ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering and Technology, Madurai, Tamil Nadu, India

Experimental Analysis of Hooks in Virtual Environment

G.Archana[#1], S.Suresh Kumar[*2], G.Dinesh[#3]

Student, Department of CSE, Anna University, Rajalakshmi Engineering College, Chennai, Tamilnadu, India

Assistant Professor, Department of CSE, Anna University, KLN Institute of Technology, Madurai, Tamilnadu, India

Associate professor, Department of CSE, Anna University, Rajalakshmi Engineering College, Chennai, Tamilnadu, India

Abstract— In computing the virtualization means act of creating virtual version. Hardware virtualization is creating of virtual machine with different operating systems. Both Windows and Linux based operating systems may run on virtual machine. Depending, RAM size is allocated. Now days there are many types of malware that affects our system. Malware like Trojan affect the system and then create the backdoor for the system. Then Hackers keeping watching the users' activity. Root kit (Backdoor) hides the malware activities .Root kit may be of user mode and kernel mode. Root kit enters via dropper (installs malware).BotNet is same as root kit that network of private computers infected malicious code without knowing to administrator. Malware after entering into system modifies kernel by installing backdoors, logging keystrokes and disabling firewalls. The hook has been detected and thus gives the Malware Rating Index, Processor Id and type of hook.

Keywords- IRP, Operating System, RAM, Virtual Box

I. Introduction

We are aware that, the evasive growth of root kits in our system and mobile devices [1] is reaching an extreme height which is unimaginable. The main difference between virus worm and malware is virus that affects other system, worm replicates and destroys files. Malware that does the malicious activity without showing its presence in the system. Especially the laptop and tablet play an eminent role in the hands and works of the people. A survey reveals that the root kit become enable in the form of stealth functionality has been identified in mid 1980.The first notable root kit that affects the storage medium is brain virus. In the mid of 1990 it was identified that user level root kits are easy to detect. The survey regarding kernel was taken and found that root kit affected in kernel level takes the control of the computer and there is a change in operating system providing fake information. Kernel level root kit is nothing but to create new code in the running system. i.e. writing code for device driver on windows/lodable kernel module (LKM) for UNIX platform. Many types of root kits [2] (figure 1) are library, kernel, and firmware and virtualized designs.

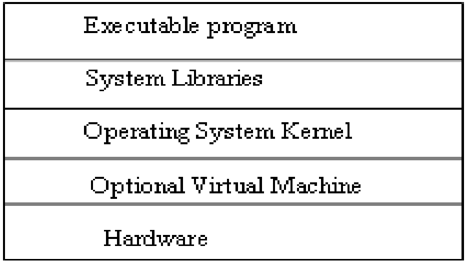


Figure1. Types of Root Kit

The top stack is user land where the program can be executed. The applications at run-time use system libraries. The application and library level are referred as user land. Below the user space comes the kernel land that access files, directories. They also check the authentication level for sending the request for appropriate response. Bottom of stack is hardware (Firm level) .The root kit detection in the kernel land is difficult even we use the detection tool which is installed below the Virtual layer. The architecture (figure 2) of virtual environment consists of hardware with operating system (Host OS), Virtualization layer and guest OS.The need for virtualization is because of its security, low down time maintenance. The software layer that provides virtualization is VMM/Hypervisor.

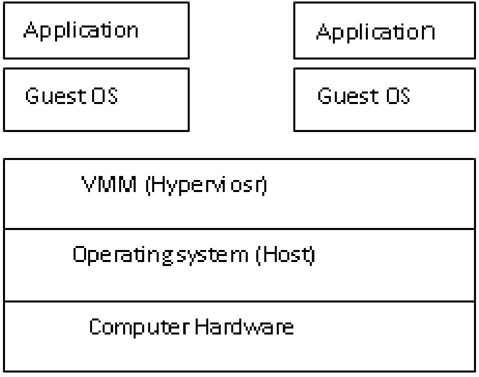


Figure2. Architecture Diagram

There are many types of malware that affecting the system. Most dangerous malware is Trojan that spread through user interaction such as e-mail or running file from internet. Trojan affects the system and allow backdoor for the malware to get inside the system and make changes in administrator level.

