ISSN 2616-5775 Vol. 5, Issue 14: 33-39, DOI: 10.25236/AJCIS.2022.051405

Analysis of Computer Virus Defense Strategy Based on Network Security

Peihong Wang

HaniYi Autonomous Prefecture of Honghe Public Resources Trading Center, Mengzi, Yunnan, 661199, China
501376056@qq.com

Abstract: *Computer viruses seriously endanger computer network information security. After the computer is generated, the security of the computer network is attacked by computer computer virus every moment. Computer viruses in computer networks can be brought into the computer through e-mail, downloading software, browsing web pages, etc. The user will unknowingly bring the computer into the computer, causing serious harm to the user's information security. The virus is extremely stealthy, and once the computer is attacked, it is difficult for users to remove it in time, and in the case of undetectable, it will cause incalculable damage to the computer's system. Once discovered, it can cause great damage to the user's computer data. In the actual use process, as people's dependence on the Internet increases day by day, once attacked by the Trojan virus, it will greatly affect people's work and life. In this paper, through the analysis of the propagation mechanism and characteristics of computer network viruses, the corresponding preventive measures are proposed, in order to provide reference for the prevention of computer viruses in China.*

Keywords: *Network Security, Computer Virus, Defense Strategy*

1. Introduction

The 21st century is a networked century, computer network has been deeply into people's life and work, it has been widely used in various fields, which has promoted the production and living standard of society, but also has many negative effects. Because people are more and more dependent on the network, once the computer is attacked by Trojan horse virus, it will have a great impact on our work and life. In fact, not only the computer network technology is developing, but also the computer viruses spread through the network are getting stronger and stronger, which has become a destructive factor threatening the network security. Therefore, it is necessary to conduct an in-depth analysis of the propagation mechanism, and characteristics of network viruses and develop corresponding preventive measures accordingly.

2. Analysis of the Causes of the Spread of Computer Network Viruses

2.1. The Network Itself has Security Problems

Due to the highly shared and open nature of computer networks, and the fact that the Internet is composed of hundreds of millions of Internet users and terminals, it both facilitates the exchange and sharing of information and poses a great threat to the network. Once these viruses have invaded the user's computer, it is easy to make the user's computer not work properly, and in serious cases, it will be stolen and tampered with. In serious cases, it can paralyze the user's computer system and cause incalculable consequences [1].

2.2. Lack of Awareness of Safe Operation Among Users

Many people do not have a strong awareness of computer security when using computers, and cannot strictly comply with the norms of computer use. Many people do not have a strong awareness of the security risks of computer networks, and most users ignore the invasion of network viruses, do not repair vulnerabilities in a timely manner, and do not spend a lot of time to maintain their information, which gives lawless elements the opportunity to take advantage of the situation, thus leading to the

ISSN 2616-5775 Vol. 5, Issue 14: 33-39, DOI: 10.25236/AJCIS.2022.051405

leakage of users' personal information.

2.3. Malicious Human Attacks

The Internet has a complex user composition, and some people who are familiar with the network will exploit the security loopholes on the network to carry out malicious attacks, and these attackers usually spread viruses through the loopholes on the network, which affects the integrity and correctness of existing system information. When a user's network is attacked or damaged, it can cause leakage of certain sensitive information, resulting in huge economic losses [2].

2.4. Inadequacy of Computer Data Security System

The entire data of the computer is stored in the hard disk, and if the hard disk fails, it will provide an opportunity for the wrongdoers to take advantage of it. This is due to the fact that the current computer security system is not yet sound, it is difficult to effectively prevent various network attacks, so it is especially necessary to strengthen the storage and protection of information. Usually, users' computer terminals are equipped with various software to execute various programs, but some software is not downloaded from normal channels, and may have a "back door". In this case, when someone maliciously uses these backdoors to carry out virus attacks, it may cause damage to the user's computer system [3].

