Advances in Intelligent Systems Research, volume 132
2nd International Conference on Modelling, Simulation and Applied Mathematics (MSAM 2017)

Research on the Hidden Technology of Troy Trojan-Horse

Ting Mao, Shengbing Che and Wei Deng*
Central South University of Forestry and Technology, Chang Sha, 410001, China
*Corresponding author

***Abstract*—The hidden technology of Trojan horses was investigated. Through the analysis of the original Trojan hiding technology, it improved the local hiding ability of the Trojan horse and construe randomly selected octed the Trojan horse which embodied the collaborative hiding ability. I put forward a Trojan horse hiding technology framework which based on the DLL. By using the remote thread technology which inserted the DLL Trojan into system process whose name was svchost.exe, which realized hidden operations of the Trojan horse. When using the remote thread technology to start-up Trojan, one of the svchost.exe as a host process. It increased the difficulty of killing the Trojans, enhanced the concealment, improved the overall anti Trojan detection and anti killing ability.**

Keywords-trojan horses; hiding technology; network security; DLL technology

I. INTRODUCTION

As a kind of computer network viruses, Trojan horse is an important aspect of network security, and it is also an important way to obtain information in the network attacks. Broadly speaking, Troy Trojan belongs to a kind of computer viruses, however, it is not the same with the computer viruses as it has its own characteristics. First of all, the concealment of Trojan horse is strong. When the Trojans invade the system successfully, it has its own unique hiding mechanism to avoid being aware of the user, which is the key of completely killing the Trojan horse. What is more，Trojan horse is essentially a kind of monitoring program， unauthorized and remote. Controlling and accessing to the targetcomputer is not approved by the legitimate user, which is determined by the nature of the Trojan horse[1]. Finally, Trojan horses have the same communication with the viruses. The common feature of malicious programs is the idea of trying to make themselves infected with more computers and covering a wider range. Trojan program is no exception.

In order to improve their viability, trojan horses used a variety of means to disguise the hidden ability so that the infected system showed normal. Such as those by Fred Cohen conducted a thorough study of the virus, they took the Trojan horse as a special case of the virus and gives the mathematical model of the virus and trojan horses, but they did not analyze the hidden features of trojan horses[2] . Harold Thimbleby studied virus and Trojan model framework and presented a formal model of Trojan. Trojan horses' hidden features are described, but the cooperative concealment of trojan horses isn't described and analyzed. the Trojan horse hidden under in the Linux environment (including collaborative hiding) has been studied by Zhang Xinyu, but did not involve the Trojan horse hidden in the Windows environment.

In this paper, based on the research of Trojan horse hiding technology, I puts forward the improvement of the hiding local and puts forward the prototype of the Trojan horse, which improves the ability of hiding and surviving. It is of great significance to study the Trojan horse technology in order to prevent trojan attack and reduce network damage

II. THE COMPOSITION AND WORKING PRINCIPLE OF TROJAN HORSE

While there are many kinds of Trojan horses, but the basic composition of the Trojans are the same. The trojan horse is essentially a client/server model (C/S) special computer program. Usually Trojan program is divided into server (Server) and client (Client). The server program is a part of that the trojan invaders uploaded to the host computer. The system is monitored by system vulnerabilities or binding. The client program is part of that the intruder controls the target host, also known as the monitoring side. Its role is to connect the server-side program and then the intruder send the command through it.

The basic working principle of trojan horses: After the server program is successfully implanted in the target host and then sets up a predetermined port. The implementation of the monitoring port. If the client to the server of the proposed port connection request is authenticated successfully after the remote monitoring function of the server will automatically activate the program, and wait for the client to send out monitoring command. Server program to achieve a variety of remote monitoring functions according to the command type. The schematic diagram of the Trojan horse is shown in Figure I.

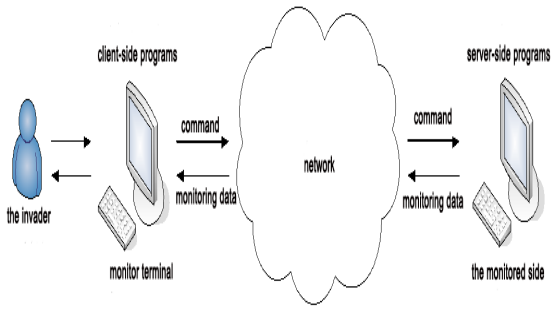

FIGURE I. WORKING PRINCIPLE OF TROJAN HORSE

III. HIDING TECHNOLOGIES

Trojan horse is a kind of illegal remote monitoring program, and it is the biggest difference with the conventional remote monitoring program. Trojan horse has a strong ability to survive. Trojan's viability is very important. If the trojan can easily be found and deleted, it is difficult for it to complete the monitoring task, replaced by exposing their identity. Furthermore, it may also be attacked by the monitor[3]. Hiding technology is one of the key technologies of Trojan horse. This paper analyzes and studies the hiding technology of Trojan horse from 3 aspects: local hiding, communication hiding and cooperative hiding.

