ROOTKITS CONFISCATION TOOLS IN CYBERSECURITY

Harish Sonawane Om Chaskar

Student Student

Symbiosis skills and professional university Symbiosis skills and professional university

Pune, Maharashtra Pune, Maharashtra

[harishsonawane4044@gmail.com](mailto:harishsonawane4044@gmail.com) [omchaskar1@gmail.com](mailto:omchaskar1@gmail.com)

Snehal Jadhav himalay jasud

Student Student

Symbiosis skills and professional university Symbiosis skills and professional university

Pune, Maharashtra Pune, Maharashtra

[ssnehaljjadhav@gmail.com](mailto:ssnehaljjadhav@gmail.com) [himalay.jasud2004@gmail.com](mailto:himalay.jasud2004@gmail.com)

ABSTRACT

Cybersecurity has become an integral aspect of the modern technological landscape, with organizations and individuals relying on digital systems for various activities. As the digital realm expands, so does the threat landscape, necessitating robust measures to safeguard sensitive information and critical infrastructures. This paper explores the importance of tools in modern cybersecurity, focusing on their role in detecting, preventing, and mitigating cyber threats.

This report aims to study trends and issues in cyber security and analyze cyber security tools. These cyber security tools help to overcome one primary type of cybercrime: malware attack. Here, we focus on one of the malware known as Rootkit, which resides in the operating system's kernel, and study various types of Rootkits. Based on the Rootkit malware, a study and analysis of various anti-rootkit tools are performed. A comparative study of various anti-rootkit tools is done to select the best tools based on different parameters used for comparison. Finally, tools best for naïve users and IT professionals are analyzed based on the analysis of other tools in the report.

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

# INTRODUCTION

The Internet has dramatically streamlined business processes across various sectors, including business, industry, government, and not-for-profit organizations. Tasks such as sorting, predicting, summarizing, coding, editing, and generating customized and generic reports can now be efficiently processed in real time. However, along with these benefits, the Internet has also introduced unintended consequences, such as criminal activities, including spamming, credit card fraud, ATM fraud, phishing, identity theft, and providing a platform for cybercriminals to perpetrate their nefarious acts [1].

The Internet represents one of the most rapidly expanding areas of technical infrastructure development. In today's business landscape, disruptive technologies such as cloud computing, social computing, and next-generation mobile computing fundamentally alter how organizations leverage information technology for sharing information and conducting online commerce [2]. With over 80 percent of total commercial transactions now occurring online, robust security measures are needed to ensure transparent and secure transactions.

Cyber security not only safeguards IT systems within enterprises but also protects the broader digital networks on which they rely, including cyberspace itself and critical infrastructures [3]. Cyber security plays a pivotal role in advancing information technology and internet services. Enhancing cyber security and fortifying essential information infrastructures is crucial for ensuring each nation's security and economic prosperity [5-6][8]. Promoting internet safety and safeguarding users have become integral to new service development and governmental policy [9][10].

This paper aims to provide an overview of cybercrime and cyber security, discuss cyber security tools, and propose solutions to these evolving challenges.

II. **METHOD TOOLS IN CYBERSECURITY**

### aswMBR

aswMBR is an anti-rootkit scanner designed to detect rootkits that infect the Master Boot Record (MBR) of your computer, including the TDL4/3, MBRoot (Sinowal), and Whistler rootkits. Before using aswMBR, an active Internet connection is required to download the definitions of the Avast virus. Rootkits are a type of malware program designed to conceal themselves or other infections on a computer, often making them more difficult to remove than generic malware.

Here are some critical reasons for using aswMBR:

Quick and efficient: This program conducts scans and repairs swiftly without requiring extended periods. While it lacks advanced features, it offers a speedy solution for removing unwanted programs.

Avast antivirus compatibility: Although aswMBR is not a standalone program, it is compatible with Avast Free Antivirus. When used together, they provide comprehensive protection for your system.

Not suitable for beginners: The program needs a Help feature and features a straightforward interface. It may not be ideal for users unfamiliar with such tools or those unable to interpret scan results. However, for users with advanced computer knowledge to ensure their system is free from malware, aswMBR offers a viable option. It's free and delivers on its promises, but it is intended as something other than a sole antivirus solution and may pose challenges for inexperienced users.

Overall, aswMBR is a valuable tool for experienced users seeking to detect and remove rootkits from their systems, mainly when used with Avast Free Antivirus.

### 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; you do not install it, and it will not slow your system to a halt. Download it, run it, click the scan button, and allow Catchme to scan your system. The catchme.exe file that can be downloaded below is hosted on proposedsolution.com, a trusted source.

### GMER

GMER is a software tool developed by Polish researcher Przemysław Gmerek aimed to detect and remove rootkits. Compatible with Microsoft Windows operating systems, including Windows NT, 2000, XP, Vista, 7, and 8, and offering full support for Windows x64 starting from version 2.0.18327, GMER has been a notable tool in the field since its initial release in 2004.

