

Study on Computer Trojan Horse Virus and Its Prevention

ZHU Zhenfang

Abstract— In recent years, the fast development of computer network technology, has become an integral part of human's life, work and study. But with the popularity of the Internet, computer viruses, Trojans and other new terms have become some well-known network vocabularies. Studies have shown that most users of computer are more or less suffered from computer virus. So people must attach great importance to the network security problem. The paper studied Trojan virus. Paper first introduced the concept, characteristics and categories of the Trojan virus and its harm, and then focused on the way and means of the Trojan's spread. It introduced the Trojan virus loading and hiding technology, too. Its last part focused on the prevention measures, it put forward reasonable suggestions to users, and paper also put forward prevention advice to improve network security..

Index Network security, Computer virus, Trojan horse, Virus defense

INTRODUCTION

The current world has entered into information time with the development of computer network, while internet has become indispensable in life, work, and study. However, the virus attack becomes increasingly popular because of the development and strengthening of internet. Various attack methods greatly threaten the property security of human beings. Trojan horse virus is one of the major methods of network. Therefore, we have to make study to know more fundamental knowledge, communication methods, and work process to take precautionary measures to further enhance the network protection and construct harmonious network environment.

TROJAN HORSE VIRUS

The full name of horse virus is "Trojan horse" which is a novel network attack program at present. It is remote control-based software controlling the other computer based on a specific program. With its implantation function or the characteristic of accessory with carrying virus, this virus can enter into user's computer to steal personal information and password, tamper data, or destroy files [1]. Trojan horse virus can be controlled by attacker to do the command, so the computer system may be destroyed because of their illegal operation.

Trojan horse is extremely dangerous because hostile attacker can control user computer with the virus in distance

to steal or viciously revise files, spy system information, steal various commands and passwords, and even format users' hardware. In addition, Trojan horse virus usually records keyboard operation by means of keyboard record, and then obtains the account and password of E-bank. Attackers can directly steal users' wealth by obtaining accounts and passwords. On the other hand, Trojan horse can also cause the native machine be affected by other vicious virus.

PREVENTION OF HORSE VIRUS

According to the above introduction, we know that Trojan horse virus is very dangerous. If we neglect the prevention, our computer may be easily attacked. For the prevention of Trojan intrusion, Trojan intrusion should be prevented by both users themselves and computer network.

3.1 Prevention in daily surfing process

(1) Never download and operate software or program with ease

Although we install some antivirus software, our computer cannot be absolutely safe. Therefore, we should not be eager to open the software and program with unknown source, but should inspect them with antivirus software to ensure its security. Users always take Trojan horse virus because they neglect the searching and killing process with few seconds in daily surfing to cause the loss and disclosure of system files and important information.

(2) Never open e-mail in mailbox with ease

The e-mail address of users can be obtained by attackers in various ways, and attackers will send users e-mails attached with Trojan horse virus. If users open unknown e-mail without prevention consciousness, the computer may affect horse virus. Therefore, we should not believe that our e-mail address will not be disclosed and think that all the e-mails are safe.

(3) Never implement software or program sent by friends

Software and program sent by friends may not be safe, so we cannot completely trust them [8] because we cannot ensure that if the friend installs virus firewall in the computer. Sometimes, their computers have been attacked by hackers, and they have become the assistant of attackers to send files with virus to you ignorantly.

(4) Never browse abnormal websites

Some files from abnormal websites are always bound with Trojan horse virus. If we open websites at will, we may be attacked by virus at ease.

(5) Be civilized when surfing

A lot of people think that website cannot threaten their personal security because of its virtuality, so they are not civilized when surfing. However, some superior programmers of computer virus and Trojan virus may attack your computer because of your rail or sneer. Therefore, it is important to be

Manuscript received

ZHU Zhenfang, School of Information Science and Electric Engineering, Shandong Jiaotong University, 250357, Jinan, China (zhuzhfy@163.com)

civilized when surfing.

3.2 Prevention by effective computer operation

(1) Install antivirus chip on the network interface card

This is a way to protect virus with hardware. This method should be combined with computer operation system. The chip can prevent the most attack against loophole from Trojan horse virus to buffer overflow under such combination.

(2) Create bootable disc and repair disc

The objective to create these discs is to recover the computer system after being affected by Trojan horse virus to avoid the loss caused by virus affection.