A) *Symptoms of Root kit*

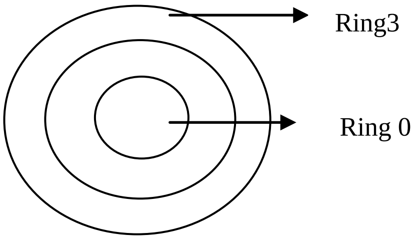
To know our system is affected by Rootkit, it is necessary to check for hardware and software of the operating system. This enters by sneaking past antivirus activity.

- There will be the message alert in system
- Problem with drives and disappearing of files every time
- Hardware problem

Some of the OS components attacked are Input/output Manager, Device and System drivers and Security reference monitor.

II. FUNCTIONS OF KERNEL AND TYPES OF MALWARE

Operating System stays in its original privilege level 0.Rootkit attempts to access the hardware directly. Ring 0 and Ring 3 mostly used by windows and Linux. Ring 0 affects the kernel mode that have access to virtual memory. Ring 3 cannot access Ring 0 if so interrupt will occur.



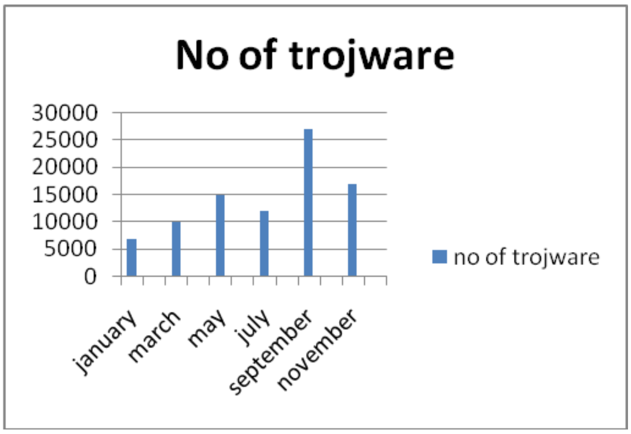
Ring 0	Ring 1	Ring 2	Ring 3
More			Less

Code can be introduced into kernel by loadable module (kernel driver). Most operating system allows kernel extensions to be loaded so that manufacturers of third party (hackers) can support. This (motherboard) is the easy way to introduce code into kernel. Once code is loaded full access is taken by the administrator so that changes can made whenever needed.CPU is responsible for memory allocation to each ring. There are many malwares that affects all over the world. Among them Trojan is very dangerous that allows way to backdoor[3].

A) *Types of malware.*

Adware	Displays Ads on the system
Spyware	Tracks the internet activities
Virus	Attacks the system and also infect other systems
Trojan	Dangerous malware for stealing users information

Trojan has been spreading vast from the year2006. After Trojan get activated it leads to damaging the host (deleting files, stealing data).Trojan spread through user interaction by e-mail/downloading/running file from internet. Many Trojan viruses are available, among them Banker Trojan is very popular for taking credit card information from the user.



The number of trojware that has been introduced from 2003 to 2007 (www.kasperskylab/malware.com). According to statics gathered Trojan.Mayachok1 (backdoor family frequently detects on users computers. It has been increased by 3.73% (May) to 5.82% (June). Program of this backdoor family can change the encrypted data and can download files into infected machine. The system call gets redirected and the hook type is named as SSDT (system service descriptor table). The system call can be tracked by paladin driver.

Table 1.1.Tracked System Call

	Total system calls	Calls processed
Kernel copy	305690	77644(25.4%)
Kernel compile	7254	1276(17.6%)

These system calls are traced by the driver. System calls can be traced with and without paladin driver.

Table1.2.System Calls With And Without Paladin

	Without paladin	With paladin
Fork	1.5µs	3.5 µs
Exit	1.5 µs	1.6 µs
Open	0.8 µs	1.5 µs
Close	0.5 µs	0.7 µs

Paladin driver [8] has the knowledge about the guest Operating system. It looks up symbol error from the kernel. It can be responsible for jump tables and rename enteries.

User request for the API and then modifications are made after installation of root kit.

III. SYSTEM CALL IN KERNEL

Program operating at user will redirect to kernel by system call. Application performs system call and it redirects to kernel which then performs for the request application and produces the result in turn. System call addresses are maintained in kernel memory .System call includes Table modification, Table target and Table redirect (figure 3).