A rootkit is a form of malware designed to conceal itself or other malicious software on a computer, presenting a challenge for removal compared to generic malware. GMER introduced innovative rootkit detection techniques upon its release, quickly gaining popularity for its effectiveness. It was even integrated into several antivirus tools, such as Avast and SDFix.

GMER is available for download as either randomly named. EXE files or a . ZIP file. In cases where GMER shuts down automatically upon execution, it's likely due to an infection detecting and terminating it. In such situations, users are advised to download the randomly named version of GMER using the EXE download link. If running the tool proves difficult, renaming the download to "iexplore.exe" before attempting to execute it may bypass the issue.

It's worth noting that GMER's website faced significant DDoS attacks aimed at blocking downloads during several months in 2006 and 2007.

In summary, GMER remains a valuable tool for identifying and removing rootkits, offering advanced detection techniques and compatibility with various Windows operating systems. If you cannot run that, please rename the download to iexplore.exe before you attempt to run it.

GMER scans for the following:

1. Hidden processes

2. Hidden threads

3. Hidden modules

4. Hidden services

5. Hidden files

6. Hidden disk sectors (MBR)

7. Hidden Alternate Data Streams

8. Hidden registry keys

9. Drivers hooking SSDT

10. Drivers hooking IDT

11. Drivers hooking IRP calls

12. Inline hooks

### SanityCheck

SanityCheck is an advanced rootkit and malware detection tool for Windows operating systems. It is adept at identifying and removing rootkits and other forms of malware that may compromise the security of your system. This tool utilizes sophisticated techniques to thoroughly scan your system for any signs of malicious activity, providing users with peace of mind regarding the safety and integrity of their computer. While its primary function is to thoroughly scan systems for threats and irregularities indicative of malware or rootkit behavior, it could also aid in identifying plagiarism or detecting unauthorized copying of content. Utilizing inventory techniques can detect hidden and spoofed processes, hidden threads, hidden drivers, and various hooks and hacks commonly associated with rootkits and malware. The program provides a comprehensible report with detailed explanations of any irregularities found, offering suggestions for resolution or further investigation. SanityCheck allows the use of the following activities:

1. Runs on almost all Windows versions: SanityCheck runs on the most recent Windows versions, including Windows 7, Windows 8, 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 uses 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 your system. Using this feature in combination with different techniques can create a comprehensive scan of irregularities in your system.

3. Detect hidden processes: SanityCheck goes to incredible lengths to detect processes that hide themselves from the Windows task manager and programming interfaces. It uses seven unmentioned safe techniques to reveal hidden processes in user and kernel modes.

4. Detect obfuscated processes: Sanity Check detects processes that make it impossible to obfuscate their names. This is a typical activity associated with malware.

5. Detect processes attempting to appear as standard system processes: Sanity Check detects processes that occur as a standard Windows process.

### Rootkit unhooker

Rootkit Unhooker is a straightforward utility that allows you to scan and remove 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, and perform BSOD. This set of options applies to all items in the panels above. Rootkit Unhooker creates a report with log activity and provides options for exporting it to a 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 newer operating systems do not support it.

### Vba32 AntiRootkit

Vba32 AntiRootkit is a potent and portable tool designed for experts to analyze PCs, potentially uncovering rootkits or other hidden malware and temporarily neutralizing them. While the program cannot permanently remove these threats, it may prevent them from concealing themselves, enabling other antivirus tools to detect and delete them. However, the Vba32 AntiRootkit is only suitable for experienced users. Rootkit detection involves intricate low-level processes, and running a scan may crash your PC. Furthermore, the tool's reports are highly technical, requiring deep Windows knowledge to comprehend fully.

Despite these complexities, Vba32 AntiRootkit offers a range of valuable features accessible through its Tools menu. It includes a built-in scanner for detecting hidden or locked files, an Autorun option providing detailed information on Windows startup configurations, and modules for managing installed drivers and services. Users can examine currently loaded kernel modules, running processes, and more, with the ability to delete suspect entries or open them in REGEDIT for further investigation. Additionally, the tool reports on low-level system tweaks such as kernel mode hooks and filter drivers, providing options to remove associated hooks if necessary, although this carries the risk of crashing the PC.

Moreover, Vba32 AntiRootkit includes supplementary tools offering insights into network settings, including the Hosts file, LSP providers, and Windows firewall configuration. While Vba32 AntiRootkit is a sophisticated tool with numerous features, it can pose a risk of crashing your PC if mishandled. Therefore, it is best suited for Windows and security experts who can navigate its complexities safely. For those individuals, the tool offers a comprehensive and valuable addition to their malware-hunting arsenal.