A. Local Hiding

Trojan' boot requires a very strong concealment and deception. When it implanted successfully, you need a Trojan program can be automatically loaded, or it can run automatically when the trigger in some specific conditions. There are 3ways to realize the concealment of initiative mode: first of all, with other documents bundled or inserted into the document to complete the hidden start; with the registry associated hidden start; complete hidden start through some special or specific file system. These start-up methods need to modify relevant documents of the system. They are easy to detect by tools. Based on the common methods to modify the registry, using API HOOK technology hook function such as ExitWindowEx, trojans turn to the implementation of the default ExitWindowEx function shut down or restart the system and avoid the detection from the registry monitoring tools by shutting down the system before the Trojans add boot operation.

B. File Hiding

File hiding includes two aspects .One is that disguising itself and confusing the user. The other is hidden Trojan files. In addition to modifying the file property name, and it will be stored in the system directory; Hidden trojan files can modify procedures which are related with the file system operation to filter out information about trojans.

In order to prevent the detection of the operating system and the third party software, the trojan code can be stored in a special area of the system. Normally, there is a gap in the system disk. As shown in Figure II and Figure III, The trojan ,hidden in these spaces, will escape the detection of third party software to achieve the purpose of hiding.

C. Process-Concealment

Process-concealment, which is that users can not find the running process of the Trojan horse by some means, or the current trojan program does not exist in the form of a process or service. Process-concealment of trojan horses includes two aspects: fake hiding and true hiding. Fake hiding, refers to the process of Trojan program still exists, but disappears in the list of processes; True hiding, letting the program completely disappear, no longer work as a process or a service mode. Process-concealment is mainly used in the Windows system.

1) Fake hiding

Fake hiding is that a Trojan horse exits in the system with the form of system services. In the Windows system, it is allowed that a process is registered as a system service. Once it registers successfully even if you call the task manager can not see the trojans. This way of process-concealment can't be detected by professional testing tools.

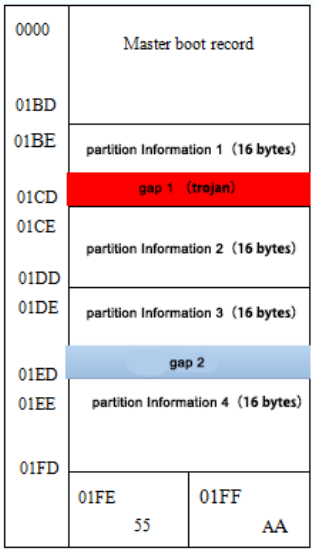

FIGURE II. ONLY PRIMARY PARTITION DISK STRUCTURE

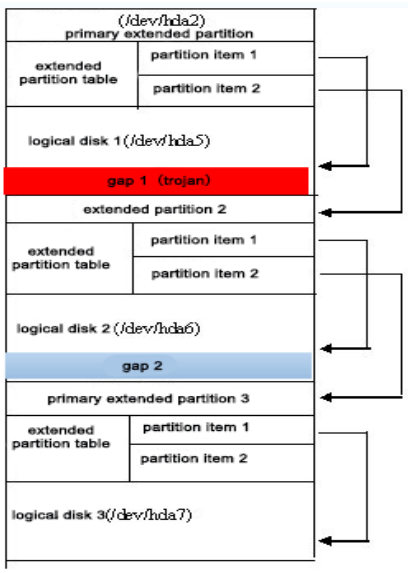

FIGURE III. DISK STRUCTURE WITH EXTENDED PARTITION

2) True hiding

The basic principle of fake hiding is that function codes plus with some special codes are written a DLL file and export related API. DLL file with complete trojan function is inserted into the remote process in a thread or DLL way[4]. Furthermore, the running of the DLL file does not produce additional process. Compared with the traditional EXE trojan, it is difficult to be found as to achieve the purpose of hiding.

The start-up process of DLL trojan horses: Using dynamic and embedded technology, DLL is hanging in a normal system process by using a trojan loader. Besides, the embedded

process called DllMain functions, stimulating the operation of the Trojan horse and loading processes The most common dynamic embedding technologies include HOOK, API, remote thread technology. By using the remote thread technology which inserted the DLL Trojan into system process whose name was svchost.exe, which realized hidden operations of the Trojan horse. Svchost.exe is a special process. You can open the task manager to view the list of processes and find many names for svchost.exe process. Although these svchost.exe processes have the same name, they can be distinguished from the parameters. When using the remote thread technology to start the trojan, one of the svchost.exe is chosen as the host process, which increases the difficulty of killing horses.

