IJCRT Publish Paper record is available at DOI: http://doi.one/10.1727/IJCRT.17175

Cybersecurity Tools and Methods

Ashwini D. Mate
ME student, Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai.

Dr.D.R.Ingle
Professor & HOD, Department of Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai.

***Abstract*—This report aims to study trends and issues in cyber security and analyze the cyber security tools. These cyber security tools are basically to overcome one major type of cyber crime known as malware attack. Here we focus on one of the malware known as Rootkit which resides in the kernel of the operating system and study various types of Rootkits. Based on the Rootkit malware, study and analysis of various anti-rootkit tools is performed. Comparative study of various anti-rootkit tools is done to select best tools based on different parameters used for comparison. Finally tools best for naïve users as well as IT professionals are analyzed based on the analysis of different tools in the report.**

***Keywords*—Cybersecurity, Antirootkit,Spy DLL Remover, Sanity Check, Root repeal.**

I. INTRODUCTION

From business, industry, government to not-for-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, it has also brought unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and a blossoming haven for cybercriminal miscreants to perpetrate their insidious acts. The Internet is one of the fastest-growing areas of technical infrastructure development. In today's business environment, disruptive technologies such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online .Today more than 80 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. The scope of Cyber Security extends not only to the security of IT systems within the enterprise, but also to the broader digital networks upon which they rely including cyber space itself and critical infrastructures. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. This paper seeks to give an overview of cyber-crime and cyber-security, cyber security tools and proffer solutions.

II. TOOLS USED IN CYBERSECURITY

A. **aswMBR**

aswMBR is a anti-rootkit scanner that searchs your computer for Rootkits that infect the Master Boot Record, or MBR, of your computer. This includes the TDL4/3, MBRoot (Sinowal), and Whistler rootkits. For this program to properly work it must first download the Avast virus definitions, so you will need an active Internet connection before using it. A rootkit is a malware program that is designed to hide itself or other computer infections on your computer. These types of programs are typically harder to remove than generic malware, which is the reason that stand-alone utilities such as TDSSKiller have been developed. When you run aswMBR, if it is shutdown automatically, then it is most likely the infection detecting that aswMBR is running and terminating it. In this situation you should rename executable to **iexplore.exe** before you attempt to run it.

aswMBR is a utility program designed to work in conjunction with other antivirus software to keep your computer safe from malware and other unwanted programs. It can complete thorough scans for rootkits associated with malware programs and remove them when a conventional uninstaller or antivirus cannot.

ADVANTAGES aswMBR

1. Quick and efficient: This program scans and performs repairs quickly. There are no fancy features involved, but you also don't have to tie up your computer for long periods of time to rid it of unwanted programs.
2. Avast antivirus compatibility: While aswMBR is not a complete antivirus program, it is made to work with Avast Free Antivirus, which you have to download and install separately. Together, they comprise a complete solution to your system protection needs.
3. Not for beginners: This program does not come with a Help feature, and the interface is as utilitarian as they come. If you don't already know your way around this type of tool or know how to interpret the scan results, this program won't be of much use to you. If you have some advanced computer knowledge and want to make sure your machine is free from all elements of malware programs, this is a good choice. It's free, and it does exactly what it promises. But it was not designed to be a one-stop solution for your antivirus needs. It's also not terribly accessible for inexperienced users.

4. Save log: This program save the log file in the specified folder.

B. CATCHME

Catchme is a powerful utility designed by gmer.net to remove malware and other malicious files.
It is NOT an antivirus program – it IS a virus removal tool..
It does not have a bloated user interface and quickly and efficiently cleans your system.

Unlike a mainstream antivirus program such as Symantec, kaspersky or McAfee, it is free and you do not install it and it will not slow your system to a halt. Simply download it , run it click scan button and allow catchme to scan your system.
The file, **catchme.exe**, that can be downloaded below is hosted right here on proposedsolution.com, a trusted source.

