Research on LAN Network Malicious Code Intrusion Active Defense Technology

Lei Ma(✉), Ying-jian Kang, and Hua Han

Telecommunication Engineering Institute, Beijing Polytechnic, Beijing, China
malei235@tom.com

Abstract. Traditional LAN networks had low defense efficiency and poor stability. In order to solve this problem, a new malicious code intrusion active defense technology was studied, and the defense technology structure was designed and the work-flow was studied. The system structure was divided into hardware layer, kernel layer and executive layer. The work-flow was divided into four steps: file judgment, file compression, file processing and file display. The working effect of the technology was verified by comparison with the traditional method. It was known from the experimental results that the studied technology had high defense efficiency and strong stability.

Keywords: Local area network · Malicious code · Code intrusion · Active defense

1 Introduction

Malicious code refers to a set of instructions that run on a computer and the system performs tasks according to the attacker's wishes. The term "malware" is used in the Microsoft Computer Virus Protection Guide as a collective noun to refer to viruses, worms, and Trojan horses that intentionally perform malicious tasks on computer systems. According to the running characteristics of malicious code, it can be divided into two categories: the program that needs to be hosted and the program that runs independently [1]. The former is actually a fragment of the program, they cannot exist independently of certain specific applications or system environments. Independent programs are complete programs that the operating system can schedule and run; According to the spread characteristics of malicious code, malicious programs can also be divided into two categories that cannot be self-replicating and self-replicating [2]. The specific malicious code types are shown in Table 1.

At present, malicious code targeted attacks are getting stronger and stronger, and personal online banking accounts, game accounts, and Internet accounts have become new targets [3]. It can be seen that if the security of the internal network terminal is not fully protected, the malicious code is bound to enter the internal terminal at will, blocking the operation of the anti-virus software, installing and setting the backdoor program, and stealing the password. Moreover, ARP spoofing infects the entire intranet to occupy network bandwidth, which seriously affects work efficiency and increases support costs, causing the company's intellectual property and personal property to be stolen and lost. The means of malicious code dissemination has become diversified.

G. Gui and L. Yun (Eds.): ADHIP 2019, LNICST 301, pp. 57–64, 2019.
https://doi.org/10.1007/978-3-030-36402-1_6

Table 1. Malicious code type.

Malicious code name	Failure mode
Computer virus	It needs a host and can be replicated automatically
Worm	An independent program; automatic replication; less human intervention
Malicious mobile code	Composed of lightweight programs; independent programs
Back door	Separate program segments, providing intrusion channels
Trojan Horse	The general need for a host; a strong concealment
Rootkit	Generally need a host; replace or modify the system state
Combined malicious code	A combination of the above technologies to enhance failure capacity

In the early days, malicious code was mainly spread through emails, system vulnerabilities, network shares, files, and so on. And the mode of communication is mainly by attracting users to click. With the development of the network, the channels and methods of information exchange and sharing are more diverse and convenient, but it also brings about the diversification of malicious code transmission [4]. There have been transmission methods such as attacks, online horses, exploits, mobile storage devices, network sharing, and network downloads. Among them, mobile storage devices such as infected disks, and the use of infected LANs and web pages have become the most popular three routes. And these three complement each other, can effectively improve the spread range and ability of the virus, as long as there is a computer poisoning in the LAN, the virus will soon spread to the entire network. It can cause network congestion such as network congestion and theft of confidential information, which poses a great threat to the normal operation of enterprise LANs and campus networks [5].

