TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 12, No. 10, October 2014, pp. 7389 ~ 7394
DOI: 10.11591/telkomnika.v12i8.5345

A New Systemic Safety Detecting Software

Xilong Qu[1]*, Yingjun Wang[2]
[1]School of Computer & Communication, Hunan Institute of Engineering, Xiangtan, 411101, China
[2]School of Information Engineering, Henan Institute of Science and Technology, Xinxiang, 453003, China
*Corresponding author, e-mail: 570040863@qq.com

Abstract

Because it is hard to find and to clear cockhorse and virus developed by root kit technology, antivirus soft at present is hard to clear virus in the system, which make the system in dangers status of hazard. So, designing a speedy clear Trojan and virus makes by root kit is very important. The article.is based on SDK, adopting the technology.of kernel to design the Clairvoyant systemic safety detecting software. It major function is monitors.the service of the system and the operation. Monitor the register changer. Search the file, process, system module hided by the virus. It can also end protected processes and delete protected files forcibly. Through the port.mapping of processes, it can find.port messages opened.by system, processes opening ports and.cockhorse effectively. This software can also find NTFS stream files so as to find virus effectively. It can also examine BHO (Browser Helper Objects) and LSP (Layer Service Provider) so as to protect browsers and networks from hijacking. It can also examine SSDT (System Service Descript Table) and SSDT Shadow (System Service Descript Table Shadow), and resume amended items. It can also examine and operating serving programmers of system. After the actual system test, it declares that the system has realized the above goals of functions.

Keywords: *SSDT, IRP, root kit*

1. Introduction

As the computer is widely used in social life each do main, the computer virus years, Such as “Big thief in the network games”, “Worm. w h boy. h” “dove” “Trojan of QQ, Dove in gray” is rampant increasingly to steal the users’ password accounts, personal privacy. The commercial secret Property in Network, according to the survey fickle kinds becomes a new trend, in the development of computer viruses. Manufacturing and selling Trojans and virus online becomes rampant gradually. The crime of using viruses, Trojan technology to theft and fraud on the network is rapidly rising. The situation of online security is very serious. Many Internet users suffered from the. “Worm. w h boy. h” that broken out in 2007.In fact, about today’s technology that mainly used some conventional methods which programming skill is not good. Such as, it infects Exe. corn and other documents through U disk auto run info. And it can’t run after infection generally. It infects the shared folder. It can enumerate and spread the weak passwords of LNN computer. Due to there is no advanced hiding technology. We would know that once it infected our computer..However, In today there are a lot of virus of high skill and hidden well in our computers. Such as the harm brought by “dove” that is hard to be found by general ordinary users than by ”Worm. w h boy. h”. Because ordinary users are dependent on antivirus software, they have no recognition of most of the emerging virus. So it can’t intercept effect very well. This situation has kept for many years. With more and more changes in the virus, the virus industry chain activities more and more rampant, this phenomenon becomes more serious, which led to a user’s mistrust of the antivirus software

In order to solve the growing new threat antivirus vendors step in two directions at the same time On the one hand. They used the traditional characteristics identification strengthening engine hulling and sample collection, speed up the updates of the virus signature Today, This is still the main way to deal with and so on. On the other hand, we should develop the new virus identification technology, such as behavior recognition registry and application protection and so on. Now, the virus Trojan needn’t evade the anti-virus software by modifying the signature passively as before they adopt Root kit technology or other technology prevent actively from being discovered by the antivirus software, or close antivirus software directly. It is difficult to remove the virus completely when it is found.

Received December 12, 2013; Revised May 25, 2014; Accepted July 10, 2014

2. Current Difficulties System Security Detects Faced

Due to the anti-virus software used by ordinary users without the basis of the computer. Thus, the anti-virus has to deal with viruses by their self. Now, because antivirus software technology hasn't reached high standards that can accurately judge the virus by itself, which caused a lot of virus escaped being removed. To the users who have certain basic computer technology, they need software that can look over the system information, then judge virus and restore the kernel date and date structures that changed by virus by themselves.

Making up for the shortage, it will make up for the shortage of the antivirus software in judgment the suspicious files through software in judgment the suspicious file through antivirus manually combination of tools and people. So as to achieve the real active defense, we need badly more efficient safety monitoring software system because most ordinary users' software system is unsafe.

