MALWARE INCIDENT HANDLING

A.Sankara Narayanan[1]
Department of Information Technology
Salalah college of technology
Sultanate of Oman

M.Mohammed Ashik[2]
Department of Information Technology
Salalah college of technology
Sultanate of Oman

Abstract -**The paper will be a detailed introduction of malware handling for security professionals. This paper will also serve as a guideline for the reader to perform malware handling by providing definitions, tools to use, and real world demonstration to the reader with enough information to successfully perform malware incident handling. . It will spotlight on step by step process, including suggestions on what tool to employ, what to look for and what to do with the disbelieving file. In our experiment we present the findings about the state of services, registry keys, security updates, and virus total results. Our analysis of the data demonstrates that malware detectors using tools and techniques.**

Keywords: **Malware, Network Security, System Security, Reverse Engineering, Malcode Analysis**

I.INTRODUCTION

Malware is the generic name or short name user to describe ***Mal***icious Soft***ware,*** developed for the purpose of doing harm. Malware can be classified in several ways, including on the basis of how it is spread, how it is executed and what it does. The major type's malware are Viruses, Worms, Trojans, Backdoors, Spyware, Rootkits, and Spam. There are so many types of malicious software afloat around the internet. Many of them existed for years. Once released into the internet they are almost unfeasible to destroy. System security is the protection ensured in an information system in order to reach the applicable objectives of preserving the integrity, availability and confidentiality of information system resources like hardware, software, firmware, information data and telecommunications. The common aim of the malware is gain access to a computer system to steal private information of anyone for financial gain.

According to the statement of Graham Cluley, Senior Technology Consultant of Sophos"More computer viruses and worms mean an unprotected windows PC stands a 50 percent change of infection by a worm after 12 minutes online". A malware program attacks an only one computer as its host. After than when the computer is ping to a network, the malware start to spread and attack to other computers, finally the network is down for maintenance. Malware infection may come through the websites, email, and third party software which is downloaded from the internet. It is not a good practice try to open the attachments sent to your email from an anonymous sender because it may have risky malware attack. Using expired software applications can also helps malware to enter in your computer. The new malware programs are complicated and cannot identify by many of the anti-malware programs, and it is hard to destroy because it has the codes are developed by using reverse engineering like command and control.

II. IDENTIFYING INSTALLED MALWARE

Almost all malware will install in similar directories in order to execute and propagate throughout a victim's computer. These are some of the more common directories in which malware will install itself on Microsoft Windows (multiple versions)

- ApplicationData%\Microsoft\
- %System%\[*FileName*].dll
- %Program Files%\Internet Explorer\[*FileName*].dll
- %Program Files%\Movie Maker\[*FileName*].dll
- %All Users Application Data%\[*FileName*].dll
- %Temp%\[*FileName*].dll
- %System%\[*FileName*].tmp
- %Temp%\[*FileName*].tmp

Affecting Processes of all malware will attempt to hook system and user processes in order to operate behind the scenes and also attempt to prevent the victim from quickly identifying its activity. These are typical system and user processes affected by malware found.

- explorer.exe
- services.exe
- svchost.exe

This is will attempt to disable operating system features in order to continue to execute and propagate.

- Windows Automatic Update Service (wuauserv)
- Background Intelligent Transfer Service (BITS)
- Windows Security Center Service (wscsvc)
- Windows Defender Service (WinDefend)
- Error Reporting Service (ERSvc)
- Windows Error Reporting Service (WerSvc)

Here are some of most common Registry locations where malware will install itself on a victim's computer in order to execute and propagate.

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\

III. MALWARE HANDLING TECHNIQUES

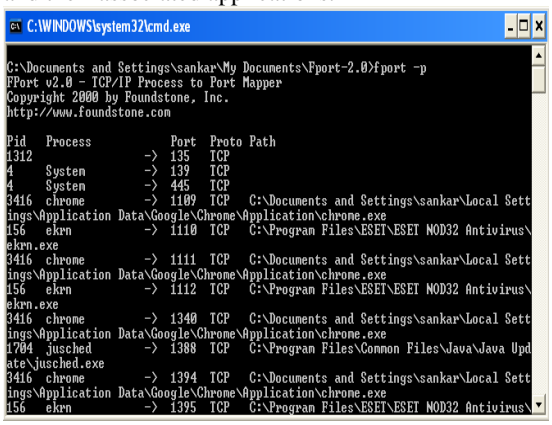
Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering
Editor In Chief Sahil Seth.
ISBN: 978-981-07-1403-1

A. FILE INFORMATION

In this section will discuss about which file or process is responsible for services, process ID and other network modifications and settings. These tools are very useful in analyzing a file and structure.