(3) Install authorized antivirus software

Authorized antivirus software can constantly update its virus reserve library and version, so it can search and kill Trojan virus more powerfully to improve the security of user computer system. After successfully installing and starting the antivirus software, it can detect the system automatically and start virus searching and killing. Moreover, it can detect programs and files before use and automatically remove virus. At present, the most common free antivirus software in China includes 360 Safe, Rising Antivirus, and KingSoft Antivirus.

(4) Install patch program and repair system loophole in time

A major method of virus attach is to attack through system loophole at present. Therefore, the system has to install patch program to recover the system loophole.

(5) Shut down the computer immediately after discovering virus

The operation system may back up the registries after normal shutdown, so the files with virus deleted may be covered. Once upon the file is covered, it cannot be repaired. However, if the computer is shut down in emergency by cutting off the power, the integrity of operation system and the most of other applications may be saved well. Then, recover tools can be used for recovery, and antivirus software for virus searching and killing.

(6) Use network firewall

Firewall can detect, limit, and change data flow passing through the firewall, and protect the information, arrangement, and operation of network to the greatest extent without informing others. Firewall can maintain the network security according this effect.

Firewall can be divided into two kinds, one is virus firewall, while the other is network firewall [9]. Virus firewall can monitor the file operation in computer and inspect the computer if there is any virus at any time, so virus firewall will affect computer operation. Network firewall has the function of screening data packages between computer and internet to effectively avoid attack from network. Therefore, the launch of such firewall will affect the operation speed of computer.

3.3 Enhance the management of computer network environment

(1) Popularize knowledge among the public with the harm cases of Trojan virus to let people know about the hazard of Trojan virus. Therefore, the prevention consciousness can be improved, and communication of Trojan virus can be reduced.

(2) Enhance the legal education and moral education for programming personnel and amateurs of computer major to reduce artificial and active Trojan horse attack.

(3) The country should strength legislation to legally call to responsibility of transmitters and producers of computer virus and give them profound education.

CONCLUSIONS

In general, computer virus is increasing with the flourishing growth of internet technology. The types and quantity of computer virus are constantly increasing, so the computer virus brings more severe hazard to human beings and the whole world. Therefore, we have to constantly focus on the development trend and momentum of computer network virus in the future to develop the most effective way fighting against attack. Meanwhile, we should continue to popularize the work content to prevent network virus and effective prevention methods and channels [10]. Moreover, the country should continue to strengthen the study on computer network virus and strive for developing new antivirus software to face changing virus and accelerate the arduous business of human beings, network purification.

ACKNOWLEDGMENTS

National Natural Science Foundation (61373148), National Social Science Fund (12BXW040); Shandong Province Natural Science Foundation (ZR2012FM038, ZR2011FM030); Shandong Province Outstanding Young Scientist Award Fund (BS2013DX033), Science Foundation of Ministry of Education of China(14YJC860042).

REFERENCE

- [1] Zhang Xiaolei. The diagnosis and prevention of computer virus [M]. Beijing: China Environmental Science Press, 2008
- [2] Zhang Yousheng. Computer virus and Trojan horse program analysis [M]. Beijing: Beijing Kehai Electronic Press, 2009
- [3] Du Lei. Analysis and prevention of computer viruses [J]. Silicon Valley, 2008 (22): 23-24.
- [4] Zhuo Wenjian. Principle of computer virus and prevention and cure [M]. Beijing: Beijing University of Posts and Telecommunications press, 2004
- [5] Wang Shusen, Chen Ping. The Trojan horse attack principle and control strategy of [J]. software guide, 2012 (6): 146-148.
- [6] Peng Guojun, Fu Jianming, Zhang Huanguo. Analysis of computer viruses and confrontation [M]. Wuhan: Wuhan University press, 2009
- [7] Zhang Xinyu, Secretary of state Schan, Ma tsuneta. Technology research [J]. Journal of China Institute of communications Troy hidden Trojan, 2004,26 (6): 21-24.
- [8] Liu Gongshen. Computer virus and its prevention and control technology [M]. Beijing: Tsinghua University press, 2008
- [9] Wang Wei, Ning Yupeng et al. Firewall principle and technology [M]. Beijing: Machinery Industry Press, 2006
- [10] Wally. Computer virus prevention art [M]. Beijing: Mechanical Industry Press, 2007

ZHU Zhenfang, PhD, lecturer, he was born in 1980, Linyi City, Shandong Province. He obtained Ph.D. in management engineering and industrial engineering at the Shandong Normal University in 2012, his main research fields including the security of network information, network information filtering, information processing etc.. The authors present the lecturer at the Shandong Jiaotong University, published more than 30 papers over the year.