- Catchme.exe removes thousands of known viruses such as trojans and worms.
- Works for all current versions of Windows up to Vista (try later versions, it might work).
- You need administrator access for this to work (default for most Windows users).

Usage Instructions

To download catchme please do the following:

1. Click the '**Like**'button in the download area below to reveal the download links .
2. Save the file **catchme.exe** to your desktop.
3. Double-click catchme.exe and it will extract launch a simple user interface.
4. Click the scan button. A dos window will launch and display progress messages.
5. When the scan is finished, go to the Scripts tab and click the Run button if anything was found.
6. Click Restart button. This download is provided free and without any guarantee that it will solve your problems.

C. GMER

Ease of Use **GMER** is a software tool for detecting and removing root kits. Written by a Polish researcher Przemysław Gmerek. It runs on Microsoft Windows and has support for Windows NT, 2000, XP, Vista, 7 and 8. With version 2.0.18327 full support for Windows x64 is added. A rootkit is a malware program that is designed to hide itself or other computer infections on your computer. These types of programs are typically harder to remove than generic malware, which is the reason that stand-alone utilities such as TDSSKiller have been developed. At the time of first release in 2004 it introduced innovative rootkit detection techniques and quickly gained popularity for its effectiveness. It was incorporated into a few antivirus tools including avast antivirus and SDFix. For several months in 2006 and 2007, the tool's website was the target of heavy DDoS attacks attempting to block its downloads..

GMER is available as a random named .EXE files or a .ZIP file. When you run GMER, if it is shutdown automatically, then it is most likely the infection detecting that GMER is running and terminating it. In this situation you should use the .EXE download link to download a random named version of GMER. If you are unable to run that, then please rename the download to **iexplore.exe** before you attempt to run it.

GMER scans for the following:

- Hidden processes
- Hidden threads
- Hidden modules
- Hidden services
- Hidden files
- Hidden disk sectors (MBR)
- Hidden Alternate Data Streams
- Hidden registry keys
- Drivers hooking SSDT
- Drivers hooking IDT
- Drivers hooking IRP calls
- Inline hooks

D. SanityCheck

SanityCheck is an advanced rootkit and malware detection tool for Windows which thoroughly scans the system for threats and irregularities which indicate malware or rootkit behavior. By making use of special deep inventory techniques, this program detects hidden and spoofed processes, hidden threads, hidden drivers and a large number of hooks and hacks which are typically the work of rootkits and malware. It offers a comprehensible report which gives a detailed explanation of any irregularities found and offers suggestions on how to solve or further investigate any situation.

SanityCheck Features

1. Runs on almost all Windows versions:SanityCheck runs on most recent Windows versions including Windows 7, Windows8, Windows Vista and Windows XP. For an exact overview of the Windows versions supported by SanityCheck and the service packs required.
2. Makes use of special deep inventory techniques:- SanityCheck makes use of a special Windows feature (a Global Flag setting) which allows it to create a deep inventory of drivers, devices, processes, threads and a lot of other information about yoursystem. By making use of this feature in combination with other techniques it is able to create a very thorough scan of irregularities on your system.

3. Detect hidden processes: SanityCheck goes to incredible lengths to detect processes which hide themselves from the Windows taskmanager and programming interfaces. It uses seven unmentioned safe techniques to reveal hidden processes in both usermode and kernelmode.

4. Detect obfuscated processes: Sanity Check detects processes which do efforts to obfuscate their names. This is a typical activity associated with malware.
5. Detect processes attempting to appear as common system processes :Sanity Check detects for processes which appear as a standard Windows process.
6. Detect processes with obviously deceptive names: Malicious processes which are received as email attachements often try to appear as an innocent document types. An example of such a process name is:”foo.txt.exe”

7. Detect processes without product, company or description information: Although not necessarily evil, SanityCheck checks for processes without a product, company or description resource information.
8. Verify signatures and checksums of processes and kernel modules: Sanitycheck verifies digital signatures on processes and kernel modules and checks them for validity. It also verifies the validity of checksums.
9. Detect SSDT hooks: SanityCheck detects kernel modules which hook the system service descriptor table. Although not necessarily the work of malware, SanityCheck will do every effort to detect the modules responsbile for these acts and generate a comprehensible report.
10. Detect Import Address Table hooks: The program detects kernel modules which hook the entry points of exported kernel routines.

