

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

I
J
R
C
M



A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.

Open J-Gate, India [link of the same is duly available at Inlibnet of University Grants Commission (U.G.C.)].

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 4255 Cities in 176 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

<http://ijrcm.org.in/>

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1.	IMPACT OF WORKING CAPITAL MANAGEMENT ON THE PROFITABILITY OF LISTED CEMENT COMPANIES IN TANZANIA <i>DR. SRINIVAS MADISHETTI & DR. NSUBILI ISAGA</i>	1
2.	A STUDY ON COST OF REJECTION (REJECTED SAMPLES) IN A NABL ACCREDITED LABORATORY AT A POST GRADUATE TEACHING HOSPITAL IN DEHRADUN, UTTARAKHAND <i>PIYALI MITRA M., RIMMA MANDAL, M. M. MATHAVAN & DR. VIBHA GUPTA</i>	9
3.	BORDER GUARDS SYSTEMS USING HYBRID WIRELESS SENSOR NETWORKS <i>T. DEEPIGA, A. SIVASANKARI & S. A. SHOBA</i>	15
4.	INDEPENDENT ACCESS TO ENCRYPTED CLOUD DATABASES <i>ROHINI GAIKWAD, VAISHALI GHATE & JALPA MEHTA</i>	20
5.	SECURE IMAGE TRANSMISSION USING LOSSLESS ARITHMETIC CODING <i>AASHA M. VANVE, ABIRAMI SIVAPRASAD & SWATI DESHPANDE</i>	23
6.	SPAM ZOMBIE DETECTION SYSTEM <i>RUTUJA BANKAR, JYOTI DESHMUKH & SWATI DESHPANDE</i>	28
7.	SECURE AND SCALABLE DATA SHARING IN CLOUD STORAGE WITH KEY-AGGREGATE CRYPTOSYSTEM <i>B. RAJESH, D. L. SRINIVAS & A. EMMANUEL RAJU</i>	32
8.	IDENTIFYING LISTENING SKILLS AMONG BOYS AND GIRLS OF ARTS AND SCIENCE COLLEGE STUDENTS <i>K. ELAMATHI</i>	36
9.	A STUDY ON FINANCIAL HEALTH OF SELECTED SOFTWARE COMPANIES IN INDIA <i>R. DEVIPRASANNA</i>	39
10.	BORDER PATROL SYSTEMS-USING ADVANCED WIRELESS SENSOR NETWORKING DEVICES <i>T. DEEPIGA & A. SIVASANKARI</i>	43
11.	THE NEW SOCIAL CONTRACT FOR GREEN BUSINESS <i>RAJEEV GUPTA</i>	46
12.	DATA SECURITY AND PRIVACY PROTECTION IN CLOUD COMPUTING <i>ROHINI GAIKWAD & JALPA MEHTA</i>	50
13.	SURVEY OF VARIOUS CRYPTOGRAPHIC TECHNIQUES <i>AASHA M. VANVE & ABIRAMI SIVAPRASAD</i>	56
14.	CYBER SECURITY TRENDS, ISSUES AND ANALYSIS OF TOOLS <i>RUTUJA BANKAR & LUKESH KADU</i>	63
15.	DETERMINANTS OF THE CUSTOMER LOYALTY IN ETHIOPIAN BANKING INDUSTRY (WITH REFERENCE TO PRIVATE COMMERCIAL BANK) <i>TEKABE SINTAYEHU & MOHAMMAD SULTAN</i>	74
16.	KNOWLEDGE DISCOVERY IN DATABASES <i>ANANT KUMAR</i>	81
17.	GREEN MARKETING: PATH TO SUSTAINABLE DEVELOPMENT <i>VANDANA BALA</i>	86
18.	IMPLICATION OF REGULATION ON THE DEVELOPMENT OF MICROFINANCE IN THE NIGERIAN ECONOMY <i>GODSPOWER GODWIN ITEMEH</i>	90
19.	AN ASSESSMENT OF TAX EVASION LEVEL AMONG NIGERIAN TAXPAYERS <i>ZAKARIYA'U GURAMA</i>	94
20.	AUTOMATIC PROFILE CHANGING USING ANDROID PHONES AS PER GPS LOCATION <i>R. SARVANI & R. KUMARI</i>	98
	REQUEST FOR FEEDBACK & DISCLAIMER	105

CHIEF PATRON

PROF. K. K. AGGARWAL

Chairman, Malaviya National Institute of Technology, Jaipur

(An institute of National Importance & fully funded by Ministry of Human Resource Development, Government of India)

Chancellor, K. R. Mangalam University, Gurgaon

Chancellor, Lingaya's University, Faridabad

Founder Vice-Chancellor (1998-2008), Guru Gobind Singh Indraprastha University, Delhi

Ex. Pro Vice-Chancellor, Guru Jambheshwar University, Hisar

FOUNDER PATRON

LATE SH. RAM BHAJAN AGGARWAL

Former State Minister for Home & Tourism, Government of Haryana

Former Vice-President, Dadri Education Society, Charkhi Dadri

Former President, Chinar Syntex Ltd. (Textile Mills), Bhiwani

FORMER CO-ORDINATOR

DR. S. GARG

Faculty, Shree Ram Institute of Business & Management, Urjani

ADVISORS

PROF. M. S. SENAM RAJU

Director A. C. D., School of Management Studies, I.G.N.O.U., New Delhi

PROF. S. L. MAHANDRU

Principal (Retd.), Maharaja Agrasen College, Jagadhri

EDITOR

PROF. R. K. SHARMA

Professor, Bharti Vidyapeeth University Institute of Management & Research, New Delhi

EDITORIAL ADVISORY BOARD

DR. RAJESH MODI

Faculty, Yanbu Industrial College, Kingdom of Saudi Arabia

PROF. PARVEEN KUMAR

Director, M.C.A., Meerut Institute of Engineering & Technology, Meerut, U. P.