System safety inspection mainly tests to detect the key position of system that hidden trouble. Such as processes threads registry, the port opened system documents, etc. The virus in order to let themselves not is easily found. So they are generally used to adopting hidden skills. For example viruses can inject into the key system in the process. Without creating process and it can also escape the firewall. The viruses also can used some HOOK technology or inline HOOKED that can be in RingHook and ringo HOOK which can.modify the IAT table as well as the EAT table Because drivers are layered and IRP pass it on layer by layer we can let the device driver hooked up to a few key drivers (such as file system) to filterer out the harm of the IRP in ourselves, so that users can't detect its existence In order to detect effectively some key information. We must deal directly with system of the bottom which can avoid fooled by the viruses.

With the emergence of lots of Rootkit technology The HIPS technology has emerged. The Chinese mean of HIPS is host intrusion on prevention system HIPS is kind of software that can monitor the operation of the computer. Files and the other files used by documents and documents changes registry and report to you request permission. If you stop, it will not be to run or change. For instance, you double-click on a virus program. HIPs report you but you stop it, then the virus is not running viruses update at a first rate, which makes the footsteps of antivirus software can't keep up with the virus, but HIPs can solve these problem, as long as you have enough professional level, you can only use HIPs without antivirus software. But HIPs can't call a firewall. It can only be called a firewall system, because it can't prevent the attack behavior to your computer by other computer on the network.

2.1. New Software Design of Testing the System's Safety

With the rising of the technical level of the virus creator and further research on Windows kernel, now the development and research direction of the virus technology have adopted the Rootkit of technology to make it disappear in user's computer for hacking. It also can use kernel technology to rid ANTIAV directly and then perform freely their operation defense is the unity of opposites no matter in which aspect, only when we familiar with both opposite can we achieve a better defense.

This system's design is based on the model.

The function need to be achieved

1>.Process management under Ring3
2>.Ring0 check process that include those hidden by viruses and force and the process
3>.Sending IRP directly to the NTFS to view the hidden file or folders
4>.Deleting files mandatory
5>.viewing and restoring SSDT
6> viewing and restoring SSDT Shadow
7.>Detecting the stream of NTFS file
8>.Checking the port opened by system and showing the progress of opening the ports
9>.Checking the LSP
10>Checking the BHO.
11>.Checking the system kernel module
12>.The service management of system
13>System monitoring
14>.Actively defense of system itself

2.2. The General Ideal Design

Designing a program interface to interact with the user at first. For LSP, BHO registry file stream drive and the rings inquiry of service startup process can call the SDK functions directly without use the driver. For SSDK, SSDK Shadow, process killing the process strongly, seeking the hidden file, are design the corresponding drive and operated in the drive.

2.3. System Architecture Diagram

Because the program is realized under the joint of Ringo and Ring3, it can be divided into two big modules. One of them is Ring0 and Ring3. They realized synchronization and communication between them through the IOCTL. Ring3 is divided into process management registry management, network management, system module query, service and the load driver query, BHO management Ring0 include process management, contact file query, SSDT management, SSDK Shadow management, active defense function modules in the system, the architecture diagram of the system is shown in Figure 1.