11. Detect kernel object callout hooks :Although rarely used, kernel object callout hooks are incredibly powerful and have the potential to instrument the complete working of the Windows kernel. Currently we do not know of any security product which detects these hooks.

12. Detect hidden drivers :SanityCheck detects various forms of kernel modules which are attempting to hide.

13. Detect hijacked driver entry points :Hijacked dispatch entry points in drivers can be used by rootkits and malware for a wide variety of purposes. SanityCheck detects both drivers which have their entry points hooked as well as the modules reponsible for these actions.

14. Find the culprit :Note that it is not always possible to make a clear distinction between malware and legitimate products. This is because certain products resort to aggressive controversial techniques as anti-piracy measures, to avoid debugging or even for anti-competitive purposes. Anitivirus or other security software that is installed on your system may be making use of rootkit-like techniques such as a hidden process in an effort to hide itself from malware. Such products may be involved in a controversial race along the lines of "defeat evil with its own weapons". For this reason SanityCheck does everything possible to pinpoint the modules and processes which are responsbile for these actions while remaining careful in drawing any conclusions.

15. Comprehensible report :We do not believe in aggressively "fixing" malware with a single click of a button. This is because there is no such thing as a clear distinction line between malware and legitimate products which make of controversial techniques. "Fixing" hooks in the kernel is a very unsafe and despicable act which is only very likely to make your system crash or worse. Instead Sanitycheck leaves your system in an unaltered state while offering comprehensible suggestions on how to proceed in any situation.
16. Optional expert mode: Optionally you can switch SanityCheck into expert mode. It will then display a wealth of information on drivers, devices, processes, threads, kernel objects and system routines which can be very useful for further analysis. A lot of the information available in expert mode cannot be obtained by any other existing utility other than a kernel debugger. Because the amount of information can be overwhelming and may be difficult to understand for novice users, it is turned off by default and only a comprehensible report is displayed.

E. Rootkit unhooker

Rootkit Unhooker is a straightforward utility that gives you the possibility of scanning and removing rootkits from your system. It also lets you terminate processes and drivers, among others. After a brief and uneventful setup procedure that does not require special attention from the user, you are greeted by a standard window with a well-structured layout. It is not eye-catching but easy to navigate. The main window includes multiple panels dedicated to SSDT, shadow SSDT, processes, drivers, stealth code, files, code hooks, and a report.
You can unhook one or more selected files, terminate processes (with or without force), view corresponding DLLs, dump all process memory, wipe or copy the file, as well as perform BSOD. This set of options applies to all items in the aforementioned panels.
Rootkit Unhooker creates a report with log activity and provides options for exporting it to file for further evaluation. Plus, you can change the background and text colors, show only hooked functions, hide grid lines, and use standard DiskIO. Settings may be restored to their factory values at any time.
The application is low-demanding when it comes to CPU and RAM. It has a good response time and finishes a task quickly and without errors. Unfortunately, Rootkit Unhooker has not been updated for a long while, and it is not supported by newer operating systems.