PROF. H. R. SHARMA

Director, Chhatrapati Shivaji Institute of Technology, Durg, C.G.

PROF. MANOHAR LAL

Director & Chairman, School of Information & Computer Sciences, I.G.N.O.U., New Delhi

PROF. ANIL K. SAINI

Chairperson (CRC), Guru Gobind Singh I. P. University, Delhi

PROF. R. K. CHOUDHARY

Director, Asia Pacific Institute of Information Technology, Panipat

DR. ASHWANI KUSH

Head, Computer Science, University College, Kurukshetra University, Kurukshetra

DR. BHARAT BHUSHAN

Head, Department of Computer Science & Applications, GuruNanakKhalsaCollege, Yamunanagar

DR. VIJAYPAL SINGH DHAKA

Dean (Academics), Rajasthan Institute of Engineering & Technology, Jaipur

DR. SAMBHAVNA

Faculty, I.I.T.M., Delhi

DR. MOHINDER CHAND

Associate Professor, KurukshetraUniversity, Kurukshetra

DR. MOHENDER KUMAR GUPTA

Associate Professor, P.J.L.N.GovernmentCollege, Faridabad

DR. SHIVAKUMAR DEENE

Asst. Professor, Dept. of Commerce, School of Business Studies, Central University of Karnataka, Gulbarga

DR. BHAVET

Faculty, Shree Ram Institute of Engineering & Technology, Urjani

ASSOCIATE EDITORS

PROF. ABHAY BANSAL

Head, Department of Information Technology, Amity School of Engineering & Technology, Amity University, Noida

PROF. NAWAB ALI KHAN

Department of Commerce, AligarhMuslimUniversity, Aligarh, U.P.

ASHISH CHOPRA

Sr. Lecturer, Doon Valley Institute of Engineering & Technology, Karnal

FORMER TECHNICAL ADVISOR

AMITA

Faculty, Government M. S., Mohali

FINANCIAL ADVISORS

DICKIN GOYAL

Advocate & Tax Adviser, Panchkula

NEENA

Investment Consultant, Chambaghat, Solan, Himachal Pradesh

LEGAL ADVISORS

JITENDER S. CHAHAL

Advocate, Punjab & Haryana High Court, Chandigarh U.T.

CHANDER BHUSHAN SHARMA

Advocate & Consultant, District Courts, Yamunanagar at Jagadhri

SUPERINTENDENT

SURENDER KUMAR POONIA

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography; Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** **anytime** in **M.S. Word format** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website ([FOR ONLINE SUBMISSION, CLICK HERE](#)).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled ' _____ ' for possible publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR :

Designation :

Institution/College/University with full address & Pin Code :

Residential address with Pin Code :

Mobile Number (s) with country ISD code :

Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No) :

Landline Number (s) with country ISD code :

E-mail Address :

Alternate E-mail Address :

Nationality :

NOTES:

- a) The whole manuscript has to be in **ONE MS WORD FILE** only, which will start from the covering letter, inside the manuscript. **pdf. version is liable to be rejected without any consideration.**
- b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail:**
New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)
- c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.
- d) The total size of the file containing the manuscript is expected to be below **1000 KB**.
- e) **Abstract alone will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.
- f) **The journal gives acknowledgement w.r.t. the receipt of every email within twenty four hours** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.
- g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE:** The title of the paper should be **bold typed, centered and fully capitalised**.
3. **AUTHOR NAME (S) & AFFILIATIONS:** Author (s) **name, designation, affiliation (s), address, mobile/landline number (s), and email/alternate email address** should be given underneath the title.
4. **ACKNOWLEDGMENTS:** Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.
5. **ABSTRACT:** Abstract should be in **fully italicized text**, ranging between **150 to 300 words**. The abstract must be informative and explain the background, aims, methods, results & conclusion in a **SINGLE PARA. Abbreviations must be mentioned in full.**
6. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations.
7. **JEL CODE:** Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php, however, mentioning JEL Code is not mandatory.
8. **MANUSCRIPT:** Manuscript must be in **BRITISH ENGLISH** prepared on a standard A4 size **PORTRAIT SETTING PAPER. It should be free from any errors i.e. grammatical, spelling or punctuation. It must be thoroughly edited at your end.**
9. **HEADINGS:** All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
10. **SUB-HEADINGS:** All the sub-headings must be bold-faced, aligned left and fully capitalised.
11. **MAIN TEXT:**

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:**INTRODUCTION****REVIEW OF LITERATURE****NEED/IMPORTANCE OF THE STUDY****STATEMENT OF THE PROBLEM****OBJECTIVES****HYPOTHESIS (ES)****RESEARCH METHODOLOGY****RESULTS & DISCUSSION****FINDINGS****RECOMMENDATIONS/SUGGESTIONS****CONCLUSIONS****LIMITATIONS****SCOPE FOR FURTHER RESEARCH****REFERENCES****APPENDIX/ANNEXURE****The manuscript should preferably range from 2000 to 5000 WORDS.**

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR, centered, separately numbered** & self explained, and **titles must be above the table/figure. Sources of data should be mentioned below the table/figure. It should be ensured that the tables/figures are referred to from the main text.**
13. **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.
14. **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.
15. **REFERENCES:** The list of all references should be alphabetically arranged. **The author (s) should mention only the actually utilised references in the preparation of manuscript** and they are supposed to follow Harvard Style of Referencing. **Also check to make sure that everything that you are including in the reference section is duly cited in the paper.** The author (s) are supposed to follow the references as per the following:
- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
 - Use **(ed.)** for one editor, and **(ed.s)** for multiple editors.
 - When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
 - Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
 - The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
 - For titles in a language other than English, provide an English translation in parenthesis.
 - **Headers, footers, endnotes and footnotes should not be used in the document.** However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders after the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 <http://epw.in/user/viewabstract.jsp>

CYBER SECURITY TRENDS, ISSUES AND ANALYSIS OF TOOLS**RUTUJA BANKAR****STUDENT****SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE****CHEMBUR****LUKESH KADU****ASST. PROFESSOR****SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE****CHEMBUR****ABSTRACT**

As a response to the changing threat landscape today, most governments are looking to establish some form of Cyber security strategy. 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

Cyber-security, rootkit, malware.