2.5. Virus Spreads Heavily in Emails

Email plays a pivotal role in people's daily work and life. Everyone will receive some inexplicable emails at one time or another, and criminals are fully capable of spreading viruses through emails. Once users open emails with viruses, they will be invaded by viruses, thus affecting the security of users' personal information. Due to the defects of email itself, it makes the user unable to refuse to receive emails, thus exposing his computer to cyber attacks. Cybercrime is an illegal act in which theft of passwords is the main means. By stealing the user's password, commercial fraud can be committed, thus causing great harm to the user's property.

2.6. Backward Firewall Technology

Through the full use of firewall technology, we can block the virus in the internal network environment of the computer, because the firewall technology has just started, the current firewall technology is not perfect, which makes some advanced viruses can break through the firewall, and then attack the internal information of the computer, which causes some harm to the security of the computer [4].

3. The Transmission Characteristics of Computer Network Viruses

3.1. Diversity of Dissemination Patterns and Strike Targets

Unlike traditional computer viruses, today's network viruses can spread through different ports and vectors, its target has shifted from the initial PC to workstations and large servers with network protocols, causing clogging and paralysis of the network and thus affecting a large number of users.

3.2. Diversity of Authoring Methods and Variations

Early computer viruses were based on assembly languages such as C. However, with the development of the Internet, the number of viruses written in scripting languages such as Jave and VB is also increasing, which leads to various types of virus mutations, thus making it difficult for anti-virus to prevent viruses [5].

3.3. High Doping Degree

In computer network viruses, using their own defense, encryption, stealth, tracking and other technologies, new viruses are constantly emerging, and they are becoming more and more stealthy and intelligent. At the same time, such viruses are more mixed with traditional viruses, worms and other

ISSN 2616-5775 Vol. 5, Issue 14: 33-39, DOI: 10.25236/AJCIS.2022.051405

viruses, and they are more lethal [6].

3.4. The Way Viruses Spread in the Network

The network provides a channel for the spread of computer viruses, which can be broadly classified into the following two categories, while the active spread pattern of viruses is shown in Figure 1.

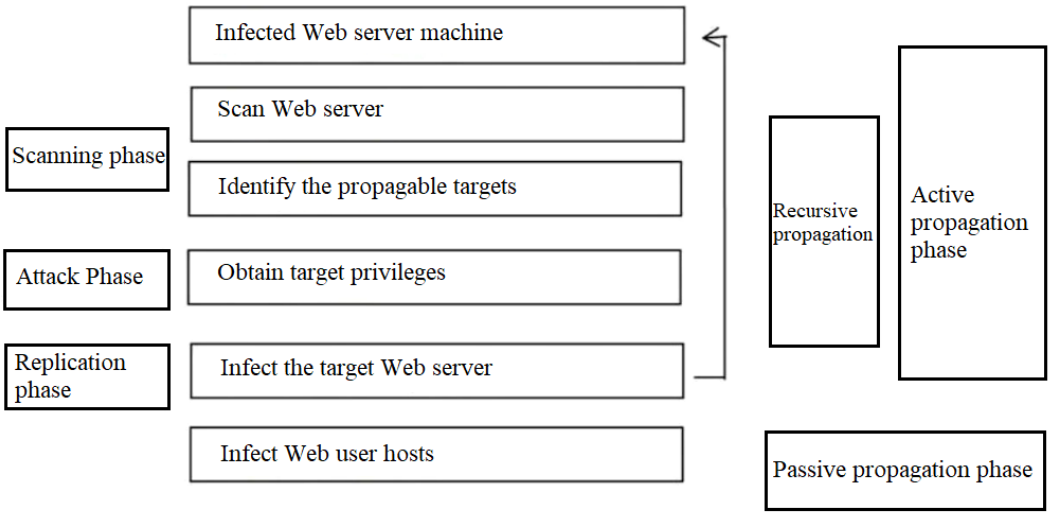

Figure 1: The main ways of spreading web viruses

3.4.1. Virus Transmission Through Communication

This is a special program belonging to computer data, which is not very different from ordinary documents, and data transmission through the Internet is an important means of virus attack. Industry experts have analyzed billions of e-mails for viruses, and found that millions of viruses have been detected through this communication method, from which it can be seen how important it is to spread this virus on the Internet. In the communication method, viruses are mainly infected with body text, attachments, etc. The virus will find a target address in your computer, and then send it to the user's attachment. Once the virus reaches its destination, it can take control of the infected computer in some way [7].

