Discussion on the harm of computer virus and its prevention

Fu Jinwei[1,a], Li Rui[1,b], Yang Zhijin[1,c]

[1] Engineering College, Honghe University, Mengzi 661100, Yunnan, China

[a]ynfjw@qq.com

Keywords: Network security; Network-type virus; Virus protection

Abstract. Transmission and spread of computer network virus seriously endanger the normal use of the computer system and the security of private information, the spread of the virus has great influence and destructive. Invasion of the virus usually causes the system to appear bugs, and produce a lot of information leakage, triggering a security crisis. This paper analyzes the characteristics of the network-type virus, harm and dissemination of view, elaborated computer network virus prevention measures, provide a reference for the network environment to maintain and enhance network security applications.

Introduction

Popularity and rapid development of computer network, so that people fully into the information age, but a new problem has cropped up that computer network security issues. Process computer viruses spread mainly through the development of the virus source files, the use of certain programs and software as attachments, to the spread of virus in the program or file is run. When using a computer, users enjoy the convenience of a computer, but also can not ignore the harm of computer viruses. Route network virus has a wide range of network coverage of our daily environment, its forms and types also have more subtle and diversity, spread and more diverse, the degree of harm caused by the virus is far more traditional large enough more time and scope has spread exponentially, undermining the normal order of the network environment. In the computer network use, work well in advance of the virus prevention is particularly important. Background information on a computer system on a regular basis to detect data is an effective means to prevent viruses, and of course, this operation is best carried out by professionals in order to achieve the desired effect, which is due to the spread of the virus and attack the decision. Prerequisite for virus transmission to be achieved through computer vulnerabilities, and invading computer systems rely on user names and passwords continue to test, and then find the correct login password to complete, this tentative method is commonly used method for viruses, extremely time-consuming and extremely low probability of success, make every attempt after data entry operation will leave traces in the background, for the professional anti-virus great reference value. To control port connected to the network server is another major means of network attackers to attack computer system. An attacker who exploited loopholes in the program interface directly attack the server, and remote control of the computer [1]. So how do you prevent virus attacks and address potential security risks, it is the primary tasks of maintenance and management of computer networks [2].

Computer network virus's characteristics and mode of transmission

Features of computer network virus. In order to enhance the aesthetics and functionality of the Web page, so as to develop ActiveX and Java technologies. However, the virus program's producers took advantage of these technologies, to infiltrate viruses into personal computers, which lead network virus to born. Network virus use network as a platform in network environments, can be transmitted, enforceability, destructive and can be common triggers such as computer viruses, but also has some new features [3, 4].

(1) The fast infection: in a stand-alone environment, the virus can only through the floppy disk, optical disk, USB flash disk and other removable storage devices to infect other computers, but in the network can spread rapidly through the network communication mechanism.

(2) The wide spread: the spread of the virus very quickly in the network, spread over a large, not only the rapid transmission of all computers within the LAN, but also can spread the virus to the thousands of miles away by a remote workstation in an instant.

(3) The complex and varied communication: computer viruses on the network, typically by "workstation to the server approach workstation" ways of spreading, but forms are complex and diverse.

(4) It is more difficult to completely remove: viruses on a single computer can sometimes by removing the poison files, low level format the hard disk and other ways to completely remove the virus. In the network, as long as there is a workstation fails to clear, it is possible to make the whole network has been infected; even one workstation removal task has just been completed, it could soon be infected by another machine on the network workstation.

(5) The damage is large: viruses on network will directly affect the network's work, ranging from reduce speeds, then crash the network, or even damage the server information and years of work to be destroyed at one time.

Like other computer viruses, network virus was man-made, its use of network information technology in order to undermine the network and information security for the purpose. In recent years, with continued advances in network technology, network viruses, also in rapid development. At present, a wide variety of common computer virus and network viruses, a type of virus, characterized by regular computer virus there is a big difference.