1) Fport:

This tool reports all open TCP/IP and UDP ports and maps them to the owning application. This is the same information you would see using the 'netstat -an' command, but it also maps those ports to running processes with the PID, process name and path. Fport can be used to quickly identify unknown open ports and their associated applications.



Installation:
Download the Fport.exe (112 KB) file to your computer.
Place the Fport.exe file directly on your C drive. Fport works only if you navigate to where it is being stored in the command prompt. (E.g. C drive you stored → C:\fport, that's it.)
Usage:

- Start → Run → cmd
- C:\>cd\
- C:\ >fport –p

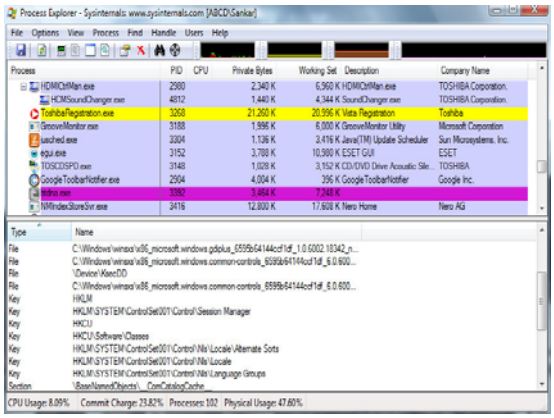
If you want to copy the output of fport into a file

- C:\>fport –p >> [filename].txt

Now look at output and see if you notice any strange programs on your machine. Then use a command line 'kill' utility such as" taskkill [specific PID]" to stop the program. Typically Trojans and some viruses will open up non standard ports which can be great clue to determining if a system is compromised or not. Watch out for open high numbered ports such as 3112, 31337, 12345, 7777, and 65000. Fport can be used on the windows NT4, Windows 2000, Windows XP.

2) Process Explorer:

This application shows you information about which handles and DLLs processes have opened or loaded. The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.



Installation:
Download the procexp.exe (4080 KB) file to your computer.
Double click the exe file, that's it.
Usage:
This will show two sub-windows
Top window will show → what processes are running, PID, CPU usage, description and company name.
Second window will show → Specific processes file path, registry key, exe thread.
Down end it will show → CPU usage, commit charge, number of process, physical usage.

B. SYSTEM INFORMATION

This section will cover tools that are malicious entries in key system areas, such as registry keys, services, and Microsoft security updates.

1) Microsoft Baseline Security Analyzer:

Microsoft Baseline Security Analyzer is a very useful tool designed for the IT professionals. It will show Microsoft security recommendations and offers specific remediation guidance.

Installation:

Download the **MBSASetup-x86-EN.msi** (1588 KB) file to your computer

- Double click the File→ Click Run
- Click Next →Select I Accept the licence agreement
- Click Next → Click Next
- Click Install → Click O.K

Usage:

a) Scan a computer:

Check a computer using its name or IP address, this scan using for home or personal computers.

- Click → Scan a Computer; then you will enter IP address or Computer name
- Click → Start Scan, it will check online Microsoft Security Updates, and then your system scan will start

b) Scan multiple computers:

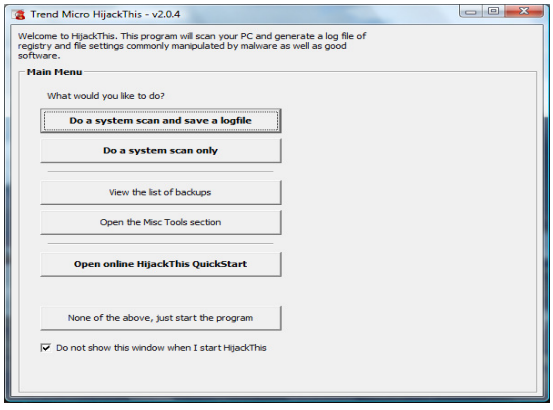
Check multiple computers using a domain name or a range of IP addresses, this scan using for network environment.

- Click → Scan multiple computers, then you will enter Domain name or IP address range
- Click → Start Scan, it will check online Microsoft Security Updates, and then your system scan will start

Both scans detailed report will show Security Update, Administrative Vulnerabilities, Additional System Information, Internet Information Services, SQL Server, Desktop Application results.