F. Vba32 AntiRootkit

Vba32 AntiRootkit is a powerful, portable, expert-level tool which will help you to analyse your PC, perhaps uncovering rootkits or other stealthy malware, and neutralise them, if only temporarily. (The program can't remove them, but it may be able to prevent the malware from hiding itself, allowing other antivirus tools to detect and delete it.) As with many similar tools, Vba32 AntiRootkit isn't for the inexperienced. Rootkit detection is a complex process involving much low-level trickery, so it's possible that simply running a scan may crash your PC. And AntiRootkit's reports are highly technical, with details of hooks, stacks, minifilters and more: you'll need plenty of in-depth Windows knowledge to properly understand what's going on. If you're willing to give the program a try, though, exploring the Tools menu reveals all kinds of useful features and functionality.
A built-in scanner will detect hidden or locked files, for instance. The Autorun option gives in-depth information on everything configured to load when Windows starts. In just a click or two you can delete suspect entries, or open them in REGEDIT for further investigation. A similar module allows you to view and manage your installed drivers and services. You can look at currently loaded kernel modules, running processes and more. And if you're sure you know what you're doing then a particular driver or DLL can be deleted at a click (though again, be hugely careful, make a mistake here and you could trash your PC).
AntiRootkit can report on many low-level system tweaks: kernel mode-hooks, notifications, filter drivers and more. If you find a hook associated with a suspect file then you can remove it, though once again, this is risky and could crash your PC. And assorted bonus extra tools provide useful information about your network settings, like your Hosts file, LSP providers, Windows firewall configuration and more.

Vba32 AntiRootkit is a complex tool which can crash your PC in a moment if you're not careful, so it's not for most people. If you're a Windows and security expert, though, you'll appreciate just how many useful features Vba32 have crammed into this tiny, portable package, and it's well worth including in your malware-hunting toolkit.

Vba32 AntiRootkit advantages:
1.Free of charge.
2. Does not require installation.
3. Can be used with any antivirus software installed on your computer.
4. Uses a unique feature of the detection of "clean" files.
5. Can be used in several modes.
6. Supports the maintenance of a system status report in html format.
7. Treatment of the system may be done using a scripting language.
8. Supports Windows7.
9. Help files in Russian and English languages.
10. Part of Vba32 Personal and Vba32 Check.

G. Rkdetector

Rkdetector was the first new generation rootkit detector tool, offering same features as the most known Sysinternals RootkitRevealer Software. Rkdetector engine is free for personal usage, however if you want to deploy it for a security reviews you can buy a license at main rkdetector website and also get a console edition, that allows you check systems from a command line, or from an startup script.
Rkdetector Features:

- Hidden File detection.
- Hidden registry keys detection.
- ADS (Alternate Data Streams) detection.
- Rootkit deletion, by wipping the used binary files and rebooting the system.
- Data recovery for both FAT32 and NTFS file system.

- File system browser.

2.8 SpyDLLRrmover

SpyDllRemover is the specialized tool for detecting SPYWARE & Hidden Rootkit Dlls in the System.
In addition to SPYWARE Dlls, it can also detect userland Rootkit processes using multiple AntiRootkit techniques. It uses Heuristic analysis and 'Online Threat Verification' for deeper analysis of unknown malware Threats. One of the unique feature of SpyDllRemover is 'Advanced Dll Ejection' which helps in completely remving spyware /Rootkit Dlls from any running Process. It works very well with any Remote process across the session boundaries imposed in Vista/Windows7.
All these unique features makes it one of the generic tool for removing known as well as Unknown Threats compared to traditional antivirus software which can detect only known threats.
SpyDllRemover is fully Portable software and works on wide range of platforms starting from Windows XP to Windows 8.

Features of SpyDllRemover.

