

An In-Depth Study on Privacy Law, Computer Viruses and Their Prevention

John Aghaei, Morgan Beren

The University of Texas at Dallas, Texas, USA

Abstract: With the wide application of computer networks, global informatization is accelerating, computer networks as a platform for information technology and applications have touched all corners of social life, but network viruses have become an important problem plaguing the security of computer systems. This paper initially analyzes the characteristics and hazards of computer network viruses, and puts forward some effective preventive measures, in order to minimize the harm caused by computer viruses.

Keywords: Computer viruses; characterization; prevention of.

1. Introduction

Today, computer network applications have been extended to all areas of the world, is working on people's work, life has an unprecedented impact, as electricity, and transportation, as increasingly indispensable components of people's lives. At the same time, with the continuous expansion of the network scale, network attacks, and other insecurity factors have seriously threatened the network and information security. Network security has gradually become a potentially huge problem, and how to eliminate security risks and ensure the safety of network information has become an important issue[1-5].

2. Characteristics and Hazards of Computer Network Viruses

2.1. Characterization of computer network viruses

Computer or network virus itself is also a computer program or a section of the computer program, but the program is used to damage the computer system or affect the normal operation of the computer system of the "malignant" program. It has the following characteristics[6].

1 Non-authorized executability:

Users usually invoke the execution of a program, the system will give control to the program, and allocate the corresponding system resources to the program, so that it can complete the user's needs. Because computer viruses have all the characteristics of normal programs, when computer viruses are hidden in legitimate programs or data, when the user runs a normal program, the virus will wait for the opportunity to steal the control of the system, and be able to run first. However, at this time, the user still thinks that it is executing a normal program.

2 Hiddenness:

A computer virus is a very small executable program. It is usually attached to the normal program or the boot sector of the disk, but also stored in the surface of the seemingly damaged disk sector, so computer viruses have illegal storage. Computer viruses try to hide themselves from the user or anti-virus software, both in the way they exist and in the way they spread[7].

3 Infectious:

Infectious is the most important feature of computer viruses, but also all kinds of virus checking software to determine whether a piece of program code is an important basis for computer viruses, virus programs, if the invasion of the computer system will be start to search for programs or magnetic media that can be infected, and then modify other programs to infect their own replicas or variants to other non-toxic objects for replication and propagation.

These objects can be a program or a part of the system. At present, the application of computer network is very extensive, which makes computer viruses can spread to other computers in a very short time, especially the application of Internet provides a global high-speed channel for the spread of computer viruses[8].

4 Latent:

Computer viruses have the ability to attach to other programs, so computer viruses have the ability to parasitize. After the invasion of the virus latent until the conditions are ripe to attack, the virus latent more hidden, it exists in the system for a longer period of time, the virus infected the wider the scope of its harmfulness will be greater.

5 Destructive:

No matter what kind of virus program, once invaded the computer system will cause varying degrees of impact on the operation of the operating system, interfering with the normal operation of the machine. There are also some virus programs will delete files in the system, or encrypted disk data, so that the computer system total collapse, so that the system can not be recovered, resulting in irreparable losses.

6 Trigger ability:

Computer viruses generally have one or several trigger conditions, when the trigger conditions are met, the computer virus will begin to attack. The essence of the trigger is a condition of control, the virus program can be based on the designer's requirements, under certain conditions to implement the attack.

In addition to the above characteristics, cyber viruses have their own features.

- Intelligent: In the past, people thought that as long as they did not open the e-mail attachment, they would not be infected with viruses, but the new generation of computer viruses is alarming, for example, the user receives the "Verona virus" virus e-mail, even if it is only a preview, the virus will automatically attack, and will send a new virus e-mail to the

address in the address book address, so that the rapid spread of the virus. The virus spreads rapidly[9].

- More destructive: network viruses can not only attack programs, but also destroy the hard disk partitions of hosts on the network, making the entire network unable to work. Take Novell network as an example. Once the server's hard disk is invaded by viruses, it may cause damage to the contents of some areas in the Net Ware partition,

The network server can not start, resulting in the paralysis of the entire network, causing incalculable losses.

- Extremely fast spreading: A network virus that invades a public utility or utility software can spread rapidly throughout the network.

- More covert: At present, new viruses can be directly written into JPG and other pictures. Once a computer user opens the picture, it will run some programs to format the user's computer hard disk so that it cannot be recovered.

2.2. The dangers of computer network viruses

With the help of computer networks, computer viruses can spread rapidly. When a virus breaks out, it will be difficult to control and eradicate it. It is extremely destructive, such as "CIHH virus" and "Panda burn incense virus". It can be said that everyone turns pale when talking about it. Computer viruses attach themselves to various types of documents, When files with computer viruses are copied or transferred from one host to another, they spread with the files. Just as many biological viruses are infectious, the vast majority of computer viruses have unique replication capabilities and the characteristics of infecting benign programs[10].

At present, computer viruses have become one of the main threats to network security; A wide variety of computer viruses will lead to computer or network system paralysis, serious damage to programs and data; It blocks the network, greatly reduces the operation efficiency, and makes some functions of the computer or network system unable to be used normally; It poses a serious threat to the normal work of users.