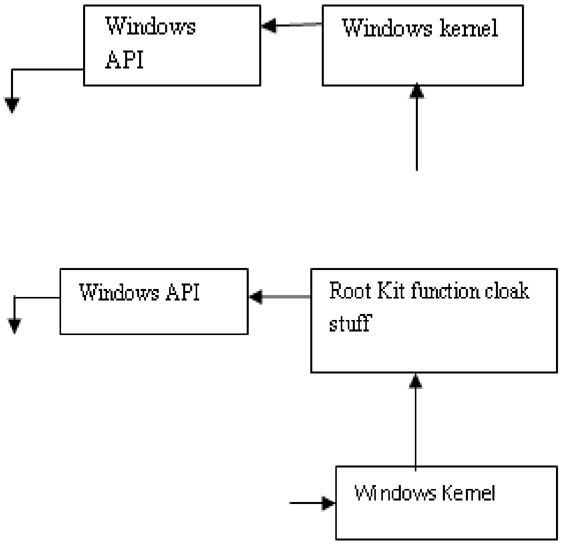


Figure3. Before And After The Attack Of Root Kit

When input is given if root kit is not infected then it redirects and gives the original output.

IV. TO IDENTIFY MALWARE AND CALCULATE TIME

To calculate the time we need to identify our malware and it should be injected. After injecting malware it should be analyzed (figure 4). The malware can be created or it can be downloaded from official website.(www.offensive computing. in) [20]. Hook can be identified by verifying digital signatures and sometimes cross view detection.

A) Initialization of operating system

First the operating system must be installed with windows 7(host) and XP (guest). Each OS contains root kit for simulation and network services to get communication between both OS.Network services such as (tfpd, ftpd) used to transfer files between their local system and guest system where they can reach network. Tools to be installed for detecting types of hooks.

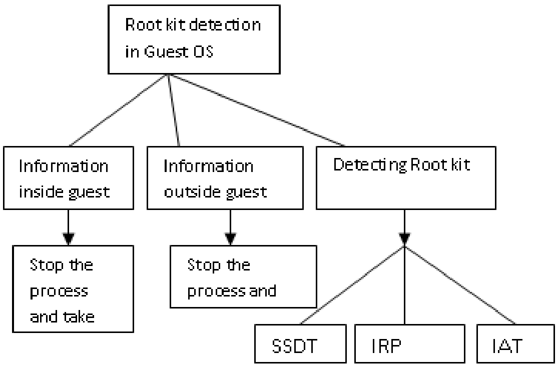

Root kit detection in Guest OS
Information inside guest
Information outside guest
Detecting Root kit
Stop the process and take
Stop the process and
SSDT
IRP
IAT

Figure4. Detection And Analysis Of Root

V.RELATED WORKS

There are some works for identifying root kits and their impact on smart phones [1]. Smart phones are increasingly being equipped with operating systems. The occurrence of root kit in Smartphone has not been detected yet. Modern Smartphone are well equipped with Linux/windows operating system and also many pre installed applications. In Smartphone through GSM the attackers may try to hack the phone numbers or the messages that is being transferred. So the same performance as in desktop will be done. i.e change in system call .By GSM location is being tracked. Root kits came into phone through downloading through malicious websites but still it is under surveillance. The increasing generalization technology [2] access by citizen brings expectations on demands on government. The proposed expert E-Governance system embodies knowledge to solve problems and to provide services to various stakeholders.ICT provide better information and encourage people. There are many types of malware [3] that have been discussed with many examples. The four classes are Type 0, I, II and III. All the applications will become malicious and will delete all files/folders from the users' directory. Type III uses the hardware virtualization technology. Viruses will change only the code/data of the system. Only root kit [9] will take the control of the system. Many viruses can be found but only root kit will take the control of the system. Types of root kit [4] user, kernel, application level and virtualized root kits. The technique for detection is cross view and kernel integrity monitoring. The benefits of virtualization are portability, manageability and efficiency. The kernel hooks are detected and scanning time is calculated. VM Workstation plays an important role in hardware [5]. Some procedures are followed to import virtual machines in the system. Kernel root kits related modification is SSDT. The modification is done by changing the expected address value.

VI. FILTER DRIVERS

Some plugin are needed so that memory image can be loaded. In memory image analysis full image is captured and plugin (IDA PRO) to investigate images. To analyse memory foresenics is used. (Securityxploded.com/malware-memory foresenics). The windows driver stack is designed in layered manner so that third party can easily use for their access. This enables the hackers to easily inject their code using root kit and can change the information in administrator. Hackers can insert their root kit by already existing drivers or creating new driver so that they can do changes by themselves (figure 5) Using Digital signatures this can be verified by authorized person using existing tools.