1. INTRODUCTION

Cyber security is rightly a priority for governments globally. The phenomenal expansion of cyberspace has brought unprecedented economic growth, opportunity, and prosperity. However, it also presents bad actors with completely new threat and crime opportunities.

The interests of industry and governments in securing and facilitating cyber-based transactions and activities are fundamentally aligned. All companies want a secure digital infrastructure for commercial transactions. To ensure the continued viability of the infrastructure and growth of their sector, technology companies are highly motivated to design and build security into the DNA of their products and systems. Governments need a secure global digital infrastructure for economic growth, prosperity, efficiency, and protection.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber crime needs a comprehensive and a safer approach. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes.

2. REVIEW OF LITERATURE

The issue of cyber-crime is one that has been discussed by many people with various perspectives on the issue, most coming at it from different sides than the others. Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as the United States. According to a publication in which states that "the adoption by all countries of appropriate legislation against the misuse of Information and Communication Technology (ICT), for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security". The illegal act may be targeted at a computer network or devices e.g., computer virus, denial of service attacks (DOS), malware (malicious code). The illegal act may be facilitated by computer network or devices with target independent of the computer network or device. Cyber-crime is complex and committed mostly from remote locations making it difficult to police. The absence of enabling law makes policing even more difficult.

2.1 TRENDS CHANGING CYBER SECURITY**2.1.1 WEB SERVERS**

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. Web servers are especially the best platform for these cyber criminals to steal the data.

2.1.2 CLOUD COMPUTING AND ITS SERVICES

World is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security.

2.1.3 APT'S AND TARGETED ATTACKS

APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks.

2.1.4 MOBILE NETWORKS

Mobile networks security is a very big concern. These days' firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.

2.1.5 IPV6: NEW INTERNET PROTOCOL

Protecting IPv6 is not just a question of porting IPv4 capabilities. [6] While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.

2.1.6 ENCRYPTION OF THE CODE

In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity.

2.2 ISSUES IN CYBER SECURITY**2.2.1 MOBILE DEVICES AND APPS**

The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber attack, as each creates another vulnerable access point to networks. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning.

2.2.2 SOCIAL MEDIA NETWORKING

Growing use of soc media will contribute to personal cyber threats. Social media adoption among businesses is skyrocketing and so is the threat of attack. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

2.2.3 CLOUD COMPUTING

More firms will use cloud computing. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing [10]. As cloud use rises, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

2.2.4 PROTECT SYSTEMS RATHER INFORMATION

The emphasis will be on protecting information, not just systems. As consumers and businesses are like move to store more and more of their important information online, the requirements for security will go beyond simply managing systems to protecting the data these systems house. Rather than focusing on developing processes for protecting the systems that house information, more granular control will be demanded - by users and by companies - to protect the data stored therein.

2.2.5 NEW PLATFORMS AND DEVICES

New platforms and new devices will create new opportunities for cybercriminals. Security threats have long been associated with personal computers running Windows.

2.2.6 EVERYTHING PHYSICAL CAN BE DIGITAL

The written notes on a piece of paper, the report binder and even the pictures on the wall can be copied in digital format and gleaned for the tools to allow a activist-type of security violation, and increasingly this will be a problem.

2.3 ROOTKITS

In the paper focus is on one of the cyber crime which is malware known as Rootkit.

A rootkit is a type of malware that has the capability to conceal itself from the Operating System and antivirus application in a computer. A rootkit provide continuous root level (super user) access to a computer where it is installed. Rootkits, or more generically stealth malware, are software components used to hide objects inside a computer system. Generally, the objects hidden by rootkits are processes and files.

2.3.1 TYPES OF ROOTKITS

Application Level Rootkits: Application level rootkits operate inside the victim computer by changing standard application files with rootkit files, or changing the behavior of present applications with patches, injected code etc.

Kernel Level Rootkits: Kernel is the core of the Operating System and Kernel Level Rootkits are created by adding additional code or replacing portions of the core operating system, with modified code via device drivers (in Windows) or Loadable Kernel Modules (Linux). They can have a serious effect on the stability of the system if the kit's code contains bugs. Kernel rootkits are difficult to detect because they have the same privileges of the Operating System, and therefore they can intercept or subvert operating system operations.

Hardware/Firmware Rootkits: Hardware/Firmware rootkits hide itself in hardware such a network card, system BIOS etc.

Hypervisor (Virtualized) Level Rootkits: Hypervisor (Virtualized) Level Rootkits are created by exploiting hardware features such as Intel VT or AMD-V (Hardware assisted virtualization technologies). Hypervisor level rootkits hosts the target operating system as a virtual machine and therefore they can intercept all hardware calls made by the target operating system.

Boot loader Level (Bootkit) Rootkits: Boot loader Level (Bootkit) Rootkits replaces or modifies the legitimate boot loader with another one thus enabling the Boot loader Level (Bootkit) to be activated even before the operating system is started. Boot loader Level (Bootkit) Rootkits are serious threat to security because they can be used to hack the encryption keys and passwords.