3.4.2. Efficient Scanning

The virus program can gain control of a computer by remotely scanning the network, and gaining access to the security vulnerabilities of the computer systems in a network, then implanting it into the computer. The virus is usually spread through multiple devices. When the device supplies computing services to a client, the virus provides security flaws to the computer service device and compromises the client, most typically Nimda.

4. Network Security Precautions and Key Technology Analysis

4.1. Network Model Security System

Establishing a security system of computer network model helps people to protect the security of the network effectively. Therefore, we have to follow the characteristics of the computer network itself, actively promote the establishment of a perfect computer network model security system, and really achieve effective protection of the security of the computer network, so as to achieve the purpose of saving manpower, material resources and improving the efficiency of resource use [8].

4.1.1. Optimized Technology Model

Computer network defense strategy optimization technology, which is based on the information and fine rules of network expansion, then transforming the network defense strategy into an operational level defense strategy. The defense strategy is designed for computer administrators, its purpose is to effectively advance the network security protection of computers, so that the computer security is guaranteed. Its main purpose is to enhance the access rights to users for the purpose of data security

ISSN 2616-5775 Vol. 5, Issue 14: 33-39, DOI: 10.25236/AJCIS.2022.051405

protection. The detection policy mainly detects external dangers and guards against foreign intrusion. And the recovery policy can repair high-level independent security functions [9].

4.1.2. Optimization of Technical Specifications

Advanced computer network defense strategies and the optimization of the operational hierarchy, which should follow the following basic guidelines. First, the statute of roles and users is refined to indicate the connection between users and roles. Second, the user-source node is optimized, where the source domain indicates the correspondence from the source area to the source. The principle of precision is the correspondence between users and source nodes in the source domain, the use of refined laws to correspond targets to resources, and to specify event occurrence, attacks, behaviors and actions [10].

4.2. Improving the Resistance of Computers to Viruses

Computer virus invasion is usually caused by human factors, and the core technology of computer system is human defense. Using mouse keyboard and other devices for operation will inevitably leave some traces on the computer. Therefore, to extract and analyze the traces of human activities from human labor, which must have a computer system. If a malicious program is found to interfere with the computer program, the user must be released from the next access operation. In addition, computer programmers can add code to the program code, with the related function, they can link the tracking code to the unauthorized access, once the user acts inappropriately, the user can be tracked, detected and stopped instantly, so that the spread of network virus can be effectively prevented. In order for a computer virus to spread through the network, it must first identify the vulnerabilities in the security strategy of the system, and use it as a breakthrough to attack. Once the virus has invaded the user's computer through the network, then it will gain the initiative to carry out a devastating attack on the user's computer, which causes a lot of data loss. At the same time, some special viruses will target devices such as SQLserver as the primary target of the attack [11]. Therefore, when defending against computer viruses, it is important to ensure the security of the system and avoid being invaded by viruses. According to the characteristics of the spread of computer viruses, the analysis of how to prevent computer viruses is carried out.

4.3. Computer Virus Detection Technology

Since the creation of computer viruses, experts and scholars in the industry have been developing various types of anti-virus software, and after continuous efforts, there has been some success in applying anti-viruses to the computer inside, which can play a good defense role. Most of the anti-virus programs are used to determine the virus by detection to prevent virus invasion. At present, there are various methods of computer virus detection, which are representative [12].

