!

It will stick to you like glue
It will modify RAM too
Send in the Cloner!

The name "Virus" was introduced after two years from the emergence of Elk Cloner. It was introduced by Len

Adleman in November 1983 in a seminar that discusses how to make viruses and protect themselves from viruses. However, people often assume that the virus that first appeared in the Brain virus Was born in 1986. Naturally, people assume that way because this virus is the most shocking and most widespread because it spreads through the DOS diskette which at that time is popular. At that time, it began to propagate extensively. It is about a year before the first virus appears to infect files. Usually this virus attacks the *.exe files. This virus is called Suriv. The speed of the spread is rapid. It attacked the mainframe from IBM about a year [3].

In 1988, a virus appeared that attacked Macintosh. The name of this virus is Macmag and Scores. At the same time, an internet-attacking virus was created by Robert Morris. In 1995, there was a virus that attacked large corporations including Griffith Air Force Base, Korean Atomic Research Institute, NASA, IBM and much more by the Internet Liberation Front on Thanksgiving Day. Therefore, in 1995 dubbed as the year the hackers and crackers [4][5][6][7].

2.2 Trojan

Trojans in a computer system is a program that is not expected and inserted without the knowledge of the owner of the equipment. This program has a remote control. Usually Trojan is a client-server program. It is designed so that trojans can be controlled and given orders by the maker remotely. It can also be a time bomb where a code will be executed at a certain time. As a result, computers infected by a trojan are completely under the control of that person. Trojan is a program used to carry out an important function of a crime. These codes are usually hidden and unknown to the user. The program performs unidentified functions and steals all necessary data and will be sent to the program's creators [4].

2.3 Spam

Spam is messages sent to somebody containing unrelated information during internet activity. The purpose of spam is to advertise certain products or services. These ads are usually inserted by viruses, trojans, or worms. Spam is disseminated via email by displaying links to specific sites or files. At this time spam is also disseminated through chat, social media, and programs that are installed on the gadget. The main purpose of spam is for promotion. However, there is also spam containing propaganda and virus content. Spam is very harmful to organizations that use email facilities primarily for military and state activities. Spam can cause stacks on useless messages. It will be fatal. The operating system will not be able to withstand the amount of spam sent to the system. Spam also often contains malware so that the system will send spam to other computers while connected to the internet [5].

2.4 Worm

A worm is a computer program that can perform self-duplication on a system. An embedded worm infects the computer's registry and creates a script to multiply itself by utilizing a computer network without the need for authentication from the brain-ware. In contrast to computer viruses, worms exploit vulnerabilities that are accidentally exposed. Some worms also spend the available bandwidth because of a continuous process. A worm is a variant of computer viruses. It can be overcome by closing the path of possibility to enter into the system. This gap is open so that the worm easily enters and infects the computer system. Worms can infect data on the computer in a subtle and hidden way. It is much better than the system done by the virus in general. Typically, the worm will disseminate itself if the computer network is connected to the outside world. Some worms may include virus codes that can damage files, steal documents, e-mail, or perform other destructive things [6].

2.5 Spyware

Spyware is a program that can record secretly any computer network activity. It can steal PIN, password, bank account and others. The recorded data will be sent to the virus maker. If there is valuable data, it will be sold to other parties who can drop the opponent. Spyware deployment can not be detected. It comes from programs that are downloaded from the internet that is usually already modified and inserted by spyware programs. It can also be infected from sites containing adult content or gambling. Spyware can degrade and damage the performance of the operating system and application programs installed on the computer. It is a program that is difficult to be discarded even though the computer is already doing the recovery process [6].

2.6 Adware

Adware is a product or service offering that is part of a site or app. Scripts written on a web page allow adware to run on its own and will appear when activating certain sites. Adware is very easy to dispose of, but there is also adware that has a strong defense. Some Adware is embedded in applications downloaded from the internet. At the time of installing the program, there are several options feature that inadvertently serves to activate adware function. As a result, they can be attached to the computer and greatly disrupt the performance of the operating system. The disadvantage of adware is that the computer will pop out a pop-up window containing certain advertisements which, when clicked, will lead to untrusted sites [7].

III. Result and Discussion

3.1 How A Virus Works

A computer virus is a code that can destruct files or system. It has many types and different ways of working. Communication technology is one way to spread the virus. With the connection of a system to the public system will increase the percentage of possibilities infected with computer viruses. The hackers easily attack and make the computers as their main target. They will insert a killer program on any system that has been successfully taken over. Viruses can spread via VPN to networks owned by the government or other legal entities. Internet of things is one medium for viruses to multiply. Use of a variety of supporting applications will allow the virus to grow. It will make it easier for hackers to exploit vulnerabilities. The following types of viruses and the workings of each virus:

1. File Virus
   This virus has a working method of infecting applications or documents that exist in your computer. When the infected application is run, then this virus will spread by infecting all files or documents accessed by the application.