2) HijackThis:

This program will scan your pc and generate a log file of registry and file settings. It will provide the ability to remove any unwanted stuff.



Installation:

Download the **HijackThis.msi** (1370 KB) file to your computer. First creating a folder named 'HijackThis' for it located someplace easy to find like 'My Documents' and place the file into the same folder.

- Double click the File→ Click Run
- Click Next → Select I Accept the terms in the licence agreement
- Click Next → Click Next
- Click Install → Click Finish

Usage:

Now open the program

- Click → Do a system scan only. When the scan is done
- Click → Save log and save the log file to the same folder HijackThis is in.

Please do not check or fix anything. Open the log file with notepad or similar text editor. Compare with log file and other reports also, after you will fix anything.

C. MALCODE ANALYSIS

This is the most technical and also most useful section as it allows you to see exactly Malcode total reports, in real time. The tools covered here are for advanced users only who are already used to handling live Malcode.

1) http://www.gfi.com/malware-analysis-tool (formerly CWSandbox)

GFI SandBox is an automated malware analysis tool which allows the analysis of virtually any Windows application or file including infected Office documents, PDFs, malicious URLs, Flash ads and custom applications.

- Click → Submit your malware sample for a free analysis, it will redirect http://www.threattrack.com/
- Click → File Chosen button upload your sample malware, Enter your email ID, then confirm your email ID, and enter the captcha
- Click → Accept and submit my file.

The detail PDF report contains an executive-level summary, including network activity and screenshots also sent you by email.

2) www.norman.com

If you have a suspicious or infected file, please submit it online by using the form below. Once the file is submitted, Norman Automated Analysis System will scan it and report will send you by email.

Click submit files for free analysis, it will redirect

http://www.norman.com/security_center/security_tools/en-us

- Enter your email id
- Click → Choose file, Select your file
- Click → Upload

3) www.virustotal.com

Virus Total is a service that analyzes suspicious files and URLs.

File Upload

- Click → Upload a File
- Click → Choose file, select the file
- Click → Send file

URL Upload

- Click → Submit URL, type Malicious URL
- Click → Submit URL

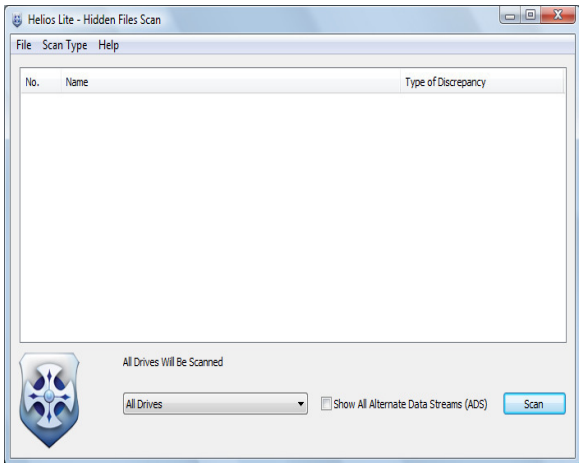
D. SCANNERS

This section covers the main options you have to get any suspected files scanned by multiple anti- malware scanners. The tools covered here are most powerful, simple, and easy to install.

1) Helios Lite:

Helios Lite is a stand-alone binary that can quickly scan a system for system service dispatch table (SSDT) hooks, hidden processes, hidden registry entries, and hidden files.

Helios Lite uses a GUI program to communicate with its kernel-mode driver, helios.sys. Together these two components are able to detect most rootkits hooking and hiding techniques.



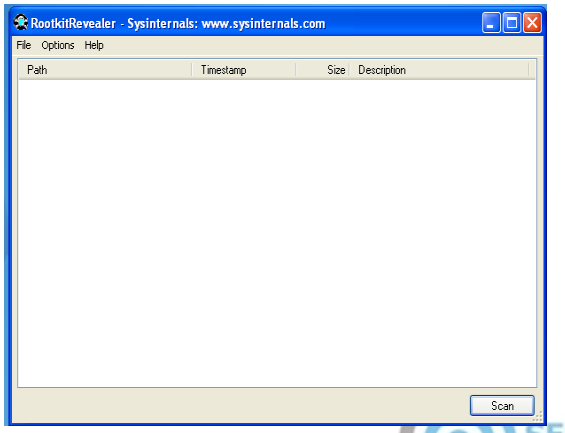
Installation:
Download the **Helios Lite.RAR** (207 KB) file to your computer.