The main shortcomings of the traditional defense against malicious code intrusion technology are as follows: (1) According to CERT statistics, nearly 90% of malicious code infections are exploited by system vulnerabilities, and traditional viruses are used to kill and cure the symptoms. (2) The virus database update is lagging behind, and it is impossible to guarantee the killing of the latest virus, worm, Trojan and other malicious code. (3) The anti-virus software uses the feature matching method to detect and kill the virus, and cannot detect and kill the new malicious code. (4) After the malicious code infects the terminal, the anti-virus software is first stopped, and the anti-virus software is difficult to isolate. Since traditional eigenvalue-based scanning-based anti-virus software is very passive, the industry's defense method that can actively detect and intercept unknown threats is called "active defense" [6]. Active defense refers to the anti-virus technology based on behavior detection, that is, the virus behavior blocking technology that determines whether it is a virus and processes it through the behavioral characteristics of the virus. The technology combines the characteristics of these viruses to determine whether they are viruses by extracting the common characteristics of computer viruses, such as modifying the registry, self-replication, and constantly connecting to the network. That is to say, the behavior of the whole process is monitored, and once the "violation" behavior is found, the user is notified or the process is directly terminated.

The protection of malicious code can not be solved by one or several technologies alone. It is a system engineering, relying on the common prevention of technology, management and user security awareness. Only the combination of technology, management, and security awareness can prevent malicious code from destroying system and user information to the greatest extent. This paper designs a malicious code defense system based on Windows platform - AV-System. The system is based on active defense. From the perspective of defense, the malicious object's destruction object is protected, and the destructive power of malicious code is greatly reduced.

2 Lan Network Malicious Code Intrusion Active Defense Technology Structure Design

The structure of the malicious code defense system AV-System based on the Windows platform is as shown in Fig. 1:

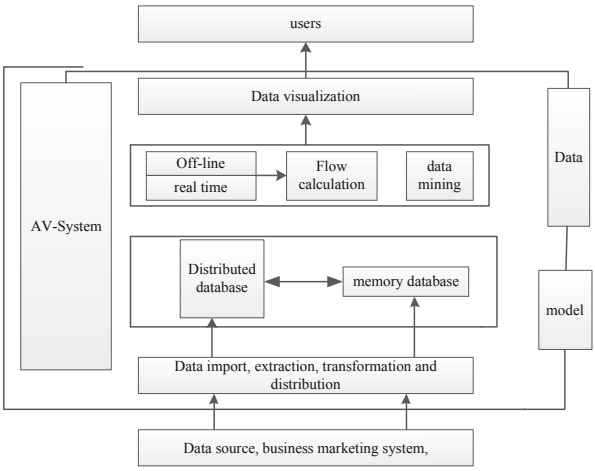

Fig. 1. Malicious code defense system AV-System structure

Looking at Fig. 1, this layer of direct dealing with hardware is called the hardware abstraction layer. The purpose of this layer is to isolate all hardware-associated code logic into a specialized module. So that the above hierarchy is as independent as possible from the hardware platform. Above the hardware abstraction layer is the kernel layer, sometimes called the microkernel, which contains basic primitives and functions such as threads and processes, thread scheduling, interrupt and exception handling, synchronization objects, and various synchronization mechanisms [7]. Above the kernel layer is the execution layer, the purpose of this layer is to provide some functions and semantics that can be directly called by the upper application or kernel driver. The kernel's executable contains an object manager for consistently managing objects in the executable. The execution body layer and the kernel layer are located in

the same binary module, that is, the kernel base module. The kernel layer and the execution layer are divided. The kernel layer implements the basic mechanism of the operating system, and all the policies are decided to be left to the executable. Most of the objects in the executable encapsulate one or more kernel objects and are exposed to the application in some way, such as object handles.