3. REPORT ON PRESENT INVESTIGATION**3.1 ANALYSIS OF CYBER SECURITY TOOLS**

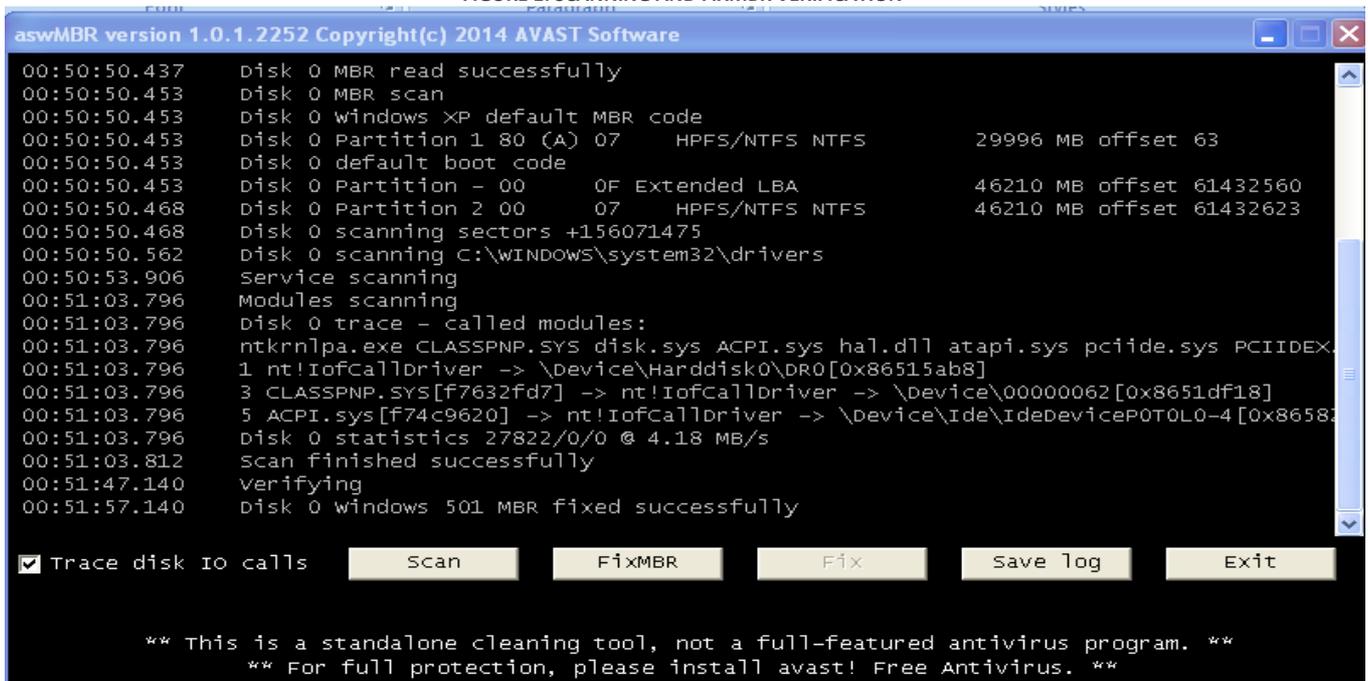
There are different tools in the field of cyber security like firewall analyzers, antivirus programs, anti malware programs, anti root kit tools, debugger tools, monitoring tools. Here in this report we mainly focus on various anti rootkit tools as it is major cyber attack which directly affects the kernel of the operating system.

3.1.1 aswMBR

aswMBR is the Rootkit scanner that scans for MBR/VBR/SRV rootkits. It can detect TDL4/3(Alureon), ZAccess, MBRRoot (Sinowal), Whistler, SST, Cidox, Pihar and other malware.

The current version of aswMBR uses Virtualization Technology to improve detection of stealth malware. It lets you scan your computer and MBR for rootkits and even fixes any issues. Removal on the other hand was not as good as some of the other tools. Normally one would have to boot to a Windows XP disc or Windows 7 recovery disc to perform this command but Avast Anti-Rootkit has a built in 'FixMBR' button that with one click will write a new Master Boot Record which is often necessary in the removal of rootkits. Avast aswMBR is a portable program for Windows. The program offers to download the latest antivirus definitions from Avast servers on first start. Those definitions are then used to scan and identify potentially dangerous files that have been discovered by the rootkit scanner. A click on the Scan button starts the scan of the system. Potentially dangerous files are highlighted in yellow and red colors on the screen. Suspicious or infected files are declared as those directly in the interface. The Fix or Fix MBR buttons are used to disinfect the system and remove the rootkit from it. The Windows Registry and local hard drives are automatically selected for the scan next to the running processes.

FIGURE 1: SCANNING AND FIXMBR VERIFICATION



FEATURES

- Quick and efficient
- Avast antivirus compatibility

3.1.2 RootRepeal

RootRepeal is an easy to use utility that detect all the rootkits in order to protect your entire system as well as prevent from crashing all the important information and data in your computer. It shows all drivers that are loaded or hidden rootkits, it will analyze the locked files and scan any drive on the system. Also, it will show all the processes that are currently running and inform you if one of them is hidden or locked as well as determined by looking for typical symptoms if the rootkits are active