4.3.1. Characteristic Code Base

This is an early method of virus processing, mainly used for CPAV diagnosis. This method will break down and parse the virus code while scanning and save it to a database. Once the user starts this antivirus software, then the signature code will compare the scanned data with the code in the database, and if there are similarities between the two, then it can be identified as a virus. The detection process of the signature code for this virus is like this. Based on a computer, a virus database is constructed to collect samples of current popular viruses, and store them in a built-up database. After the program starts, different codes are made according to the viruses in the database, and the detected information is compared with this code, when the similarity reaches a certain threshold, it is determined to be a new type of virus. Although this technique has a high detection accuracy for viruses, it cannot be analyzed because the virus is always updating itself, and when a new virus is detected, it cannot be analyzed because the corresponding code is not available. Therefore, the application of this technique is limited [13].

4.3.2. File Inspection

A virus itself is a program that contains a large amount of data, which is usually in a stored form in a computer file. Because there are so many viruses, once they are saved in a file, then that file becomes larger. File checking takes advantage of the characteristics of such viruses to check. Normally, the virus protection software within the computer will be based on the security of the system, the inventory of all files is made and each program is checked. If a file is found to be very different from previous checks, then it is possible that it is infected by a virus. In this way, not only known viruses can be detected, but

ISSN 2616-5775 Vol. 5, Issue 14: 33-39, DOI: 10.25236/AJCIS.2022.051405

also some unknown new viruses. The more common methods of file checking are as follows. First, add the file checker to the computer system's anti-virus software, activate it when the anti-virus software is running to detect and protect with the anti-virus software. Secondly, the file checking program is implanted into the computer's application program, and once it is started, it will be checked automatically. Finally, the file checking program is written into the computer system's memory, and then detects viruses when the program is started [14].

Although file checking can effectively detect viruses, it can only determine the presence or absence of a virus, but not the type of virus and the threat it poses to the computer. However, in practical applications, there are often checksum errors, which can lead to false positives.

4.3.3. Virus Characterization Detection

Different viruses have their own unique characteristics that can be used to effectively detect the virus itself, which is called behavioral inspection. Currently, the viruses that are popular on the Internet are basically written by hackers. They are distributed through the Internet to invade the user's computer and steal important information.

4.3.4. Simulation Testing

It can be used to discover the working mechanism of a virus by replicating and emulating the current operating state of the computer, from which the similarities and differences between the two can be identified. Software emulation is a very effective method, its can be used for complex viruses and also for encryption [15].

4.4. Standalone Antivirus Technology

The network is the main means of virus transmission, and the computer system is the final destination of transmission. In order to gain control of the computer, it must be invaded. If the computer itself is not sufficiently protected against viruses, it is difficult to protect against such viruses. Therefore, virus protection for individual computers becomes very important. Anti-virus software is currently the most effective means of protecting individual computers against viruses, and it can protect personal computers to a certain extent against virus invasion in the network. Anti-virus software belongs to the software category, with the function of cleaning up viruses, some anti-virus programs, it will automatically recover the information, which is the most efficient protection measures at present. Currently more commonly used anti-virus programs are 360 Security Guard, Norton Anti-Virus, etc.. Among these systems, 360 anti-virus program performs much better, it is a completely free, efficient, low consumption of system resources, regular upgrades of cloud anti-virus software. What's more, 360 anti-virus program, which can co-exist with other anti-virus systems and does not attack each other, it is the best defense system [16].

4.5. Virus Defense Measures for Multiple Computers Online

In order to meet specific antivirus needs, there are often multiple computers connected to each other in the same area, so that they can share data and information with each other. Once one computer is invaded by a network virus, the other computers will also be infected. To deal with this situation, we can take the following measures to prevent it. Set up a virus defense system, set up virus monitoring software and establish a connection with the virus monitoring center, and then monitor the operation of each computer in real time. Once found, quarantine immediately. At the same time, anti-virus software is distributed to each computer to prevent the invasion of certain specific viruses.

4.6. LAN's Antivirus Technology

The best feature of LAN is its small geographical scope. LAN is a closed and simple network architecture, many businesses and enterprises often choose LAN for their offices. LAN is a private network, which can connect computer systems and databases in a certain area to form a communication network. When the LAN is attacked, the computers and databases in the LAN are attacked, so it is necessary to strengthen the defense of the LAN, which requires effective means and tools.