- Right click the file → Select extract to Helios Lite; you will get a folder Helios Lite.
- Double click the Helios Lite folder → two files are available, Helios Lite.exe and Helios.sys.
- Double click Helios Lite.exe → It will run.

Usage:
Click → Scan type, select hidden files,
Enable → Show all alternate data stream (ADS), click scan
Click → Scan type, select hidden registry, hidden processes, ssdt hooks, click scan

2) RootkitRevealer:

RootkitRevealer uses a cross view approach and focuses only on the file system and Registry. The benefit of this tool is fast, simple and effective. It does not scan for loaded kernel modules; it quickly detects both the hidden registry keys and the files being hidden by the rootkit.



Installation:

- Download the **RootkitRevealer.exe** (326 KB) file copy to your computer.
- Double Click → Agree → Agree, that's it.

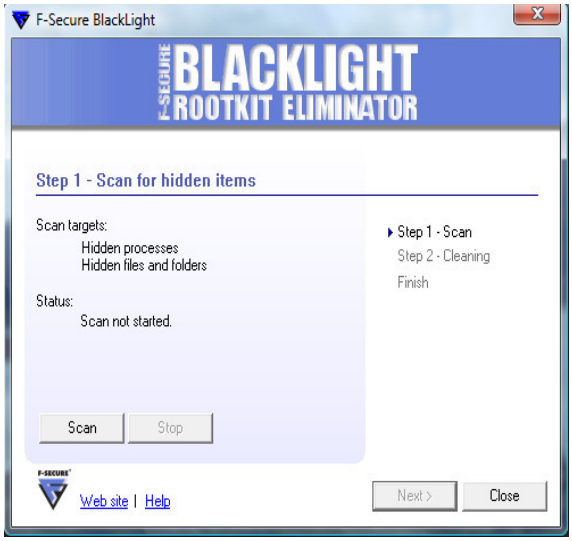
Usage:

- Click File → Scan, it will show number of discrepancies.
- Click File → Save.

You should examine all discrepancies.

3) BlackLight Eliminator:

F-secure's BlackLight is provide a simple, clean, and user friendly. Blacklight used to detect DKOM rootkits that hide processes. This is a stand-alone rootkits eliminator.



Installation:

Download the **fsbl2.2.exe** (1111 KB) file to your computer

- Double click the file→ Click Run, it will show error message F-secure BlackLight requires administrator privileges.
- Click → O.K. Now select the file right click select 'Run as administrator'
- Click → Run, select I accept the agreement
- Click → Next.

Usage:

Step1

- Click → Scan, after scanning 'show all processes' tab will appear
- Click → Show all processes, it will show number of process

Step2

- Click → Next, select the malicious file
- Click → Next, cleaning Malicious files
- Click → Close

IV. CONCLUSION

This paper provided a very high level practical techniques and tools. Any services are not 100% safe. If this scanner says 'OK', it does not necessarily mean the file is clean. There could be a new virus on the loose. Never ever rely on one single product only, in our suggestion minimum three or four different tools use, then take decision. We recommend using tools that are highly rated by industry magazines, industry experts, and security companies.

V. REFERENCES

1) Kris kendall, Practical Malware Analysis, Mandiant Intelligent Security. http://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Paper/bh-dc-07-Kendall_McMillan-WP.pdf

2) Lenny Zeltser, Introduction to Malware Analysis, SANS Institute. http://zeltser.com/reverse-malware/intro-to-malware-analysis.pdf

3) Michael Davis, Sean Bodmer, Aaron Lemasters. Hacking Exposed Malware & Rootkits Secrets & Solutions. The McGraw-Hill Companies.

4) Martin Overton, Malware Forensics: Detecting the Unknown. http://momusings.com/papers/VB2008-Malware-Forensics-1.01.pdf

5) Hitpop DDoS Malware Analysis, Public Version, Copyright Arbor Networks. http://atlas-public.ec2.arbor.net/docs/Hitpop_DDoS_Malware_Analysis_PUBLIC.pdf

6) Dean De Beer, Malware Analysis Challenge Part III. http://handlers.sans.org/pbueno/MALWARE%20ANALYSIS%20PART%20III.pdf

7) http://www.spyware-removal-info.com

8) http://searchsecurity.techtarget.com