FIG. 2: SSDT SCAN OF ROOTREPEAL

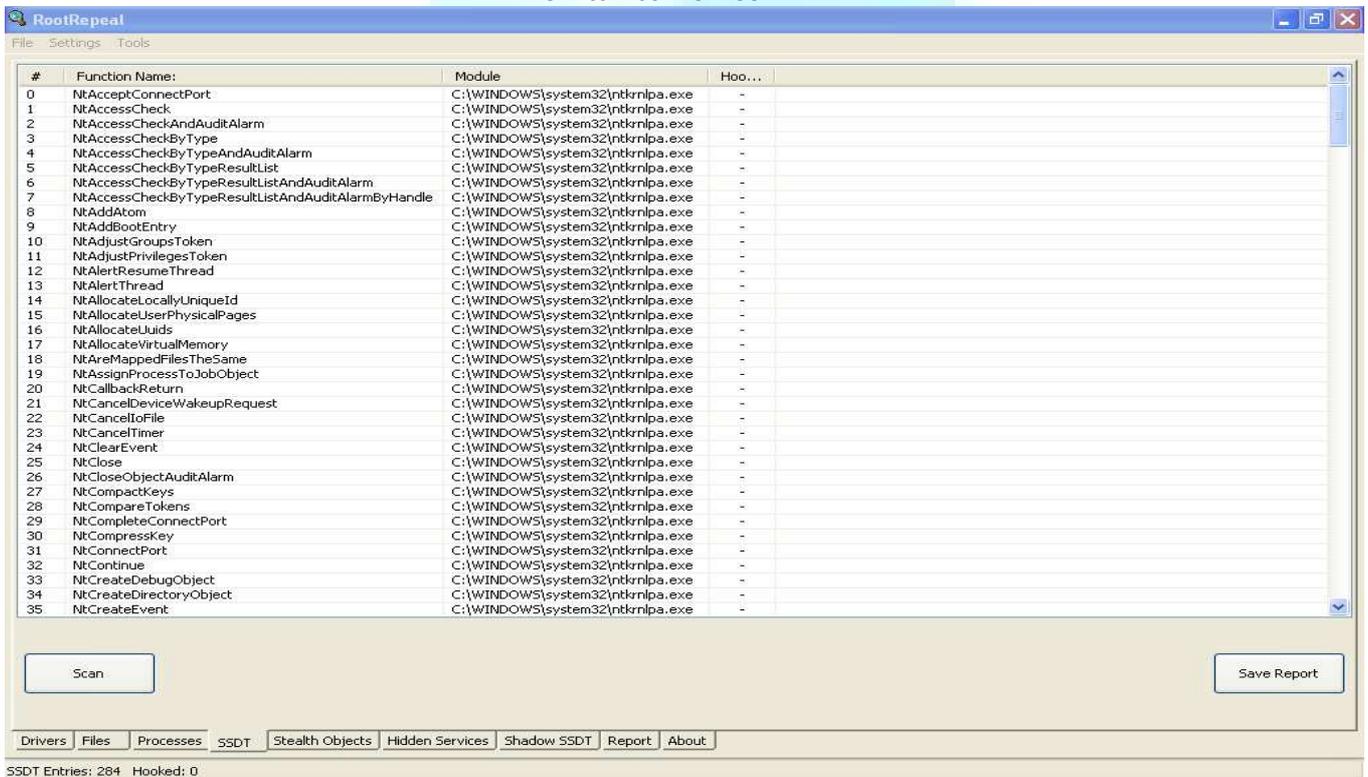
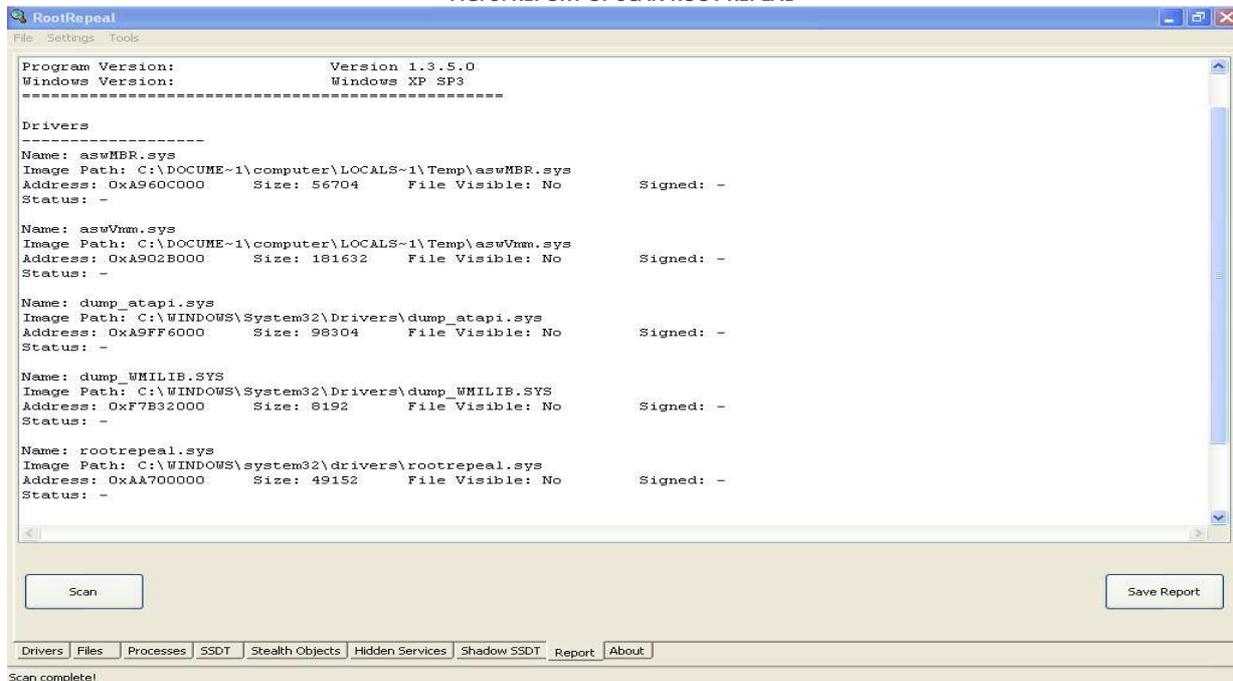


FIG. 3: REPORT OF SCAN ROOT REPEAL



FEATURES

- Easy to use
- Powerful
- Stable
- Safe
- Driver Scan
- Files Scan
- Processes Scan
- SSDT Scan
- Stealth Objects Scan
- Hidden Services Scan
- Shadow SSDT Scan

3.1.3 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 Rootkit 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.