4.7. Enhanced Anti-virus Performance of the Gateway

The gateway is a key link to prevent computer viruses. In order to avoid the spread of viruses in the

ISSN 2616-5775 Vol. 5, Issue 14: 33-39, DOI: 10.25236/AJCIS.2022.051405

intranet, it is necessary to strengthen the virus detection capability of the gateway and build an effective anti-virus mechanism. With the development of the Internet, e-mail has become an important means of information transmission, especially in government agencies, companies and other organizations. To effectively stop virus invasion, we need to give full play to the mail gateway's interception and screening capabilities, so that it can automatically detect viruses in emails on the network and filter fake and malicious emails. At the same time, when the gateway finds irregularities, it will immediately trigger the firewall's chain defense and issue action commands to the gateway, so that the virus is quickly isolated from the gateway, thus preventing the virus from causing harm to the gateway.

4.8. Improving Computer Confidentiality

In computer networks, there are a large number of security risks, the most serious of which is the leakage of computer information. This requires the technical personnel concerned to improve the confidentiality of the computer, and then improve the security of the computer, especially in some subtle points. Only by establishing the right security system can the problem of information leakage be reduced. Confidentiality of data is a very important issue in computer systems. In order to protect network users and information resources from damage, it is necessary to ensure its security. Therefore, we have to research and develop the firewall, maintenance management and virus prevention, so that we can ensure that the security performance can be effectively played. Software encryption technology can also be used to shield some illegal programs in one form or another, so as to limit hackers from invading computer systems or stealing confidential information. In addition, we need to strengthen the confidentiality of documents in the data files, because users use a large number of electronic version of the operating system in the network, which will lead to the storage of this information on the server.

5. Conclusion

The security of information systems is a pressing issue today. Many scientists are working on everything from security models to specific security techniques, but the models and security techniques currently in use are limited to one or more applications to information security. It can be seen that the way of network intrusion is constantly changing, the means of attack is increasing, and advanced stealth attack techniques are becoming increasingly popular. In the face of an increasingly complex and changing network environment, techniques such as establishing firewalls and actively identifying threat characteristics can no longer be adapted to the current security requirements of information systems. At present, many scholars address the current situation of network security, and combine artificial immunity technology and network security organically. Establishing a new type of network security system, which is a new research hotspot on information security issues in the international arena at present. This paper discusses the main strategies and technologies of computer network security from the current security problems of computer network information, and gives the corresponding solutions. It not only has the characteristics of fast computing speed, but also has powerful data storage and so on. The emergence and wide popularity of computers have greatly changed the way people work, live and learn. Computer virus is a kind of virus that comes with the computer, which can be destructive to the computer system and can spread on the computer or on the cell phone. If a computer is infected by a virus, it will not only affect the normal operation of the computer, but also cause the loss of important information in the computer, which can seriously paralyze the computer and even damage the computer hardware. Therefore, it is very necessary to effectively prevent viruses. This paper intends to make a brief analysis and discussion on the spread of computer viruses on the network and protection methods, hoping to help the industry.

References

[1] Ravi Tomar, Yogesh Awasthi. A Systematic Review of Network Security Breaches and Solutions[J]. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2020, 9(11): 125-128.

[2] Wu Xu, Wei Dezhi, Vasgi Bharati P., Oleiwi Ahmed Kareem, Bangare Sunil L., Asenso Evans. Research on Network Security Situational Awareness Based on Crawler Algorithm[J]. Security and Communication Networks, 2022:26-32.

[3] Jialin Chen, Zheng Zhou, Yi Tang, Yi He, Shiwen Zhao. Research on Network Security Risk Assessment Model Based on Grey Language Variables[J]. IOP Conference Series: Materials Science and Engineering, 2019, 677(4):177-181.

ISSN 2616-5775 Vol. 5, Issue 14: 33-39, DOI: 10.25236/AJCIS.2022.051405

[4] Yu Tianxi, Yin Xiaoyao, Yao Menglin, Liu Tong. Network Security Monitoring Method Based on Deep Learning [J]. Journal of Physics: Conference Series, 2021, 1955(1):236-241.