The proliferation of computer viruses will also cause serious psychological pressure on the user, always worried about virus infection, when the computer crashes, the software runs abnormally and other phenomena, people tend to suspect that these phenomena may be caused by computer viruses. Infected with viruses may bring great time, energy and economic losses, which makes people fear of viruses, computer viruses like "ghosts" in the minds of the majority of computer users, causing great psychological pressure on people, greatly affecting the efficiency of modern computer use, the resulting intangible losses are difficult to estimate.

The resulting intangible losses are difficult to estimate. With the increasing importance of network applications in daily work and life, this harm will only get bigger and bigger.

3. Preventive Measures Against Computer Network Viruses

The establishment of a reasonable computer network virus prevention system and system, timely detection of computer virus intrusion, to take effective means to stop the spread of computer viruses and damage, recovery of the affected computer systems and data. The most important software and hardware entities in the computer network system are servers and workstations, so the prevention and treatment of computer network viruses should first consider these two

parts.

3.1. Based on server prevention technology

The network server is the center of the computer network. Once the network server is destroyed, the loss is irretrievable and immeasurable. At present, anti-virus loadable module (NLM) is widely used in server based anti-virus methods to provide real-time virus scanning capability. Sometimes, it also uses the anti-virus card insertion technology on the server to protect the server from

The virus is attacked by the virus, thus cutting off the pathway for further transmission.

3.2. Based on workstation control technology

Workstation is like the gate of the computer network. Only good look at this gate, in order to effectively prevent the invasion of viruses. Workstation anti-virus there are three ways: First, software prevention and control, that is, on a regular basis from time to time with anti-virus software to detect the virus infection of the workstation. The second is to insert anti-virus card on the workstation.

Anti-virus card can achieve the purpose of real-time detection, but the anti-virus card upgrade is not convenient, from the practical application of the effect of the workstation's operating speed has a certain impact. Third, the installation of anti-virus chip in the network interface card. It will workstation access control and virus protection into one, can be more real-time and effective protection of workstations and the bridge to the server.

3.3. Strengthening computer network management

Computer network virus prevention, is the technical means and management mechanism is closely integrated to improve people's awareness of prevention, from the root to protect the network system security operation. Due to the computer network virus prevention and treatment of technical means is always in a relatively passive position, this defect can be made up through the management mechanism to take proactive measures. Should be from the use of hardware equipment and software systems, maintenance, management, service and other aspects of the development of strict rules and regulations, network system administrators need to learn to understand the use of different platforms and management methods, and the application of these management and control platforms to manage the objects in the network. The events and information generated by each device and system are associated and analyzed in order to discover new or deeper security problems.

3.4. Strengthening the management of the legal and regulatory aspects of the computer network

One of the main reasons why criminal activities utilizing computer network information systems are quite rampant in current societies is the fact that computer network information systems security legislation in various countries is not yet sound.

Laws and regulations on computer network systems are norms that regulate people's general social behavior; they issue decrees or bans to prevent any violation of the requirements of the regulations and clarify the rights and obligations of the staff and end-users of computer network systems.

4. Summary

In short, network security is a comprehensive subject, involving technology, management and many other aspects, including both the security of the information system itself, as well as physical and logical technical measures, although there are many network security products, such as firewalls, antivirus software, intrusion detection systems, but the illegal invasion of hackers are pervasive.

The fundamental reason is that the network's own security risks can not be eradicated. In the face of the ever-changing virus, we must always be vigilant, and constantly develop network security technology to create a safe and smooth network environment.

References

- [1] Li, X., Wang, X., Chen, X., Lu, Y., Fu, H., & Wu, Y. C. (2024). Unlabeled data selection for active learning in image classification. *Scientific Reports*, 14(1), 424.
- [2] Liang, Y., Wang, X., Wu, Y. C., Fu, H., & Zhou, M. (2023). A Study on Blockchain Sandwich Attack Strategies Based on Mechanism Design Game Theory. *Electronics*, 12(21), 4417.
- [3] Lee, Zhitong, Ying Cheng Wu, and Xukang Wang. "Automated Machine Learning in Waste Classification: A Revolutionary Approach to Efficiency and Accuracy." *Proceedings of the 2023 12th International Conference on Computing and Pattern Recognition*. 2023.
- [4] Guo, H., Ma, Z., Chen, X., Wang, X., Xu, J., & Zheng, Y. (2024). Generating Artistic Portraits from Face Photos with Feature Disentanglement and Reconstruction. *Electronics*, 13(5), 955.
- [5] Wang, X., Wu, Y. C., Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes. *Frontiers in Blockchain*, 7, 1306058.
- [6] Strahilevitz, L. J. (2010). Reunifying Privacy Law. *Calif. L. Rev.*, 98, 2007.
- [7] Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law*. Aspen Publishing.
- [8] Richards, N. M., & Solove, D. J. (2010). Prosser's privacy law: A mixed legacy. *Calif. L. Rev.*, 98, 1887.
- [9] Kephart, J. O., & White, S. R. (1993, May). Measuring and modeling computer virus prevalence. In *Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy* (pp. 2-15). IEEE.