D. Kernel Module Hiding

Kernel level Trojan horse prototype BOES(Back Orifice for Electronic Scout) provide remote and control functions of common trojans, such as remote file operations, registry operations, screenshots, remote command line interpreter, using Rootkit to realize the hidden of files, processes, registry and communication port. Rootkit can be achieved through two levels, namely user mode Rootkit and kernel mode Rootkit. Kernel mode Rootkit for all users of the system and the kernel memory space with full access, can modify any program code and data structure system. But kernel mode Rootkit needs a driver into the kernel, using many API functions of bottom. High complexity easily lead to instability of system, so BOES uses mixed- type Rootkit (The structure is shown in Figure IV).

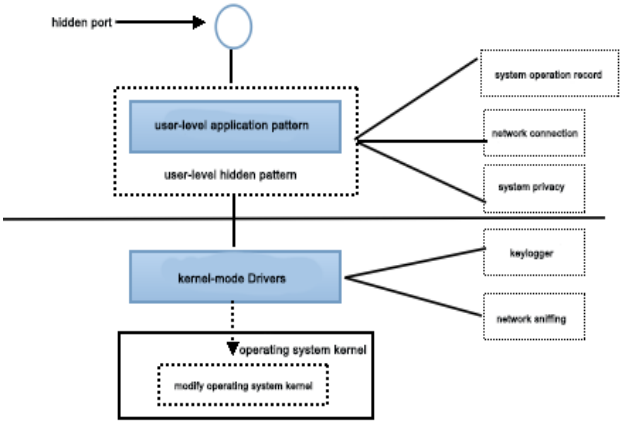

FIGURE IV. HYBRID TROJAN HORSE BASED ON USER MODE AND KERNEL MODE

E. Communication-Concealment

After trojan horse runs, it is need to define it own means of communication with the monitoring terminal for information exchange, which include the transmission of data to the monitoring terminal and receive client's command. As with systems and other network applications, the trojan's client and server is using TCP/UDP protocol for communicating. Usually the Trojan program will directly bind one or more TCP/UDP ports for data communication. At this time, if the port is not hidden, port View tools can easily find all the state of the ports is currently in use. The port has become a key clue to find traces of the Trojan horse. Therefore, in the design of the Trojan, we must adopt new technology to hide and make it difficult to find the port.

In this paper, the technology of reverse connection is used to realize the communication's hiding. In essence, the difference between forward connections and reverse connections is not significant. When the client is connected to the positive, the server is a monitoring terminal. we can use the normal programming method respectively. However, the technology of reverse connection is reversed: the monitoring procedure uses server-side programming method and monitored by the client programming method. As the firewall is often used to monitor the system's and external connection, it tends to filter strictly. Therefore, the use of reverse connection technology can be very convenient to penetrate the target host firewall in order to achieve the purpose of covert communication.

The reverse connection technology is adopted in the monitoring terminal, and the active port is used in the monitoring terminal. After the Trojan program is running, the IP address and the port are connected to the outside of the network. If the monitoring program is on the line, then connect the monitor to the passive port. For this IP address and port information, monitoring and monitoring by the end of the third party storage space for negotiation. The storage space can be a web site. Encrypted information which combined IP address and port information will be sent to the monitoring terminal of the space[5]. After the Trojan horse program runs, the encrypted connection information is downloaded from the web site immediately. The IP address and port information of monitor can be dynamically changed, even if the user can find a trojan, and from which to make a very thorough analysis on the attacker's IP and port information.

In order to enhance the concealment, port TCP 80 is used as the passive connection port. The user uses the command "netstat" or the port view tool to check the status of all ports.it gives the tips are: TCP USERIP: 1026 CONTROLLERIP: 80 ESTABLISHED.

IV. THE FRAMEWORK OF TROJAN HORSE HIDING TECHNOLOGY BASED ON DLL

Firstly, the technology of trojan hidden which bases on the DLL, with the form of dynamic link library, implements a program. And then we should choose a specific process in the target host. Through remote insertion method, the Trojans will be attached to the DLL process and invade the system to get resources and authority of special purpose.

Start-up steps of DLL Trojans

The use of remote thread technology to start DLL trojan is divided into the following steps.

First, find the PID of the host process

(1) Using the function creates a snapshot for the specified process and calling the function process32First to get the handle of the first process[6]. Then, by using the function Process32Next to find the same process as the name of the host process in the process snapshot and record the pid. Close the process snapshot handle at the end.

(2) System privileges to enhance this process

Because the trojan loader operate other processes in the

system, without enough system permissions, there will not be able to read or write to other processes memory address. Using the API function OpenProcessToken to open the process token, and then call the LookupPrivilegeValue to return to a unique ID within the local system, the ID for system permissions change. Using the function AdjustTokenPrivileges is to change permissions of the process.