1. Free of charge.

2. Does not require installation.

3. Can be used with any antivirus software installed on your computer.

4. It uses a unique feature to detect "clean" files.

5. Can be used in several modes.

7) *SpyDLLRrmover*

SpyDllRemover is a specialized tool to detect SPYWARE and hidden rootkit Dlls within a system. Alongside identifying SPYWARE Dlls, it possesses the capability to detect userland rootkit processes through the utilization of multiple AntiRootkit techniques. Employing heuristic analysis and 'Online Threat Verification,' SpyDllRemover conducts deeper analyses of unknown malware threats. One of its standout features is 'Advanced Dll Ejection,' which facilitates the complete removal of spyware and rootkit Dlls from any running process.

SpyDllRemover excels in working with remote processes across session boundaries imposed in Vista and Windows 7. Its unique attributes distinguish it from traditional antivirus software, as it can detect known and unknown threats. Being fully portable, SpyDllRemover is compatible with various platforms, from Windows XP to Windows 8.

Overall, SpyDllRemover is essential in combating spyware and rootkit infections, providing users with advanced features for comprehensive threat detection and removal. The SpyDllRemover provides the platform with the following features:

1. Advanced Spyware Scanner: Detects Hidden userland Rootkit processes and suspicious/injected Dlls within running Processes.

2. Hidden Rootkit Detection & Removal: Multiple techniques 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.

3. Unique 'Advanced DLL Ejection': This is one of the Advanced & Unique features of SpyDLLRemover used to remove the injected DLL from the Remote Process.

4. Sophisticated Auto Analysis: Dll & Process Heuristics to help in the Identification of known as well as Unknown Threats.

5. Color-based Representation: For precise and more straightforward analysis of various types of SPYWARE Threats.

6. Online Threat Verification: Scan suspicious Processes/DLLs using online services such as VIRUSTOTAL, Threat Expert, Process Library, and Google.

7. 'DLL Tracer' Feature: Search for suspicious DLL within all running processes.

8. Cooler GUI Interface: Attractive, Easy to use & Customizable interface.

9. Advanced Report: Generates a complete report of Processes/Dlls and Threat Analysis.

10. Portable Version: You can quickly run it directly without installation.

11. Integrated Installer: It also comes with an Installer to help you with local Installation & U installation.

# COMPARISON TABLE OF TOOLS USED IN CYBERSECURITY STUDY

Table 1: Comparative analysis between various tools used in this study

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Anti-rootkit tools | Version | Active | Memor y scanni ng | Register scan | Driver scan | SSDT scan | Scan time min | Hookin g detectio n | Remo val | Best feature |
| aswMBR | 1.0.1.22 52 | 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 |
| SpyDLLRe mover | 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 | 2.1.193 57 | 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 |

# Table 1 represents the comparative analysis between the antirootkit tools using various parameters such as version, memory scanning, driver scan, SSDT scan, scan time, hooking detection, removal and features

# 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. G.Nikhita Reddy, G.J.Ugander Reddy, “Study of Cloud Computing in HealthCare”, Industry International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518
2. R. Bloomfield and J. Lala, "Safety-Critical Systems: The Next Generation," in *IEEE Security & Privacy*, vol. 11, no. 4, pp. 11-13, July-Aug. 2013, doi: 10.1109/MSP.2013.95
3. <https://www.yumpu.com/en/document/view/4796989/eight-trends-that-are-changing-network-security-sophos> [Accessed on date: 7th March 2024]
4. “Cyber Security: Understanding Cyber Crimes”- Sunit Belapure, Nina Godbole ISBN-13 978-8126521791,Publisher Wiley, Publication date,1 January 2011
5. Seng-Phil Hong and Sungmin Kang. “Ensuring privacy in smartcard-based payment systems: a case study of public metro transit systems”,. In Proceedings of the 10th IFIP TC-6 TC-11 international conference on Communications and Multimedia Security (CMS'06). Springer-Verlag, Berlin, Heidelberg, 206–215. 2006. https://doi.org/10.1007/11909033\_1
6. “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.
7. Noor, Basirah, and Sana Qadir. 2023. "Machine Learning and Deep Learning Based Model for the Detection of Rootkits Using Memory Analysis" *Applied Sciences* 13, no. 19: 10730. <https://doi.org/10.3390/app131910730>
8. Xiongwei Xie, Weichao Wang," Rootkit Detection on Virtual Machines through Deep Information Extraction at Hypervisor-level ",4th International Workshop on Security and Privacy in Cloud Computing 2013, pp 498- 503
9. xingyiquan - simple linux kernel rootkit for kernel 3.x and kernel 2.6.x. <https://sw0rdm4n.wordpress.com/2014/11/03/xingyiquan-simple-linux-kernel-rootkit-for-kernel-3-x-and-kernel-2-6-x/>
10. Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, *et al.* 2019. Spectre attacks: Exploiting speculative execution. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1–19.