3 Lan Network Malicious Code Intrusion Active Defense Technology Work-Flow Analysis

The malicious code prevention technology based on Windows platform is a more complicated work, and the working process is as shown in Fig. 2:

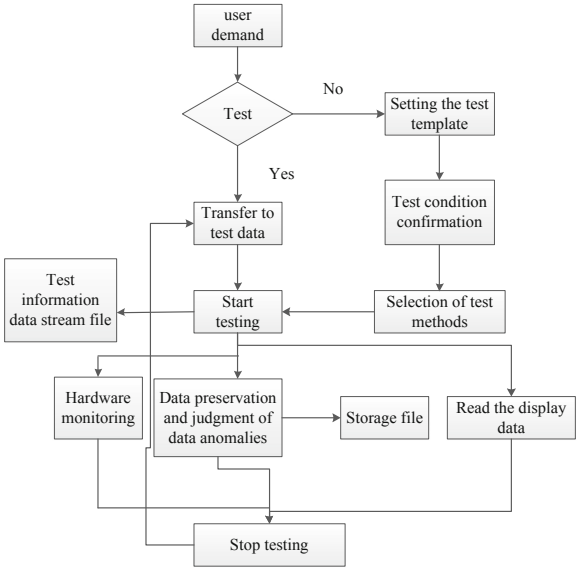

Fig. 2. Based on the Windows platform for malicious code prevention technology flow

The work-flow of Fig. 2 is described in detail as follows: The file type is judged by the type detection module. This is the premise for classifying the malicious code. For the compressed file, the file is decompressed first, and then the extracted file is returned to the type detection module for processing [8]. Consider a recursive decompression module that handles problems such as multiple and mixed compression. For non-compressed types of objects, there are different ways of handling them depending on the type. For the executable file, first of all, through a shell detection module, to determine whether it has passed, and the current popular executable file packer processing. This shelling module is also recursive until it is not required to be unpacked, and finally handed to the binary detection engine for processing [9]. For text type files, the main purpose is to perform script virus detection, which is first handed to the parser

for processing, and the result of the parser is then passed to the detection engine for matching processing. The macro virus detection of some anti-virus software is done by the script processing engine. The source code of the macro is extracted by the pre-processor, and then passed to the parser [10].

The host of the propagation model maintains three states that are susceptible to infection, infection, and immunity. The differential equation expression for the model is:

$$\frac{dJ(t)}{d(t)} = \beta J(t)[N - J(t)] \tag{1}$$

$$\frac{dR(t)}{d(t)} = \gamma I(t) \tag{2}$$

$$J(t) = I(t) + R(t) = N - S(t) \tag{3}$$

In the formula, I(t) represents the number of hosts that are still infectious at time t; R(t) represents the number of hosts that have been immunized from the infected machine at time t; J(t) represents the number of all infected hosts at time t, including those that are still infectious and have been immunized from the infected machine. β is the infection rate; γ is the recovery rate of the host removed from the infected machine; S(t) represents the number of hosts that are still vulnerable at time t; N represents all node hosts in the network. When the infected node is immune, it is equivalent to remove this node from the entire network node host, and the total number of network nodes changes from N to N-1.

4 Experimental Study

In order to detect the management effect of the malicious code intrusion active defense technology of the LAN network studied in this paper, compared with the traditional technology, a comparative experiment was designed.

4.1 Experimental Parameters

The experimental parameters are as follows (Table 2):

Table 2. Experimental parameters.

Project	Parameter
Operating system	Windows XP SP3
Cpu	Intel Core 2 T5750
Virtual machine	Vmware workstation
Debugger	WinDbg X76
Memory	2 GB
Compiler	IFS DDK 2005
Development tool	VC++ 6.0 SP6

4.2 Experiment Procedure

Experiments were carried out according to the parameters set above, and the working results of the two methods were analyzed and compared.

4.3 Experimental Results and Analysis

The experimental results obtained are shown below.

Looking at Fig. 3, we can see that the defense efficiency is increasing with time, but the efficiency of the defense system in this paper is always higher than the traditional method. This article's defense system is able to detect malicious code attacks in a timely manner and prevent further spread of malicious code. It is a new way to effectively defend against malicious code attacks.