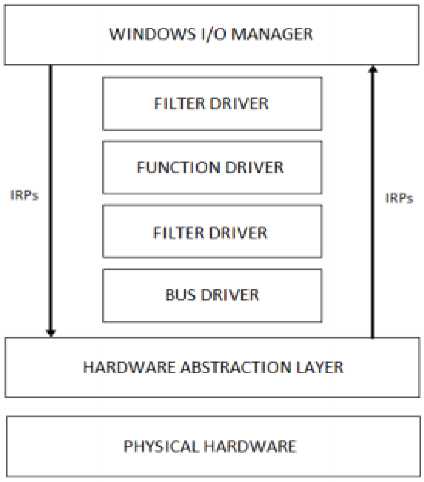


Figure5. Filter Driver Functionality

VII.IDENTIFYING SSDT AND IRP HOOKS THROUGH REDLINE

SSDT (System Service Descriptor Table) has been employed as Windows root kits. It hides files, process, and registries from the targeted operating system. It can be identified by redline and capturing memory image by volatility framework. Microsoft Windows use the SYSENTER [12] to jump instructions from user mode (ntll.dll) to kernel mode (ntoskrnl.exe).Redline is the tool that detects the kernel level hooks. The memory can be extracted from the drivers or the we can run script to gather memory image data and create analysis session. Redline also gives information about how to analyse data from collector. Then by analyzing we get the timeline, describing about ParentProcessorID, MRI (Malware Rating Index), and Kernel time and parent name. Some hooks can be analyzed.[18] [19]. Hooks are injected and then followed by further steps (figure 6) hook type is created.

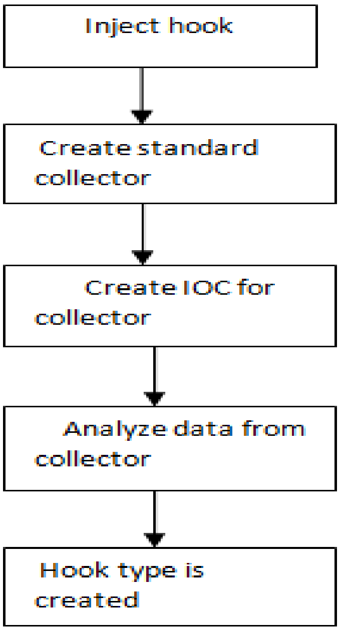


Figure6. Block Diagram for hook creation

Another procedure for creating memory analysis is by volatility framework. It must contain framework, SSDT plugin, other plug in such as SSDT_EX, psx view, impscan.

VIII. MEMORY IMAGE ANALYSIS

Memory foresenics [13] is to capture the image in running computer. We must need the images for capturing. Then plugin are needed to find what type of operating system and type of image captured. To run the plugin we must need python to be installed. Volatility [16] is used in all the operating systems for analyzing RAM dumps in both 32 and 62 bit operating systems. Snapshot is taken so that comparative analysis (figure 7) can be done based on that. (sourceforge.net). The time for each scan is noted and graph is drawn by comparing types of hooks. Kernel hooks does not depend upon virtual memory size but if time increases then snapshot time increases. The snapshot [14] taken will be saved in a particular location for root kit detection. Hibernation that saves the machine state to the disk when the computer is powered off. When the system is turned on then physical memory is written to disk as hiberfil.sys [15]. This file can be decrypted for obtaining the memory image.

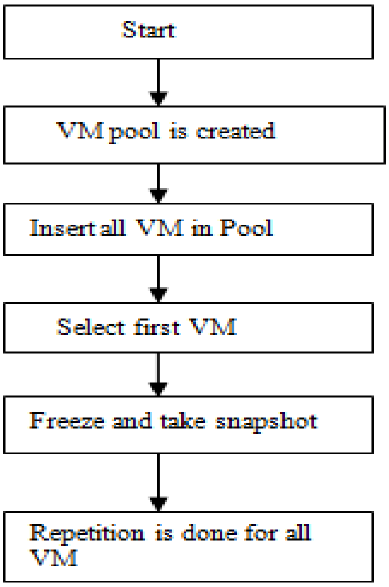


Figure7.Snapshot Analysis in Virtual Machine

IX. RESULTS AND DISCUSSION

Hook is injected and by using redline tool it is analyzed to find the process name and kernel time it takes for calculating. Lists of ioc are collected so that it gets analyzed to find what type of hook it is. The EPROCESS is shown in Table1.3

It belongs to AURIGA family. It contains the functions of keystroke logging, performing file systems, registry modifications, injecting hook. The verification was done by digital a signature which checks the particular address. In Analysis session redline automatically groups data such as file write agents and processes. The data available for analysis depend upon data in analysis session. If we need not use ioc then compromise collector is used for gathering data. Malware Rating Index gives when we are using kernel level hooks.IRP is the type of hook related to operating system.