FIG. 4: ANALYSIS OF SANITY CHECK

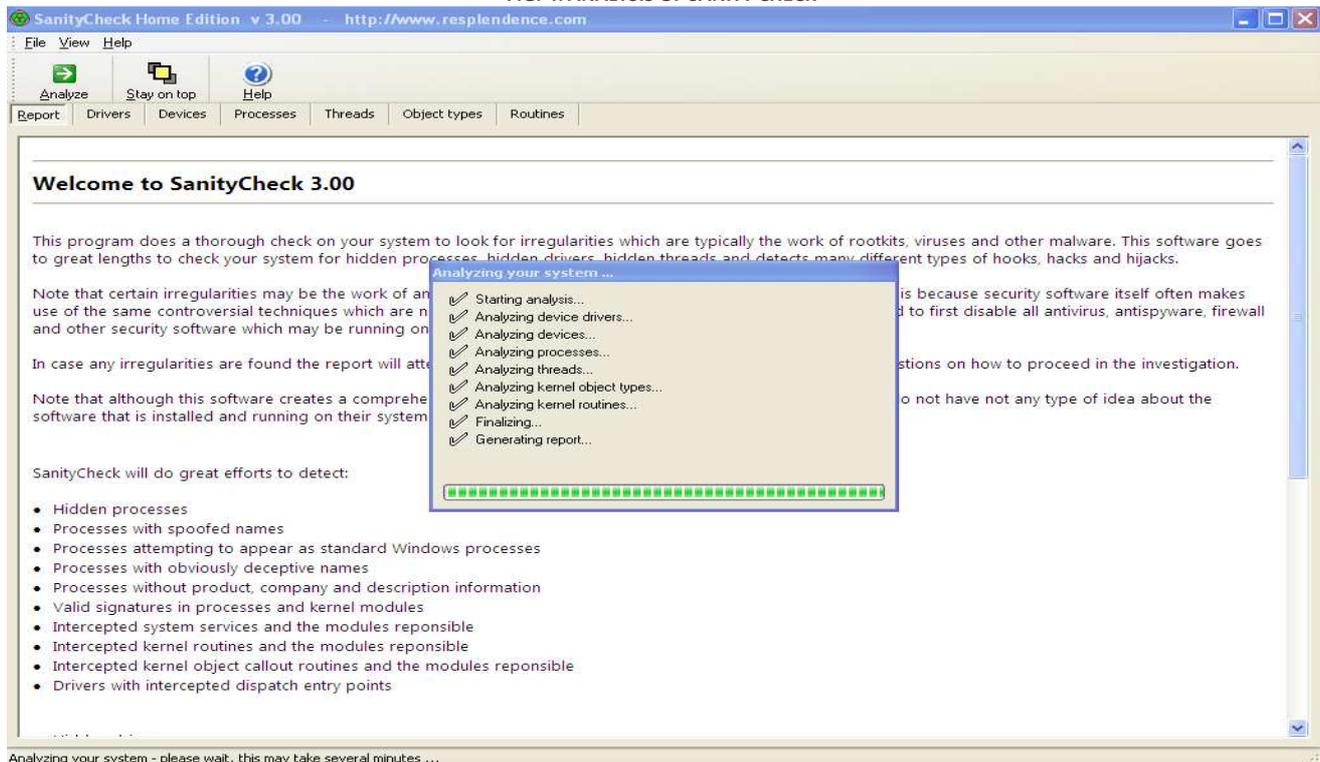
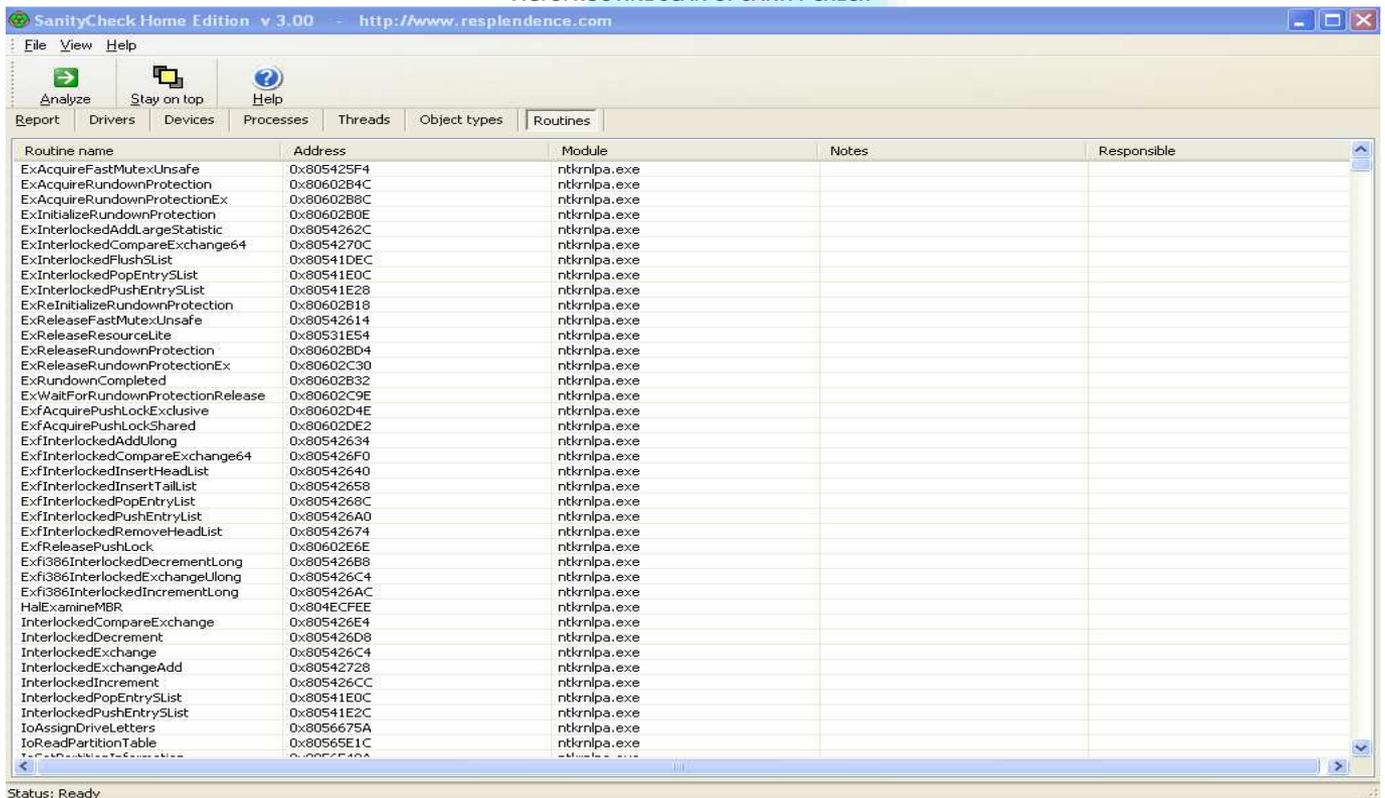