- Advanced Spyware Scanner: Detects Hidden user land Rootkit processes as well as suspicious/injected Dlls within running Processes.
- Hidden Rootkit Detection & Removal: Uses multiple techniques to detect user land Rootkits
  Direct NT System Call Implementation.
  Process ID Brute force Method (PIDB) as first used by Black Light.
  CSRSS Process Handle Enumeration Method.
- Unique 'Advanced DLL Ejection': This is one of the Advanced & U nique feature of SpyDLLRemover used to completely remove the injected DLL from Remote Process.
- Sophisticated Auto Analysis: Dll & Process Heuristics to help in Identification of known as well as Unknown Threats.
- Color based Representation: For clear and easier analysis of various type of SPYWARE Threats.
- Online Threat Verification: Scan suspicious Processes/DLLs using online services such as VIRUSTOTAL , Threat Expert, Process Library and Google.
- 'DLL Tracer' Feature: Search for suspicious DLL within all running processes.
- Cooler GUI Interface: Attractive, Easy to U se & Customizable interface.
- Advanced Report: Generates complete report of Processes/Dlls along with Threat Analysis.
- Portable Version: You can easily run it directly without installation.
- Integrated Installer: It also comes with Installer to help you in local Installation & U ninstallation.

III COMPARISON TABLE OF TOOLS USED IN CYBERSECURITY

Anti-rootkit tools	Version	Active	Memory scanning	Register scan	Driver scan	SSDT scan	Scan time min	Hooking detection	Removal	Best feature
aswMBR	1.0.1.2252	Yes	Yes	No	No	No	0.23	No	Yes	Memory scan
SanityCheck	3.00	Yes	Yes	No	Yes	No	0.20	No	No	Driver scan
Catchme	0.3	Yes	Yes	No	No	No	0.15	No	Yes	Removal
SpyDLLRemover	6.0	Yes	Yes	No	No	No	0.10	No	No	Memory scan
Rootkit Unhooker	3.7.300.509	Yes	Yes	No	Yes	Yes	7.30	Yes	Yes	Hooking
RKDector	2.0	Yes	No	No	No	No	1.0	No	Yes	Hooking
GMER	2.1.19357	Yes	Yes	Yes	Yes	Yes	9.0	Yes	Yes	Removal
Vba32 Antirootkit	3.12.5.4	Yes	Yes	No	No	No	12.5	Yes	No	Hooking

IV CONCLUSION

SPYDLLRemover and GMER are the best tools to work with as they does not include complex terms and for IT professionals who have thorough knowledge of various terms used in security, RootkitUnhooker and VBA32 Anti Rootkit are the best tools to use as Rootkit Unhooker provided ability to unhook the Rootkit attached to the code and VBA32 provides all the kernel modules driver files location size related information which can be used to detect rootkits residing in the kernel of the system.
Based on the results of the Anti Rootkit scans, further research should focus on developing an optimal set of heuristic-based rules to detect rootkit activity, which maximizes the rate of detection while minimizing the rate of false positives.

REFERENCES

[1] International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy.
[2] IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July2013.
[3] A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
[4] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole.
[5] Yang, Miao, "ACM International Conference Proceeding Series", vol. 113.
[6] International Journal of Engineering and Technology Volume 4 No. 1, January, 2014 ISSN: 2049-3444 © 2014 – IJET Publications UK. All rights reserved. 48 "A Study of Cyber Security Challenges and I Technologies" G.Nikhita Reddy1 G.J.Ugander Reddy2.
[7] "Privacy and Cybersecurity: The Next 100 Years" By Carl Landwehr, Senior Member IEEE, Dan Boneh, John C. Mitchell, Steven M. Bellovin, Susan Landau, Member IEEE, and Michael E. Lesk, Member IEEE.
[8] Computer Science and Telecommunications 2010|No.6(29) ISSN 1512-1232 56 "CYBER SECURITY: CHALLENGES AND THE WAY FORWARD" Azeez Nureni Ayofe, Barry Irwin
[9] "Meeting the Cyber Security Challenge" Gustav Lindstrom GCSP Geneva Papers — Research Series n° 7, June 2012.
[10] Volume 4, Issue 4, April 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering "Cyber Security Issues and Recommendations" Anoop Kumar Verma Aman Kumar Sharma.
[11] "Some Fundamental Cybersecurity Concepts" KELCE S. WILSON1 (Senior Member, IEEE) AND MÜGE AYSE KIY2 date of publication February 11, 2014, date of current version February 20, 2014.