Computer Virus and Anti-Virus Technology

Naifu Zhang

Department of Information Security, School of Computer Science and Technology, Southwest University of Science and Technology
3301789647@qq.com

ABSTRACT
With the rapid development and application of computer technology, the accompanying problems caused by computer viruses are becoming more and more serious. The main content of this paper includes the definition, type, characteristics, harm of computer virus, anti-virus technology and its application, including the detection and removal of virus. The purpose of this article is to impart some antivirus knowledge to computer users, and to minimize the possibility of computer users being harmed by computer viruses.

Keywords: *Computer Virus, Anti-Virus Technology, virus detection technology*

1. INTRODUCTION

Since the beginning of the 21st century, the application of computers has become more and more extensive, and it is used in almost all walks of life. As computer technology accelerates people's development, computer viruses also appear along with it. Computer viruses are recognized as the number one enemy of data security. Since 1987, computer viruses have received worldwide attention. In 1989, computer viruses were first discovered in my country. At present, computer viruses are also developing in the direction of greater destructiveness and concealment. Therefore, it is very important to develop a set of effective anti-virus technology.

2. DEFINITION OF COMPUTER VIRUS

A computer virus refers to a set of computer instructions or program codes inserted into a computer program by a compiler that destroys computer functions or destroys data, affects the normal use of the computer and can replicate itself. The essence of a computer virus is a program, just as the essence of an enzyme is a cell. Like biological viruses, computer viruses are contagious, stealthy, infectious, latent, excitable, expressive, or destructive.

3. TYPES AND CHARACTERISTICS OF COMPUTER VIRUSES

A computer virus refers to a set of computer instructions or program codes inserted into a computer program by the compiler to destroy computer functions or destroy data, affect the normal use of the computer and be capable of self-replication. Computer viruses have the following characteristics: First, computer viruses are parasitic. Just like biological viruses must be parasitized in living cells in order to survive, computer viruses also need a host to survive, and this host is the computer. Second, computer viruses are reproductive: computer viruses can reproduce like biological viruses. When a normal program runs, it also replicates itself. Whether it has the characteristics of reproduction and infection is the primary condition for judging a program as a computer virus.Third, latent: computer virus latent refers to the ability of computer virus to attach to other media to parasitize. After the virus invades, it will not attack until the conditions are ripe, which will slow down the computer. Fourth, latency: computer virus latency refers to the ability of computer viruses to attach to other media to parasitize. After intrusion, the virus does not occur until the conditions are ripe, which will slow down the computer. Like the new coronavirus, the incubation period in the human body is in the Within 14 days, after the incubation period, the attack will occur. Finally, computer viruses are executable. Like other legitimate programs, a computer virus is an executable program, but it is not a complete program, but parasitic on other executable programs, so it enjoys the power that all programs can get.

Computer viruses are classified in two ways:

1. Classification of attached media types

(1) Network virus: A computer virus that infects executable files through a computer network.

(2) File viruses: viruses that attack files in the computer.

(3) Boot virus: It is a virus that mainly infects the drive sector and the boot sector of the hard disk system.

2. Classification of computer-specific algorithms

(1) Incidental virus: usually attached to an EXE file, its name is the same as the EXE file name, but the extension is different, generally it will not destroy the change file itself, but it is this kind of virus that is activated first when DOS reads it.

(2) Worm virus: it does not damage computer files and data, and its destructiveness mainly depends on the deployment of computer networks. You can use computer networks to switch from one computer storage to another computer storage to calculate network addresses to infect viruses.

(3) Variable virus: It can apply complex algorithms on its own, and it is difficult to find because the content and length expressed in another place are different.

4. RESEARCH ON ANTI-VIRUS TECHNOLOGY

4.1 virus detection technology

Although there are various types of computer viruses, they can also be detected. Several common virus detection techniques are described below.

4.1.1 Intelligent Broad Spectrum Scanning Technology

Intelligent broad-spectrum scanning technology is designed according to the ever-changing patterns of current viruses, mainly to bypass anti-virus software, analyze every byte of non-continuous and transformative viruses, and integrate them. , forming a highly mutated virus.*Intelligent Broad Spectrum Scanning Technology*

4.1.2 Virtual Machine Technology

Virtual machine technology is to run the virus in a virtual environment to analyze the execution behavior of the virus. The encrypted virus needs to be encrypted during the execution process, so the virus can be detected and killed through the signature code, and the operation of the virus in the virtual environment will be monitored. This technique has the advantage of being predictable in advance and being inspected quickly.

4.1.3 Heuristic scanning technology

Due to the various forms of viruses and new viruses emerging constantly, the traditional signature technology has been unable to effectively detect viruses. The heuristic scanning technology can better detect the relevant code of the virus. This technology cannot identify some ambiguous viruses, but can remind the user to terminate the program in time when the virus is found.

4.1.4 Integrity Detection Technology

The technology first needs to understand the content of the computer, and when it is detected that the information has been modified, it is covered with the original information. This technology can detect all viruses, regardless of the type, quantity, code, etc. of the virus.

4.2 Anti-virus technology

As viruses tend to spread faster and more stealthy, antivirus technology is also evolving. At present, common anti-virus technologies include signature scanning and killing technology, sand table virtualization technology, active defense technology, real-time virus monitoring technology, and "cloud security technology".