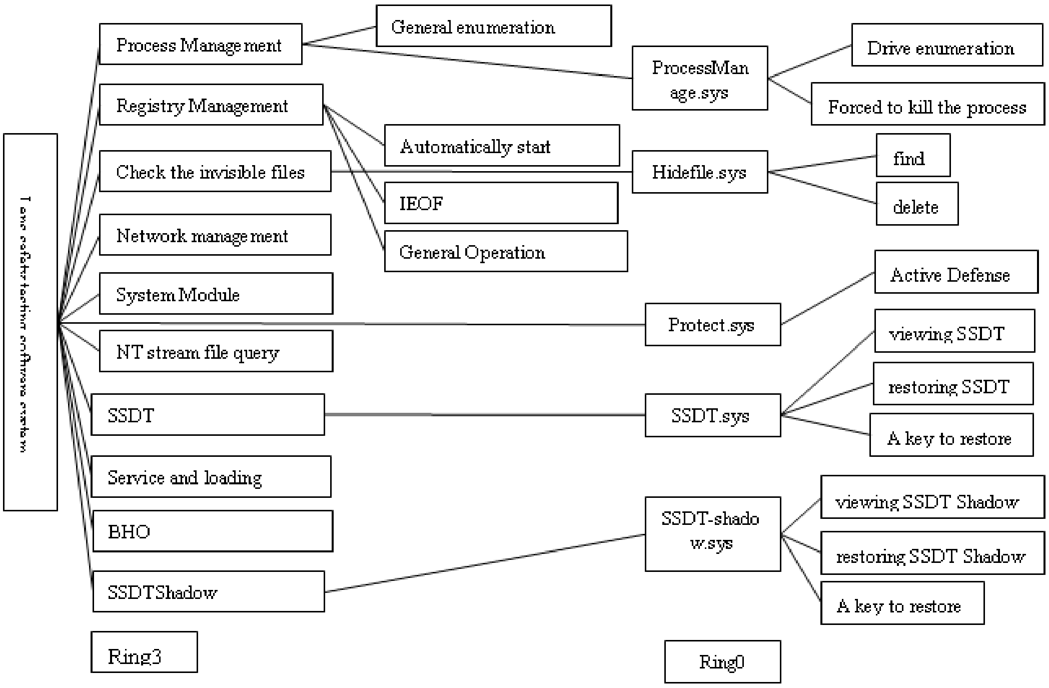


Figure 1. System Architecture Diagram

Service and loading

(1) Process management, process management includes conventional enumeration that uses the snapshot and the end of the process that uses the Terminate process. Driving process enumerate the process by traversal system. Process management is to view process that hidden by virus. The process killed forcibly and the process by terminal process. Because this function can't reach to the bottom. It can end most of the process that remain fore process only.

(2) The registry management: The registry come true the window operation that brings the register itself. It mainly prevents the registry from IEOF by the virus. Moreover it can directly provide the information of looking over IEOF and the information from the start by themselves so that the user can use it easily.

(3) Viewing the hidden files: The function realize the function of deleting and enumerating the file by through send IRP to the NTFS file system

(4) Network management :Net work manage is divided into port process mapping that can view the port of system and show the process of opening port, so that realize the function report and LSP viewing

(5) Module information query system: This function is mainly look over the model information that loaded into the system kernel and let the user view the driver module of loading virus into the kernel. It realized by calling the Nt Query System Information.that system don't announce to query module in the kernel space.

(6) Viewing the NTFS stream file: Due to design flaws in windows explorer can't, view the stream file of blinded in files and fleers that viruses hidden regularly, this function is designed for this situation which can display the stream files' name of file and folders.

(7) SSDT: Because the SSDT is the portal of ring3 entering ring0.It is a battleground of virus and anti-virus software, SSDT management major view the changed SSDT entries and read original SSDT from the NTDLL, dll and drt the correct SSDT table address through the reposition and use it to selectively restore the process of Hooked (Because some antivirus software also use this technique). SSDT Shadow is similar to SSDT but it doesn't have export.

(8) SSDT Shadow: This function is similar to the SSDT, but the SSDT Shadow is another table of the system it will be need to use only if the application is the form of window.

(9) Active defense: System realizes the active defense primarily by the HOOK Zw Open Process function which can prevent other process to opening protected process.

(10) Information services and drivers loaded: It is mainly to check the system service program information. Viruses of registered itself as a system service program. Soaps to realized take the initiative to start with the system.

(11) BHO: BHO is a helper object of browser, which belongs to the COM components. After installation, they will become a part of the browser; you can directly control the browser for the specified operation. According to the need, it can let you open the specified website. or even to collect all kinds of private letter in your system. Such as the home page is changed. IE boot will POP up ads and so on. At present, the browser hijack has become one of the biggest threat to Internet users. Actually "browser hijack is through the BHO technology is legal".
BHO management is by reading HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\

The key name under Current Version\Explorer\Browser Helper Objects, which reading the DLL file path by loading the corresponding. Services and loading the driver is to view the path of the service program in the system. Many viruses register itself for the service to start with system.

3. Implementation

Due toy the limitation of space, this article only lists the implementation process that Ring3 layer view the process.