FIG. 5: ROUTINE SCAN OF SANITY CHECK



FEATURES

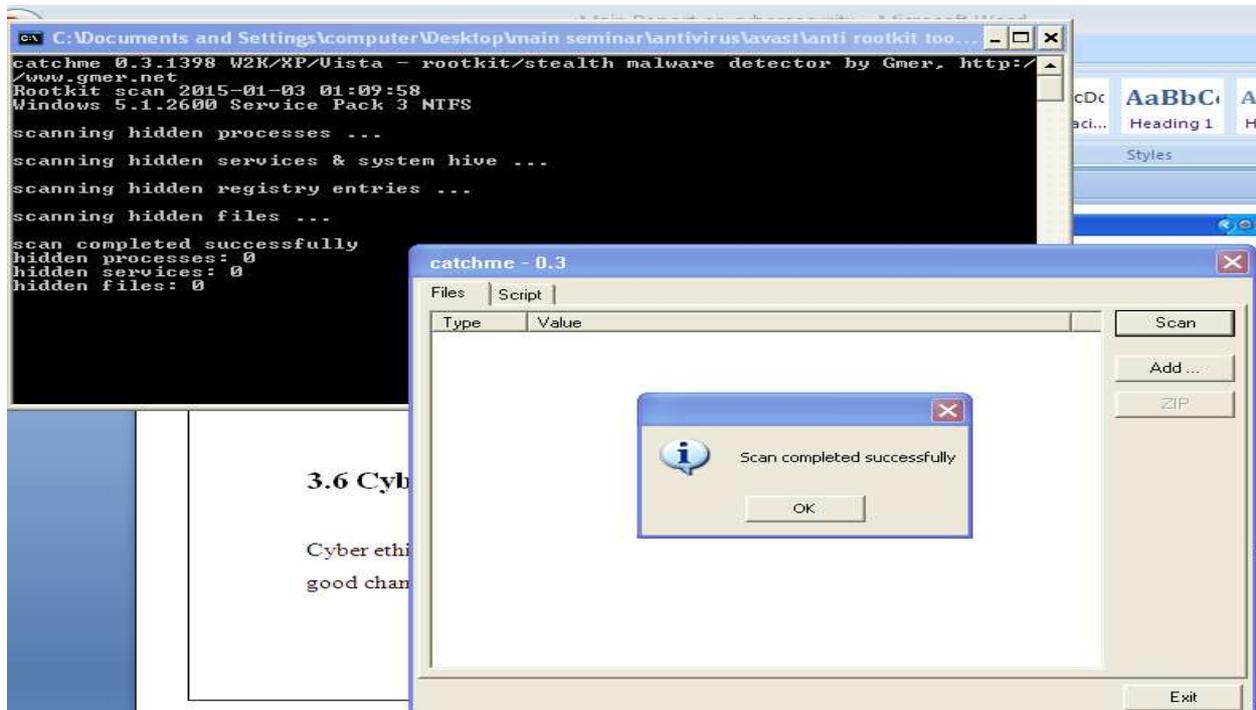
- Runs on almost all Windows versions
- Makes use of special deep inventory techniques
- Detect hidden processes
- Detect obfuscated processes
- Detect processes attempting to appear as common system processes
- Detect processes with obviously deceptive names
- Detect processes without product, company or description information
- Verify signatures and checksums of processes and kernel modules
- Detect SSDT hooks
- Detect Import Address Table hooks

- Detect kernel object callout hooks
- Detect hidden drivers
- Detect hijacked driver entry points
- Comprehensible report
- Optional expert mode

3.1.4 CATCHME

Catchme is the rootkit/stealth malware scanner that scans for hidden processes, hidden registry keys, hidden services, hidden files. Catchme can also delete, destroy and collect malicious files.