4.2.1 Feature code killing technology

A signature is generally a string of hash values or bytecodes that determine whether a file or buffer contains malicious code. This technology is an anti-virus technology that consults and analyzes known viruses. The premise of using this technology is to obtain the virus program, that is, to collect a lot of virus source codes, and then analyze and extract a series of binary string virus signatures from them, and then carry out one by one with the program files according to the extracted virus signatures. By comparison, virus programs can be distinguished from normal programs by relying on the signatures of these viruses, and virus files can be identified and removed. Regularly upgrading antivirus software is to update the new virus signatures in the antivirus software virus database, so as to detect and kill new viruses.

However, according to the survey, the traditional "signature scanning and killing technology" has increasingly exposed its inherent drawbacks, that is, it lags behind the emergence of viruses. In a network environment with an increasing number of computer viruses, it will be difficult to satisfy users' needs. security needs. Therefore, many enterprises do not use signature scanning and killing technology.

4.2.2 Sandbox Virtual Technology

Sandbox virtualization technology is to imitate the existing virtual environment, then run the program, and judge whether it is a virus by the result of the program execution. When the virtual machine is restarted, the system is restored to its original state. Compared with the common virtual machine technology, this technology solves the problem of excessive virtual machine resource occupation. Therefore, sand table virtual technology has been widely used.

4.2.3 Active Defense Technology

Active defense technology is mainly used when the signature technology cannot identify the virus, that is, the virus database is old. The principle is to extract the common characteristics of virus behaviors, use these behavioral characteristics to determine whether a program file is a virus, and combine these behavioral characteristics such as self-establishment process, self-establishment of startup items, registry modification, self-replication, and continuous network connection to determine whether a program file is a virus. Whether a program file is a virus. The disadvantage of this technology is that the program must be executed before it can be judged, and the virus cannot be directly and statically detected.

Under the circumstance that there are more and more types of viruses and a surge in quantity, the application of active defense technology will become more and more extensive.

4.2.4 virus real-time monitoring technology

Because the virus is real-time and dynamic, anti-virus software must have real-time monitoring technology functions. Any program must be filtered when it is called. Once a virus is found, it needs to be disinfected or terminated immediately to avoid future troubles.

4.2.5 "Cloud Security" Technology

"Cloud security" technology is the embodiment of information security in the network era. This technology combines emerging technologies such as distributed computing, parallel processing, and unknown virus behavior detection. The latest information on Trojan horses and malicious programs is pushed to the server side for automatic analysis and processing, and then the solutions for viruses and Trojan horses are distributed to each client. The use of "cloud security" technology can speed up anti-virus software to extract viruses and greatly improve the efficiency of anti-virus.

However, this technology is still in the development stage, the standards of each enterprise are different, and a unified standard has not yet been formed, and misjudgment of the virus will often occur.

5. COMPUTER VIRUS PROTECTION STRATEGY

Although the current anti-virus software develops rapidly and becomes more and more powerful, it is not a panacea. Therefore, our users must do the following in our lives to effectively protect us from the threats brought by viruses:

(1) The computer should be patched in time and a reliable password should be set;

(2) Install the correct anti-virus software. Now with the upgrading of computer operating systems, the anti-virus technology that comes with the system is getting stronger and stronger, and some anti-virus software has become "rogue" software, such as 360 Security. , Kingsoft Internet Security, etc., and the correct antivirus software includes Windows Defender and Tinder Security that come with win10;

(3) Do not randomly click on the links that often pop up in web pages, these are likely to be potential viruses;

(4) Download the software from the official website instead of downloading the software in some irregular places;

(5) Do not browse unknown websites;

(6) Do not chat with some strangers and unfamiliar people on some unknown chat platforms;

(7) Try not to use some rogue software, such as Quick Press, 360 Browser, Kingsoft Internet Security, etc.

6. CONCLUSION

With the widespread use of computers, it is not uncommon for viruses to damage computer systems. Due to the various forms of viruses, the forms of anti-virus are becoming more and more severe, and the use of a single anti-virus technology cannot effectively prevent viruses. Therefore, it is necessary to combine the advantages of various anti-virus technologies to minimize the harm of viruses to us.

AUTHORS’ CONTRIBUTIONS

Zhang Naifu: Collecting data and writing papers.

ACKNOWLEDGMENTS

After months of hard work, I finally finished this thesis. I also encountered a lot of confusion in writing, but they were finally resolved through the guidance of the teacher and the process of consulting various documents.

The successful completion of this article is inseparable from the help of teachers, as well as various documents and video materials. I know that my academic level is still limited and I need to study harder.

REFERENCES

[1] Zhang Renbin. Computer Virus and Anti-Virus Technology [M]. Beijing: Tsinghua University

Press, 2006: 91-103.

[2] HAN Xiaoqing. Analysis and Prevention of Computer Virus Encyclopedia[M]. Beijing: Electronic Industry Press, 2008.

[3] Yu Xiaozi. Research and implementation of classification-based unknown virus detection technology [D].Beijing University of Posts and Telecommunications, 2013.

[4] Zhang Boyun. Research on computer virus intelligent detection technology [D]. National Defense Science University of Technology, 2012.

[5] Bill Blunden. System Gray Areas Lurker[M]. Yao Lingtian. Beijing: Mechanical Industry Press, 2013.

[6] Hu Xiaoye . A brief analysis of the research of computer virus detection system Research and Implementation[J].Henan Science, 2014,07:1255-1258.

[7] Wang Xin, Jiang Hua. Computer virus and its prevention technology in network environment [J]. Computer and Digital Engineering, 2008(2): 88-90.

[8] Gao Xuemei, Exploring anti-virus technology from the intrusion characteristics of computer viruses [M]. Journal of Shenzhen Institute of Information Technology, 2014

[9] Zhang Fan. Research on unknown virus detection method and system implementation technology [D]. Xi'an: Northwestern Polytechnical University, 2003.