Study on the Technology of Detection and Prevention of Computer Virus

Dongying Zheng

Weifang University of Science and Technology, ShanDong ShouGuang, 262700,China;

zdy7817@163.com

Keywords: Computer virus; Virus characteristics; Testing; Virus prevention technology

Abstract: The article first makes a simple overview of computer virus definitions, characteristics and classification. Then it conducts the research on the virus detection method based on computer virus invasion pathways, including: appearance inspection method, the feature code method, system data comparison method and software simulation method. Finally, it is about the computer virus prevention technology from the three aspects of the prevention and cleaning computer virus and repairing computer system.

Introduction

To do research on anti-virus technology, the characteristics and behavior mechanism of computer viruses should be understood,, which provides a reliable basis for preventing and eliminating computer viruses. Therefore, it is very practical to study computer virus and prevention. Then, from the characteristics of the computer virus, the article discusses the prevention strategy of computer, analyzes the forms of computer virus. The virus can be destructive to the computer and the network. Finally, it puts forward the prevention and control of the basic methods and treatment measures.

Definition of computer virus

The so-called "computer viruses" is actually called computer code or program that is produced and transmitted to a special purpose. It also can be called “a malicious code ". The reason why these procedures are called viruses are mainly because of their similarities with the virus in biomedicine with many same points, such as they are parasitic, infectious and destructive.

The characteristics and classification of computer viruses

Characteristics of computer viruses. The computer viruses have different characteristics which can be summarized as follows:

1) Infectivity

The infectivity of computer viruses refers to the ability of the virus to replicate itself to other programs. A computer virus is a manually compiled computer program code which is into the computer and executed. It will search can be infectious programs or magnetic media, then by self replication spread rapidly. Normal computer programs don't typically link their code to other programs. So it is one of the most important conditions for judging whether a program is a computer virus.

2) Non authorization

The normal procedure is to call by users, and then by the system to allocate resources, complete the task of users confessed. For users, it is visible and transparent. The virus is not the users’ permission or in the form of deception, so the system is unauthorized.

3) Concealment

A computer virus is a kind of very high programming skills and executable program. It is usually attached to the normal program or disk boot sector, or the disk is labeled as the bad cluster sector, and some of the idle probability of the larger sector, which is its illegal storage. The virus tries to hide itself, in order to prevent users from perceiving.

4) Latent

The computer virus has the ability to attach to other media, which is called the host computer virus. Relying on the virus's parasitic ability, the virus infects with the virus which is the legitimate program and the system does not immediately attack, but quietly hides, and then users are not aware of the case of infection. The virus latent, the longer it exists in the system, the virus transmission range is also the more extensive, the greater the harm.

5) Destructive

No matter what virus program once the intrusion system will have different degrees of impact on the operation of the operating system. The virus program does not directly cause damage, it also takes system resource. While the vast majority of virus program displays some text or an image of the normal operation of the system, there are some virus program delete files, disk data encryption, even destroy the whole system and data, which cannot be recovered and causes irreparable loss. Therefore, light side effects of the virus program reduce the working efficiency of the system, even lead to system crashes and data loss. The performance or failure of the virus program reflects the real intention of virus designer.

6) Non predictability

It is not expected that the virus detection, the code of different viruses varies widely.

7) Can be triggered

Computer viruses generally have one or more triggers. Meet its trigger conditions or activate the mechanism of the virus to infect, or activate the performance of the virus or damage part of the virus. The essence of the trigger is the control of a kind of condition. The virus program can carry out an attack according to the requirement of the designer. This condition can be typed in a particular character, using a specific file, a specific date or at a specific point in time, or built-in virus counter reaches a certain number.

Types of computer viruses. According to the computer virus attack operating system to classify: attack DOS system virus; Windows system virus; UNIX virus; OS/2 system virus; mobile phone virus etc..

According to computer virus attack type to classify: attack microcomputer virus; computer virus; workstation virus, etc..

Classified by computer virus: source type virus, embedded virus, shell virus, decoding virus, operating system virus, etc..

According to the degree of computer virus damage to classification:malignant virus; benign virus.

Detection and prevention technology of computer virus

The way of computer virus invasion. To be familiar with the detection method, the way of computer virus invasion must be understood at first. As the development of computer technology, the way of virus invasion is constantly updated and changed.

1) Removable storage device

Mobile hard disk, U disk and CD infection are major channels, because of a virus storage tools to move elsewhere in the use and maintenance, will clean the computer transmission and diffusion. The virus cannot be cleared on the disc for the read-only disc and can't be written.

2) Through the network

The spread is fast and can spread over the machine in a very short time. Internet brings two different security threats, a threat from file downloads, these are viewed or downloaded files may exist virus. Another threat from email.

Detection method for computer virus. According to the characteristics of computer viruses, people have found many computer virus detection, but no kind of detection method is universal, comprehensive use of these detection methods based on according to the characteristics of the virus in order to accurately virus is found.

Appearance detection method:

After the virus intrusion system, some parts of the computer system can change, and some abnormal phenomena are caused, such as screen appears anomalous rolling, or a regular anomalies, being unable to use the keyboard, the keyboard function substitution, computer buzzer appearing abnormal sound, abnormal hair into sounds or music; print speed reducing or being out of control; reducing the speed of the system work, magnetic disc guiding the crash phenomenon, abnormal decrease in computer storage system of the capacity of the storage device or not being stored in read and write phenomenon; missing files, file length changing, inexplicable file, file attributes change and so on.