Network viruses spread using network system, network system contains a wide variety of devices, which make it impossible to use the appropriate means to eliminate hidden dangers. However, the Internet in the spread of the virus, which is mediated by networks in the process, if you leave the network, then the network virus could not be spread. But in the current network environment, which is difficult to prevent the spread of viruses for most of them direct presence in online equipment systems, to destroy the integrity of network information, making the whole security of network equipment drops drastically.

Portion of the network viruses in online equipment will not affect the security of network information data, but destroy the accessibility of computer network system, which can lead to network device is not working properly.

Network virus is generated artificially, its appear largely have a very close relationship to hackers, which use them to modify or destroy the network system, so as to achieve the goal of stealing file information.

Computer network virus propagation mode. Network viruses have a great impact on the development of computer information technology, can be divided into two categories, namely the worm and Trojan virus. Worm virus replicate itself or a part to all kinds of computer information system via computer networks by e-mail or any other means to disseminate itself, so as to cause harm. Trojan virus is a fake and latent viruses, leaks from the onset of the virus itself to various privacy information.

Computer network virus basically has the following kinds of dissemination way [5]: The first is transmitted through a variety of communication software, such as the user in the use of Msn or other instant messaging software, and download the unknown executable program; it will cause the virus intrusion into computer networks. Secondly, the computer network virus can also be spread with the help of the email. In addition to the above two methods, computer network virus can also spread through the website directly, but this mode of transmission needs the help of security vulnerabilities of system or software to threat the computer security. By entering into the internal procedures used by the computer web markup language to change the operating system registry, or on the system resources of all kinds of improper control, and thus to harm the user's computer information.

Computer network virus prevention measures

In order to enhance the security of computer network, must come to realize the maintenance of the computer network from the two aspects of management and application of technology, operators

need to know about a variety of computer virus, and master various preventive measures [6]. In addition, according to the daily operation of computer networks in a variety of situations to develop practical preventive measures, computer networks may be affected by a variety of viruses or system vulnerability to systemic checks, once the existence of security risks, should take immediate measures to maintain. Ensure that the main way is to do a good job of computer network security protection measures for the computer virus, we must start from the main ways and means of transmission, the maximum extent to reduce the harm caused by computer network virus.

Improve and strengthen the management and technical measures. To prevent computer network virus, can begin from the two aspects of management and technology measures.

(1) Management measures. For the computer network management need to strengthen the operation of computer personnel training, to help them to set up the awareness of computer network security and virus prevention, to know about the means of intrusion and harm of network virus, so as to make them to inhance protection consciousness in the work; according to the specific circumstances of the itself of computer network system, formulate the corresponding executable operation regulations, and strictly in accordance with the requirements of the operation, ensure that policies can obtain the very good implementation; grasping the development trends of network virus in a timely manner, in view of its intrusion methods and technical features, modify and improve the protective measures in a timely manner.

(2) Technical measures. Due to the large number of network viruses, a wide range, and spread rapidly, dependent on the network characteristics and traditional computer virus protection is difficult to play an effective role, so it should aim at the propagation and damage link of network virus to take technical measures, can effectively protect the safety of computer network system.

Protection against virus attacks. For the virus attack mode to establish the multi-level, three-dimensional defense system. Route of transmission for the virus can use close management, for example, to monitor the mail server, prevent virus spread through e-mail. Common anti-virus software and Internet firewall should be installed and fair use, but also to ensure timely upgrades for loopholes to be repaired in order to prevent virus damage the registry and other important information, the data are complete and valid backup.

Improve network security.

(1) Proper use of firewalls. A firewall is a network security technology within the network and external network isolation, which provides security by controlling the transmission of information between internal and external networks. A firewall with appropriate setting can filter out most potential threat from external network, avoid the spread of the virus effectively, and minimize the harm of network virus [7].

(2) The legal download and install software. Part of the network virus and Trojan hidden in most software programs through camouflage, some users due to negligence download a virus software, however more users for the sake of a little small cheap and go blind to download, a computer system to enable the virus to successfully enter the user equipment and network, infection harm to the network security.