[5] Bai Yong, Huang Dong, Liao Yong, Pen Guangbin, Xu Luyao, Deng Yongsheng, Wang Chun. Information Network Security Situation Awareness Technology Based on Artificial Intelligence[C]//. Proceedings of 2019 International Conference on Information, Communication Technology and Automation(ICICTA 2019).Francis Academic Press,2019:58-62.

[6] Yang Yang. Construction of Network Security Law Enforcement Virtual Simulation Experiment and Teaching Platform[C]//.Proceedings of 2021 6th International Conference on Education Reform and Modern Management (ERMM2021).2021:165-169.

[7] Shahid Naveed, Aziz-ur Rehman Muhammad, Khalid Asma, Fatima Umbreen, Sumbal Shaikh Tahira, Ahmed Nauman, Alotaibi Hammad, Rafiq Muhammad, Khan Ilyas, Sooppy Nisar Kottakkaran. Mathematical analysis and numerical investigation of advection-reaction-diffusion computer virus model [J]. Results in Physics, 2021:98-102.

[8] Dong Nguyen Phuong, Long Hoang Viet, Giang Nguyen Long. The fuzzy fractional SIQR model of computer virus propagation in wireless sensor network using Caputo Atangana–Baleanu derivatives[J]. Fuzzy Sets and Systems, 2022:458-462.

[9] Madhusudanan V.,Srinivas M.N.,Nwokoye C.H.,Murthy B.S.N,Sridhar S.. HOPF- BIFURCATION ANALYSIS OF DELAYED COMPUTER VIRUS MODEL WITH HOLLING TYPE III INCIDENCE FUNCTION AND TREATMENT [J]. Scientific African, 2022(prepublish):109-116.

[10] Titus Ifeanyi Chinebu, Ikechukwu Valentine Udegbe,Edmund Onwubiko Ezennorom. Analysis of Optimal Control Strategies for Preventing Computer Virus Infection and Reduce Program Files Damage with Other Symptoms [J]. Journal of Scientific Research and Reports,2021:361-365.

[11] Coronel Aníbal, Huancas Fernando,Pinto Manuel. Sufficient conditions for the existence of positive periodic solutions of a generalized nonresident computer virus model[J]. Quaestiones Mathematicae, 2021,44(2):111-119.

[12] Raza Ali, Fatima Umbreen, Rafiq Muhammad, Ahmed Nauman, Khan Ilyas, Sooppy Nisar Kottakkaran, Iqbal Zafar. Mathematical Analysis and Design of the Nonstandard Computational Method for an Epidemic Model of Computer Virus with Delay Effect: Application of Mathematical Biology in Computer Science[J]. Results in Physics,2020(prepublish):208-212.

[13] Muhammad Shoaib Arif, Ali Raza,Muhammad Rafiq, Mairaj Bibi,JaveriaNawaz Abbasi,Amna Nazeer,Umer Javed. Numerical Simulations for Stochastic Computer Virus Propagation Model[J]. CMC: Computers, Materials & Continua, 2020,62(1):36-45.

[14] Coronel Aníbal, Huancas Fernando, Pinto Manuel. Sufficient conditions for the existence of positive periodic solutions of a generalized nonresident computer virus model[J]. Quaestiones Mathematicae, 2019:251-255.

[15] Nauman Ahmed,12,Umbreen Fatima,Shahzaib Iqbal,Ali Raza,Muhammad Rafiq,4,Muhammad Aziz-ur-Rehman,Shehla Saeed,Ilyas Khan,Kottakkaran Sooppy Nisar. Spatio-Temporal Dynamics and Structure Preserving Algorithm for Computer Virus Model[J]. Computers, Materials & Continua, 2021, 68(1): 267-274.

[16] João N.C. Gonçalves, Helena Sofia Rodrigues, M. Teresa T. Monteiro. Preventing Computer Virus Prevalence using EpidemiologicalModeling and Optimal Control[J]. Discontinuity, Nonlinearity, and Complexity, 2020,9(2);101-106.