2. Boot Sector Virus
   This virus has a working way of infecting a region in the hard drive that was first accessed when the computer is boot up. If the boot sector virus is active, the user will not be able to boot his computer normally. It slows down the speed.

3. Macro Virus
   It is usually embedded in some application. It cannot be a stand-alone virus. It infects Microsoft Office applications, such as Word and Excel. Documents infected by Macro Virus will modify or add existing commands to propagate itself when the command is executed.

4. E-mail Virus
   This virus works by e-mail. It especially has an attachment. It has special features such as extension .exe, .pif, or .bat. If the virus is active, then it will send a destructive code to many e-mail address randomly.

5. Polymorphic Virus
   It can change the code when infected to another computer. It is done to hide them from being detected. It is more difficult to remove since they are hidden and no properties.

Virus attacks can be prevented or mitigated using antivirus software. This type of software can also detect and remove computer viruses. The software vendor must provide and renew the computer virus database to kill the infected computer.

3.2 Prevention

System security can be divided into two ways, prevention, and treatment. They are differentiated based on the time of infection. Prevention efforts are performed before infection. It is an action so that the system does not have a gap that can be exploited by the virus to thrive. Treatment can be done after a system has been infected. It aims to fix a weak and open security hole. Prevention is done by finding the weak point of the security hole that has been exploited and eliminates the cause of infection. Viruses often modify startup files, add or modify commands to the registry and also write code to run a command on a computer system. It works to override the system at boot time. With these reasons, then to remove the virus takes a long period and high accuracy. This process is a process full of dangers, including removing the suspected registry. This security measure may lose some of the valuable information.

3.3 Recovery

Anti-virus works to detect viruses, not to detect Trojans, Malware, Adware, and Spam. However, when these types of viruses begin to develop and cause many problems, anti-virus makers add additional data to the coding.

The simple steps taken to remove the virus from the system are:

- Identify the virus file on the hard drive.
- Find out how the virus activates itself and take necessary action to prevent it from running virus after reboot.
- Reboot the computer and remove the virus.
- Observe the difference in computer performance before and after healing.

The above steps are one option to remove a virus from a computer. However, the best step is to re-install all computer programs with new ones. The virus will automatically disappear when the computer has a new system.

IV. Conclusion

The development of computer system technology is a computer virus media to disseminate killer codes. It starts from spreading through floppy disks and boot sectors early in the development of computers, then goes through the internet. Moreover, when the system is already using wireless technology, various other types of viruses will continue to grow up. Viruses are a threat to computer users in cyberspace. Understanding of viruses such as trojans, worms, malware, adware and others need to be known and anticipated by computer network users. It has a great potential danger when the computer is connected globally. Understanding includes how work, types, sources, and goals are the first steps to anticipate. Computer network users often do not know that a virus has infected their computers. It is expected to give lessons to the user to be able to detect and eliminate viruses that are already in the system. It aims to prevent re-infection of systems that are already free from such threats. With that knowledge, computer users will be more careful and conscientious of the system connected publicly.

V. REFERENCES

[1]. S. Natarajan and S. Rajarajesware, "Computer Virus: A Major Network Security Threat," International Journal of Innovative Research & Development, vol. 3, no. 7, pp. 229-302, 2014.

[2]. S. Chakraborty, "A Comparison study of Computer Virus and Detection Techniques," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, no. 1, pp. 236-240, 2017.

[3]. M. Khari and C. Bajaj, "Detecting Computer Viruses," International Journal of Advanced Research in Computer Engineering & Technology, vol. 3, no. 7, pp. 2357-2364, 2014.

[4]. L. X. Yang, X. Yang, L. Wen and J. Liu, "A Novel Computer Virus Propagation Model and its Dynamics," International Journal of Computer Mathematics, vol. 89, no. 17, pp. 2307-2314, 2012.

[5]. P. R. Shah, Y. Shah and S. Madan, "Mobile Viruses," in International Conference on Recent Trends in Information Technology and Computer Science, 2011.

[6]. P. Qin, "Analysis of a Model for Computer Virus Transmission," Hindawi Publishing Corporation Mathematical Problems in Engineering, pp. 1-10, 2015.

[7]. S. Ramadhani, Y. M. Saragih, R. Rahim and A. P. U. Siahaan, "Post-Genesis Digital Forensics Investigation," International Journal of Scientific Research in Science and Technology, vol. 3, no. 6, pp. 164-166, 2017.

[8]. Hariyanto and A. P. U. Siahaan, "Intrusion Detection System in Network Forensic Analysis and Investigation," IOSR Journal of Computer Engineering, vol. 18, no. 6, pp. 115-121, 2016.