This function get a snapshot by: CreateToolhelp32Snapshot and it also can get a process PID and process name by: Process32First and Process32, Next process enumerating the process snapshot. The implementation of opening the process operation will fail when didn't put the process of permission to debug permissions. So call: Adjust Token Privileges.right to bring up this process to the Debug permissions, Then call ::Open Process.open.the process to get the process handle. Finally, we can get the path name by process handle calling: "Get Module File Name Ex"

The code implementation is as follows:

1) Get a snapshot of the process

```
H Process Snap = ::CreateToolhelp32Snapshot( TH32CS_SNAPPROCESS,.0 );
```

2) Improving the program permission to Debug

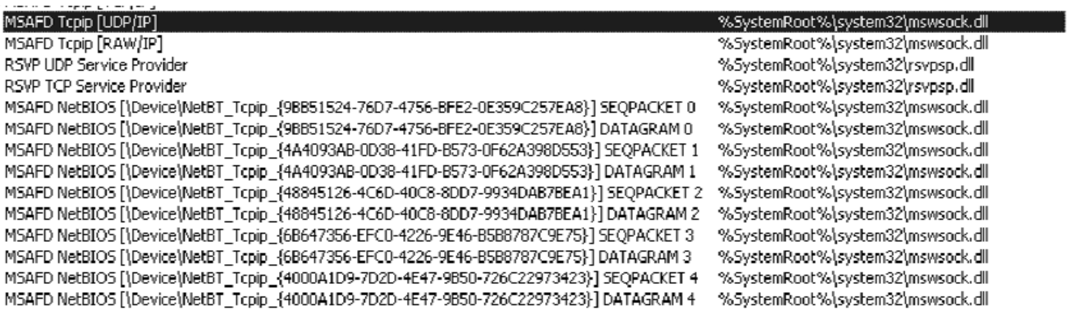
```
……
if (!::"Open Process Token "(Get Current Process
(),.TOKEN_ADJUST_PRIVILEGES|TOKEN_QUERY,.&h Token))            Return
FALSE;.
Privileges. Privilege Count = 1;.
Privileges. Privileges [0].Attributes = eable?SE_PRIVILEGE_ENABLED:0;
if (!::Look up Privilege Value (NULL, SE_DEBUG_NAME,.& Privileges. Privileges [0]..
Lucid ))……
B Result = ::Adjust Token Privileges ( h Token, .FALSE, .& Privileges, .size of
(TOKEN_PRIVILEGES),.NULL,.NULL);.
```

3) Enumeration process snapshot to get a the process PID and process name

……

```
If ( ! Process32First( h Process Snap,.& process Entry ))
                Return;
……
        Do {      ……     .h Process=:: Open Process(PROCESS_ALL_ACCESS, false,
processEntry.th32ProcessID);
                ::Get Module File Name Ex (h Process, NULL, Process Path,
MAX_PATH);
                                …: Close Handle(h Process);
        }
        while( ::Process32Next( h Process Snap,.& process Entry ));
         :: Close Handle (h Process Snap);/
```

Results are as follows:



```
MSAFD Tcpip [UDP/IP]                                                                     %SystemRoot%\system32\mswsock.dll
MSAFD Tcpip [RAW/IP]                                                                     %SystemRoot%\system32\mswsock.dll
RSVP UDP Service Provider                                                                %SystemRoot%\system32\rsvpsp.dll
RSVP TCP Service Provider                                                                %SystemRoot%\system32\rsvpsp.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{9BB51524-76D7-4756-BFE2-0E359C257EA8}] SEQPACKET 0   %SystemRoot%\system32\mswsock.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{9BB51524-76D7-4756-BFE2-0E359C257EA8}] DATAGRAM 0    %SystemRoot%\system32\mswsock.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{4A4093AB-0D38-41FD-B573-0F62A398D553}] SEQPACKET 1   %SystemRoot%\system32\mswsock.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{4A4093AB-0D38-41FD-B573-0F62A398D553}] DATAGRAM 1    %SystemRoot%\system32\mswsock.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{48845126-4C6D-40C8-8DD7-9934DAB7BEA1}] SEQPACKET 2   %SystemRoot%\system32\mswsock.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{48845126-4C6D-40C8-8DD7-9934DAB7BEA1}] DATAGRAM 2    %SystemRoot%\system32\mswsock.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{6B647356-EFC0-4226-9E46-B5B8787C9E75}] SEQPACKET 3   %SystemRoot%\system32\mswsock.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{6B647356-EFC0-4226-9E46-B5B8787C9E75}] DATAGRAM 3    %SystemRoot%\system32\mswsock.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{4000A1D9-7D2D-4E47-9B50-726C22973423}] SEQPACKET 4   %SystemRoot%\system32\mswsock.dll
MSAFD NetBIOS [\Device\NetBT_Tcpip_{4000A1D9-7D2D-4E47-9B50-726C22973423}] DATAGRAM 4    %SystemRoot%\system32\mswsock.dll
```

Figure 2. General Enumeration Process

Results 1 deliberately chose some well-known both at domestic and foreign several antivirus software and perform a comparison test of the system.