(3) Enter the host memory space

A number of PID, from which a random selection as a host process, call the function OpenProcess to obtain the process which has been injected code. If getting the process handle is successful, then we use the VirtualAllocEx function in the host process to open up a memory space for storing the DLL Trojan's path name. We use the WriteProcessMemory function to write the path name in the host's memory space.

(4) A new thread in the host

In order to make the DLL Trojan run in the host process space, you can call the function LoadLibraryA to load and call the GetProcAddress function to get the LoadLibraryA's entry address[7]. Then we use the CreateRemoteThread function to insert the DLL Trojan to the host process, so that the host process to carry out the remote monitoring code.

V. THREAD GUARD

In the operating system, the process is the processor scheduling object and the allocation of memory, peripherals and other resources. In the windows system, the concept of thread is introduced to improve the concurrency in the process. Typically, a simple program contains one main thread, which is automatically generated when the process is created. We can insert the code into the main thread and use the main thread to create additional threads to prevent the program which is closed or deleted by the user, in order to achieve the protection of the program process. This is the three thread technology.

Through the analysis of the three thread technology, a unique thread guard structure is designed in this paper, as shown in figure V. In the svchost.exe, it contains two Trojan threads which is DllMain thread and Watch thread. DllMain thread is also the Trojan main thread, through which to create a local Watch thread and remote daemon thread. In order to make the Trojans in the system when the next reboot will also run, requiring the target machine before closing the Trojan program to start the operation. The system will turn off or restart the ExitWindowEx function will be called, which can be used API HOOK technology to connect the function ExitWindowEx. In this way, the system will be notified before the closure of the Trojan horse program, Trojan program to add the start of the implementation of the operation, before turning to the default ExitWindowEx function to shut down or restart the system. API code linked to the Windows function in the Watch thread.

VI. SUMMARY

With the improvement of the windows system, the Trojans are increasingly hidden. However, there is no uniform solution for trojan's detection, which is based on the research of the known Trojan horse. In order to improve the trojan's concealment, we have done research on the trojan hidden technology and have improved local hiding technology. I have put forward a trojan horse hiding technology which based on DLL framework and inserted the DLL Trojan into the svchost.exe by using the remote thread technology to achieve the hidden operation of the trojan program. The framework, applied to solve the problem of Trojan horse hiding in Windows system, greatly improves the anti trojan detection and anti killing ability.

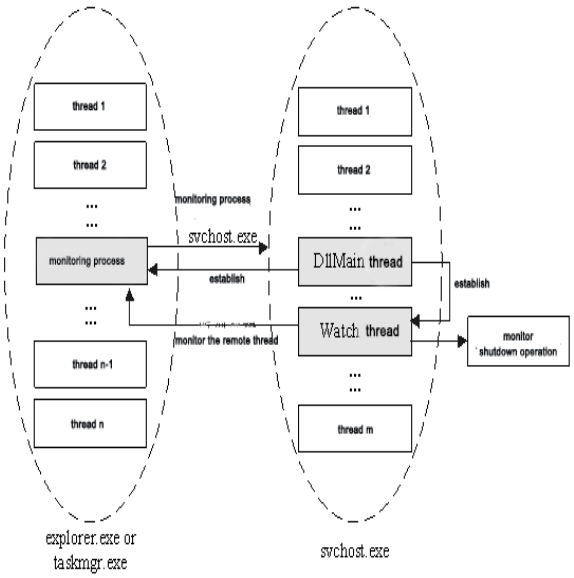

FIGURE V. THE STRUCTURE OF THREAD GUARD

ACKNOWLEDGEMENT

The research was financially supported by Hunan science and Technology Innovation Fund (CX2015B297),Central South University Of Forestry And Technology Graduate Technology Innovation Fund (CX2015B19).

REFERENCES

[1] Adleman L M.An abstract theory of computer viruses[C].In:8th Annual International Cryptology Conference, Santa Barbara, California, USA,1988

[2] Cohen F.On the implications of computer viruses and methods of defense[J].Computers and Security, 1988; 7(2): 167～184.

[3] SETI@Home.http://setiathome.berkeley.edu

[4] Kang Zhiping Xiang Hong.Research and Practice on the Concealing Technology of Trojan Horses[J],Computer Engineering and Applications,2006

[5] Ge Xiuhui,Tian Hao.Research on Information Hiding Theoretic Model. ICEMI'07.8th International Conference on Electronic Measurement and Instruments . 2007

[6] ZHANG Xin-yu, QING Si-han, MA Heng-tai, Research on the concealing technology of Trojan horses[J].Journal on Communications., 2004, 25(7) : 153-159.

[7] PENG Ying-chun, TANHan-song. Researchon the concealing technology of Trojan horse based on DLL[J],Information Technology, 2005,29(12):41-44.