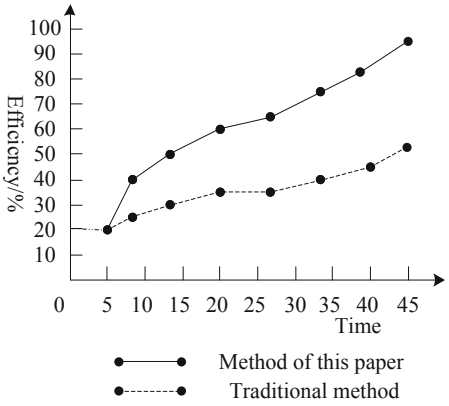

Fig. 3. Defense efficiency experiment results

4.4 Experimental Results

According to the above experimental results, the following experimental conclusions are obtained: Although both the traditional method and the method can prevent malicious code intrusion, the active defense system of this method can indeed intercept the unknown virus or Trojan. The process monitoring module, the registry monitoring module, and the file access monitoring module all run well. The process detection tool and the file detection tool can detect hidden processes and files well. In the process of using, the protection of files, registry, and processes is realized under the condition that the resources are scarce. The efficiency and stability of the operating system are both good, and will not cause any bad feedback to the user, and achieve the expected results.

5 Conclusions

In the communication network engineering, risk assessment and safety protection work protection have been carried out for many years, and certain experience and achievements have been obtained. With the development of communication technology, the deepening of network interconnection applications, the security of computer systems and the security of network security of communication networks are increasing. Traditional passive defense technologies have been unable to cope with the current automated, complex and large-scale network attacks. The active defense technology system can be effectively applied to the construction of network security assurance projects, which can ensure the safe and reliable operation of the network and meet the communication security requirements. Accurately analyze the causes of communication failures and security incidents, and develop and adopt effective solutions and countermeasures to provide a basis for scientific decision-making. The research results will help to analyze the security posture of the network operation, enhance the network operation, maintenance and management level, and improve the reliability of the system.

This paper first studies the development of malicious code prevention technology at home and abroad, analyzes the current status of automatic detection of malicious code at home and abroad, and points out their problems. Then research on the technology related to malicious code prevention: Windows kernel mechanism, Windows file system filter driver, Windows service, Windows device driver preparation, Windows PE file principle, registry principle. Based on the research of the above related technologies, a malicious code prevention system AV-System based on Windows platform is designed and implemented. Based on the research of the above related technologies, a malicious code prevention system AV-System based on Windows platform is designed and implemented.

References

1. Wang, Z., Yu, A., et al.: Construction of network security immune system. Eng. Sci. Technol. Power Monit. Control Syst. Trusted Comput. Technol. **49**(2), 28–35 (2017)
2. Tong, Q., Zhang, Z., Wu, J.X.: Inf. Secur. J. Divers. Hardware Softw. **2**(1), 1–12 (2017)
3. Intrusion detection research and implementation based on pattern recognition method. Hubei Mechanization **12**(6), 61 (2017)
4. Network security active defense technology and application. Netw. Secur. Technol. Appl. **56**(5), 28 (2017)
5. Wang, Z., Yu, A., et al.: Based on trusted computing technology, the network security immune system of power monitoring and control system. Eng. Sci. Technol. **49**(2), 28–35 (2017)
6. Li, X.: Analysis of the design and implementation of network active defense system. Electron. Des. Eng. **25**(1), 27–30 (2017)
7. Wang, Z., Hu, H., Cheng, G., et al.: The architecture of mimic defense under the software definition network architecture. Netw. Inf. Secur. J. **3**(10), 52–61 (2017)
8. Su, S.X., Zhu, Z.: Design and implementation of embedded active defense system based on honeypot. Internet Things Technol. **7**(7), 86–88 (2017)

9. Yu, A., Wang, Z.H., Zhao, B.: Research and application of trusted computing technology in power systems. Inf. Secur. Res. **3**(4), 353–358 (2017)
10. Chen, J.: Mobile network optimization design for effective intrusion prevention design of intrusion signals. Comput. Simul. **34**(7), 277–280 (2017)