Characteristic code method:

A virus may infect many files or the system of more than one place, and in each infected file, where the virus program in a different location, but a computer virus program generally has obvious characteristics of the code and the characteristics of the code, it may be virus infection marker. Feature code method steps: collect samples of the virus; virus samples in feature extraction code; the feature code into the virus database; open detected file, search in a computer system, check the computer system whether it contains virus database in the virus feature code.

Systematic data comparison:

The contrast method is a comparison of the original backup and the detected boot sector or a detected file. Comparison can be printed by the code list of comparisons, or procedures to compare. This comparison method does not need to use a special computer virus program, as long as conventional DOS and PCTOOLS software and other software can be carried out. And this comparison can find the computer viruses that cannot be found by the existing computer virus programs

Software simulation:

Its operating mechanism is: generally detecting tool into the software simulation method, these tools starts running, using characteristic code method for virus detection, if hidden virus or polymorphic virus are found, suspect that initiates software simulation module, HIV surveillance operation until virus since the password decoding, and then use the feature code method to identify the virus species.

Computer virus prevention technology

Computer virus prevention. Computer virus prevention refers through the establishment of reasonable computer virus prevention system and the system, timely detection of computer viruses, and to take effective means to prevent the computer virus propagation and destruction and recovery is subject to the influence of computer systems and data. The principle is to protect the computer virus as the initiative, mainly in the detection of the dynamic and preventive methods of the wide range of methods.

1) Windows account security

Windows account as the computer first level naturally cannot slack, a password is needed to become strong, being not easy to guess.

Right mouse hit “my computer”, management options, select the "user", remove the right side all users, in addition to the guest, administrator, the two built-in account, and users need to use the account, all the others do not leave, if users do not have administrator, it is suggested to add it on a very strong password, and then disable it and guest, ensure that only users’ personal account can use, put an end to the troubles.

2) Windows service

Start - > Run - > input sector.msc "and to determine the list on the left hand side of the - > in the left side of the tree list select the following" services and Applications ", then select" service ", will see a lot of things in the list on the right. Windows services are provided in many of them, and one more service is more dangerous and can stop and disable them.

3) Windows shared

Computer management clicks the shared folder in the left tree list, then choose to share, the right side of a list will appear, ADMIN$, D$, C$, E$. If users are required to share, server does not stop, IPC$ will not delete, in addition, users need to share the directory left, which can be said to be shared manager.

4) Close the automatic playback of mobile devices

5) Windows patch upgrade

6) Anti-virus, firewall, system optimization

Basic techniques, for cleaning computer viruses. The removal of computer viruses is not the only virus removal program, or the virus program cannot run, should as far as possible to restore the file system or true nature, to reduce the losses to the minimum. The removal method is different, but follows a definite principle.

1) The removal of computer viruses is the best in the nontoxic environment.

2) On the root system of the system disk and antivirus software on the disk, write protective tags to prevent its virus in the process of removing the virus.

3) Before removing the virus, it must be sure that the system or the file does exist, and determine the virus type accurately, in order to ensure the effectiveness of anti-virus.

4) Anti-virus work is in depth and comprehensive.

5) Try not to use the virus to detect the virus.

6) Virus cannot generally identify the virus.

7) Be sure to clean the computer and all the same viruses on the disk are clear and thorough.

8) For the same host program by several viruses cross infection or repeat infection, according to the reverse order of the infection from the forward sequence to remove the virus.

Computer system repairs. General repair methods for computer virus infection:

1) Firstly, a comprehensive understanding of the degree of damage to the system must be understood at first, and according to the extent of damage, determine which kind of effective computer virus removal methods and countermeasures should be used.

2) Before the repair, as far as possible to backup important data files.

3) Start the antivirus software and scans the whole hard drive.

4) After the discovery of a computer virus, the computer virus in the computer virus software is generally used to kill the virus in the file.

5) If the computer virus cannot be removed in the executable file, the general will be deleted.

6) Antivirus is complete. Restart the computer, again with anti whether there's a computer virus killing computer virus detection software system and determine infected damage data really is completely restored.

7) For the computer virus that cannot be cleared by anti-virus software, the computer virus sample should be sent to the research center of the software manufacturer for antivirus software for detailed analysis.

Conclusions

Computer virus prevention system construction is a social work, which cannot be realized by one single person or a company. It needs the participation of the whole society and makes full use of resources so as to be able to use the whole society of computer virus prevention system network. Although computer virus is terrible, computer virus prevention and safety strategies can avoid the infection of computer viruses and ensure the safety of the computer and network.

References

[1] Qingshui Xue, Yuanzhong Zhu, computer network security technology, Dalian University of Technology press, April 2010 first editions.

[2] Yongcan Guo, Qinglong Zhan, computer virus analysis and confrontation, Wuhan University press, October 2010.

[3] Beichang Wang, near the computer virus, people's Posts and Telecommunications Press, January 2011.

[4] Jianbin Yu, hacker attack means and user countermeasure, Beijing people's Posts and Telecommunications Press, June 2010.

[5] Ruinan Chi, Shi Shuhua, computer network security technology, people's Posts and Telecommunications Press, March 2009.