Table 1. The Four Core Functions in the Test Results of the System Compare with the Software used at Home and Abroad

	Process Management Test:Select IceSword process,.click right then mandatory try to end of the process	Test of find hidden files: use the "Worry hidden"software.Hide the folder of c: \ demonxjj	SSDT detection: Open spy sword, if HOOK can be detected, or HOOK function can display module resides.	Test of Active defense: Open the system, introduces its process by use the Task Manager。
The system	can	can	can	Can not
Kaspersky	Can not	Can not	Can not	can
Avast	Can not	Can not	Can not	can
Kingsoft	Can not	Can not	Can not	can
Rising	Can not	Can not	Can not	can

4. Conclusion

This treatise designed the new type of system security detection software mainly use a lot of driver programming technology and Windows core programming technology. The application layer software directly uses the SDK to write interface, driver user WDK to. The SDK to write interface, driver uses WDK to he main advantage of the software is able to view the hidden process and hidden folder. It also can fore end process, mandatory delete folders can view the restore SSDT, LSP the process of port mapping and so on, One of the biggest characteristic is to view and restore SSDT Shadow. The BHO registry and system monitoring module is introduced in detail, because their principle and implementation is simple, we can modify the BHO and registry through the registry API function. In the aspect of system monitoring primarily through HOOK Z w Create Key and Z w Open Key. and prevent files to be deleted.

Due to the software development time is limited their level is not high, so in the compatibility and stability of the software is very poor and is not very powerful. It is badly short of the famous. Ices word and uses check in many filed..The only advantage is able to view the SSDT Shadow and restore those addresses of HOOK. Please keep the important date when using to avoid BSOD.

Acknowledgements

The authors gratefully acknowledge the support from the following sponsors: Provincial Natural Science Foundation of Hunan (13JJ9022) & (11JJ9018) and Provincial Science & Technology Plan Project of Hunan(2010GK3048) & (2013GK3029).

This research is supported by the construct program of the key discipline in Hunan province.

References

[1] Sun Li, Li Yang, Li Ji-Yun. The CEP-Based Correlation Solution of Monitoring Events on Distributed It Resources. *Computer Applications and Software*. 2013; 30(8): 303-306.

[2] QU XiLong, HAO ZhongXiao, BAI LinFeng. Research of Distributed Software Resource Sharing in Cloud Manufacturing System. *International Journal of Advancements in Computing Technology*. 2011; 3(10): 99–106.

[3] Jian-quan Ouyang,Hua Nie, Min Zhang. Fusing Audio-Visual Fingerprint to Detect TV Commercial Advertisement. *Computers and Electrical Engineering*. 2011; 37(6): 991–1008.

[4] QU XiLong, BAI LinFeng HAO ZhongXiao MD3 Model Loading in Game. *Journal of Computers*. 2012; 7(2): 521-527.

[5] Wang Bin-Jun, Wang Jing-ya, Du Kai-xuan, Han Yu. Research on attach and strategy of CAPTCHA technology. *Application Research of computers*. 2013; 30(9): 2776-2779.

[6] CHEN Yue E, WANG Yong, QU Xi-Long. Estimation of the Maximum Output Power of Double-Clad Photonic Crystal Fiber Laser. *Chinese Physics Letters*. 2012; 29(7): 74214-74217.

[7] Chen Qiao, Xu Mai-chang, Qu Xi-long. Heat Generation by Electrical Current in Quantum Dot System with Fano Resonance. *Commune Theory. Phys.* 2012; 58(2): 295-299.

[8] PENG Xiao, HU Zhi Gang, QU Xi Long. Hybrid-Policy Co-allocation Model in Computational Grid. *Journal of Software*. 2012; 7(2): 382-388.

[9] Zhou You-yi, Dong Dao-guo, Jin Cheng. Design and Application of Main Memory Database in High-Concurrency Cluster Monitoring System. *Computer Applications and Software.* 2011; 28(6): 128-130.