Process name	MRI	PId	Start time	Kernel time	Parent PID	hook
Redline.exe	45	532	31,24 s	122s	1464	IRP
Smss.exe	46	1968	25,9s	3604s	1500	IRP

Table 1.4 Results of SSDT hook

Object Name	Object path	Hook
ZwOpenThread	NULL	SSDT
ZwTerminateThread	NULL	SSDT
LastTimeHour	HKEY_LOCAL_MACHINE	Registry value
firefox.exe	C:firefox.exe	Process
svchost.exe	C:svchost.exe	Process

Thus the hooks with object path and object name were found by tool. Mandiant tool must consider the following guidelines for collecting malware.

- Automate the collection of a standard data set.
- Minimize reaction time.
- Minimize interaction with the suspect computer.
- Minimize changes to suspect computer

.Net Package is essential for Mandiant installation. Thus the malware is verified and detected.

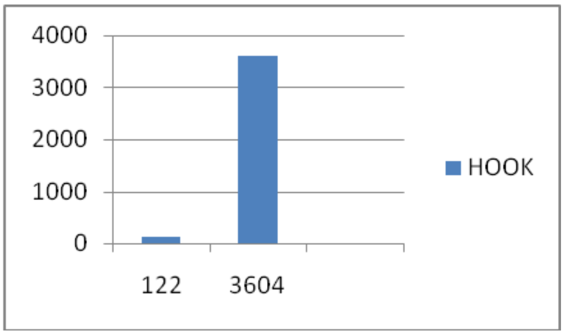


Figure8. Kernel Time Analysis

Thus the kernel time gets increases second time when scanning is done. It does not depend upon the virtual memory size.

Table 1.5 Results of IRP hook

298c558	ctfnon.exe
2998da0	wscntfy.exe
29a2650	alg.exe
29a71c8	smss.exe

X.CONCLUSION

Thus time is calculated and type of hook is created using virtual box. The scanning is done by tool[17] and analysis data contains system information, processes, handles, memory sections, Ports, Device tree, Hooks and Acquisition history. The port displays the process name and process id of the hook. Device Tree contains about the algorithm that is being verified by digital signatures. Hence the time gets increases when scanning is done. However by analyzing many hook we can find the time and object path that was infected

ACKNOWLEDGEMENT

I would like to thank Head of the department and colleagues of Rajalakshmi engineering college who supported and encouraged for preparing this paper.

REFERENCES

[1] Jeffrey Bickford Ryan O'Hare†Arati Baliga

[2] *Vinod Ganapathy Liviu Iftode*. Root kits on Smart Phones: Attacks, Implications and Opportunities.

[3] *www.kaspersky/malware.com*

[4] *ShadidNaseem* Cloud Computing and E- Governance

[5] *JoannaRutkowska* Introducing Stealth Malware Taxonomy.

[6] *J. Toldinas, D. Rudzika, V. Štuikys, G. Ziberkas.* Root

[7] Root Kit detection experiment within virtual environment.

[8] *Palo Alto, CA 94304*.Using VM Work station.

[9] www.google.com

[10] www.wikipedia.com

[11] Snapshot feature of Oracle VM VirtualBox

[12] A comparative analysis of root kit detection techniques by thomas martin arnold.

[13] The study of ssdt hook through comparative analysis between live response and memory image muteb alzaidi, ahmed alasiri, dale lindskog, pavol zavarsky, ron ruhl, shafi alassmi information systems security management concordia university college of alberta, edmonton, Canada.

[14] Madiant Redline –User Guide

[15] Time keeping in VM Ware Virtual Machines – Information Guide

[16] Hacking-lab.com

[17] Code.google.com (Volatality)

[18] Sourceforge.net (open source for tool)

[19] www.offensiveComputing.net

[20] Identifying Rootkit Infections Using Data Mining Desmond Lobo, Paul Watters and Xin