(3) Timely upgrading software and system. A lot of network virus will use the system and software vulnerability. In general, developers will be timely to update and maintain the development of the product, eliminating loopholes to protect network security. So, should upgrade in time system and the latest version of the software, or is likely to cause vulnerability attack, the network virus caused great harm to the computer system and network security.

(4) Use the correct command system. The correct use of the system command, communication sometimes can prevent some network virus in a timely manner. For example, some network virus need to be attached to a computer system in some unnecessary procedures can be run, as long as we stop running the program or file, can indirectly prevent network virus operation.

(5) Secure Internet skill. The rapid development of high-speed expansion of computer and network, more foil a people not perfect Internet skills, most people do not have the knowledge of computer and network of basic security awareness. Causes the network security system exists in name only, not for the computer network security protection. So for this user, to cultivate their good

habit of using internet. You can also often see the updated firewall and antivirus software, and prevent access of unknown origin site, the installation is not legitimate software.

(6) The regular backup of important data. This is an important security measure which ignores most people. Although a lot of people with related exercises, but because of lazy thinking work, no timely backup. When the computer system and network attacks

In time, this method can spread and harm of network virus to a minimum, to minimize the loss. To maintain the security of network is not simple to install antivirus software, but to establish a strict firewall from the thought, eliminated lazy and covet small profits behavior, can effectively protect the network security.

Conclusion

Because of the openness and vulnerability of computer network system, allowing network viruses can exploit the bugs of system, software and protocols for network attack. The large number of the computer network virus, a wide range, and rapidly spread, has become a major threat to computer network security [8]. Only from management and technical measures two-pronged approach, to block the spread and destroy link of the virus, it is the fundamental way to control virus spread and protect computer network system security.

With the development of computer technology, to protect the security of computer networks has become particularly important. In the daily maintenance of computer network security, the computer security vulnerabilities should be discovered promptly and take appropriate control measures to control, to protect the computer network security and promote the healthy and rapid development of the computer industry.

In order to ensure the security of computer networks, the maintainer need first understand and analyze a variety of viruses, computer network for daily use may suffer from a variety of viruses or other security hazards, to take certain measures to control and prevent ; use a firewall or other type of virus prevention software to protect the operating system, but also uninterrupted and procedures for various software updates; for important data or information do backup; when installing a variety of computer software, be sure to carefully consider, comprehensive screening, the official website or downloaded from the regular channels, so as to avoid the computer network intrusion by a variety of security risks, so as to ensure the normal operation of computer networks. The development of computer network security technology is relatively slow, affected by various factors, the popularity of computer network security technology is not very comprehensive; only to ensure the maintenance of computer network security level reaches a certain height, can promote the comprehensive development of computer information technology, and provide a strong impetus and protection for production and people's daily life.

All in all, the computer network security continual emergence of new problems, not only the technical aspects of innovation, but also need to protect the laws and regulations, but also need multi-pronged approach to create synergy; in the rapid development of the Internet today, continue to study new ways to solve this a potential network security problems for people's production and life and consumption provide a healthy and secure network environment.

References

[1] Han Yang. The Characteristics and Prevention Policies of Network Virus. Computer Engineering, 2003(9).

[2] Wang Xiguang. Current Situation and Development Trend of computer viruses Almost. Computer Knowledge and Technology, 2010 (12).

[3] Guo Lina. The damage and control technique of computer network virus. Read count (Teacher): Quality Education Forum, 2014 (26) 263.

[4] [Xi Xiaohong. Discussion on computer viruses and preventive measures. Sci-Tech Information Development & Economy, 2010 (35).

[5] Han Yang, Li June. The characteristics and prevention policies of network virus. Computer Engineering, 2003 (1) 6-7.

[6] Xu Yansheng. Computer network safety and network virus prevention. Consumer Electronics Review, 2014 (10): 150.

[7] Li Shaobiao. Study on the Countermeasures of network virus and characteristics of computer network security risks. Silicon Valley, 2014 (9).

[8] Zhang Yuwen. Characteristics of computer viruses, harm and prevention research. Computer CD Software and Application, 2013 (10).