FIG. 6: SCAN OF CATCHME



FEATURES

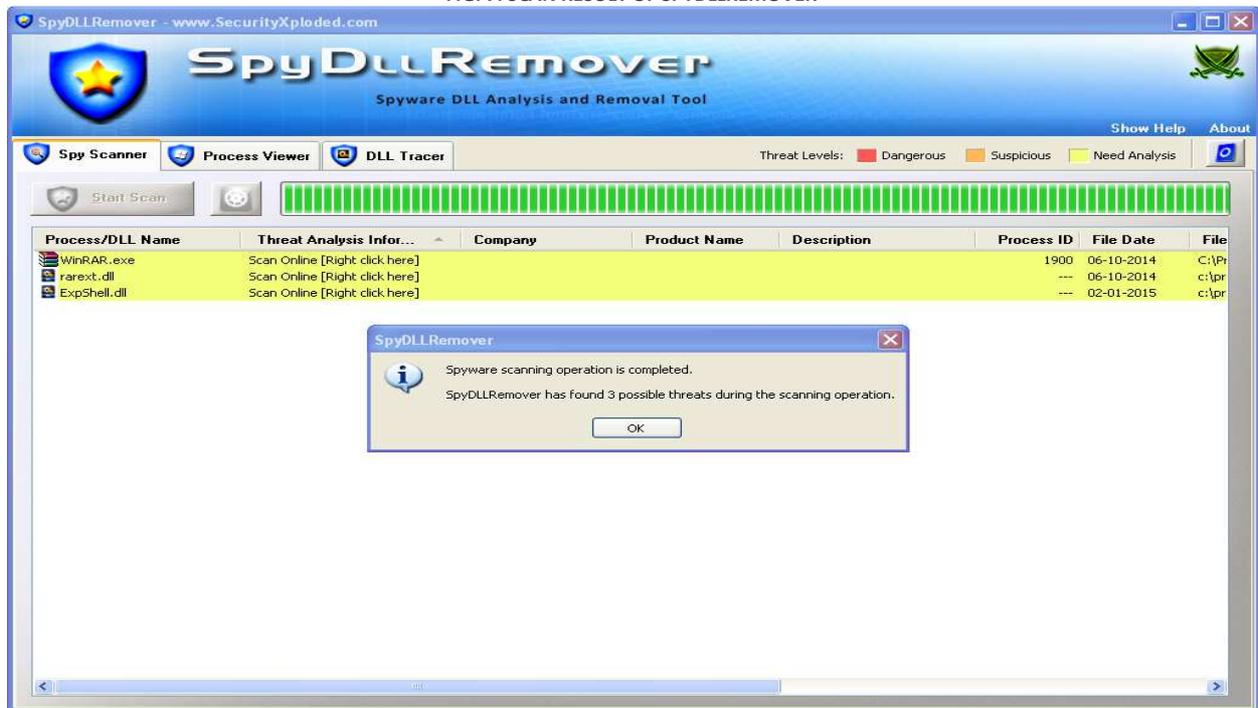
- It scans for hidden processes, hidden registry keys, hidden services, and hidden files.
- Catchme can also delete, destroy and collect malicious files.

3.1.5 SpyDllRemover

SpyDllRemover is the specialized tool for detecting Spyware & Hidden Rootkit DLLs in the System. SpyDllRemover is one of the apps that could add a new security layer to your computer, trying to detect spyware and hidden rootkits DLLs on your computer. SpyDllRemover is indeed a handy tool and does its job very fast, scanning the system and letting you act accordingly in case some suspicious files are found on your computer. It's far from being a resource hog and it runs smoothly on all Windows versions, without even asking for administrator privileges when used on Windows 7. Overall, SpyDllRemover is undoubtedly a very handy piece of software, running on low resources and providing advanced tools to detect any malicious file that may hide on your system.



FIG. 7: SCAN RESULT OF SPYDLLREMOVER



FEATURES

- Advanced spyware scanner
- Hidden rootkit detection and removal
- Unique 'Advanced DLL Ejection' technology
- Sophisticated auto-analysis
- Color-based representation
- Excellent user interface
- Advanced removal reports
- Integrated installer
- Available as a portable app

3.1.6 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.

FIG. 8: CODE HOOKS SCAN OF ROOTKITUNHOOKER

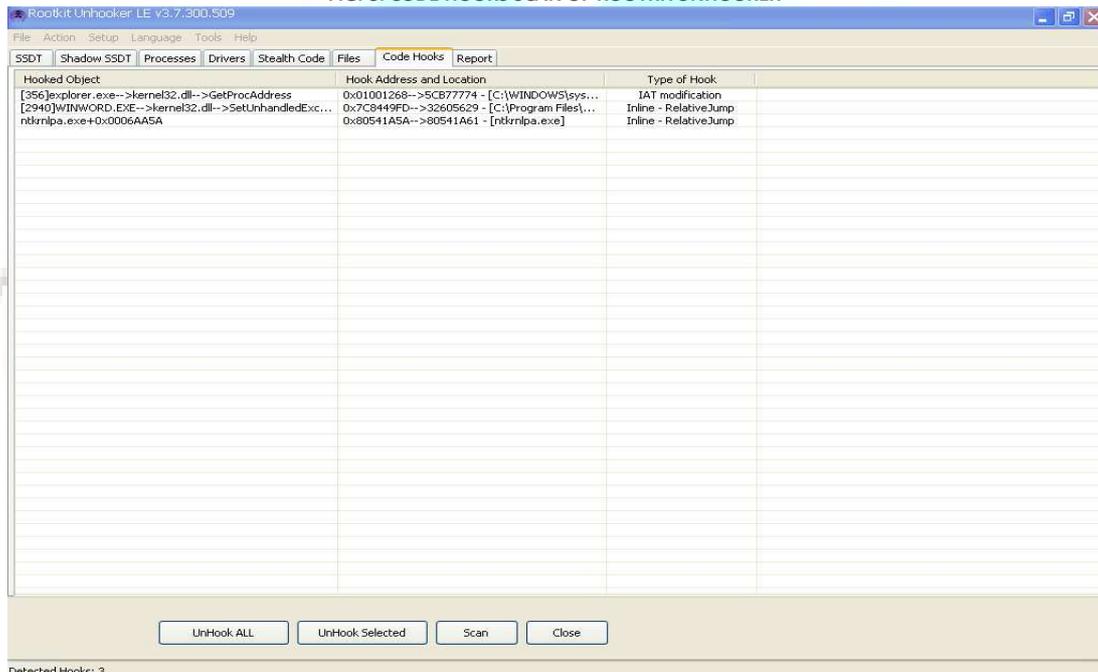
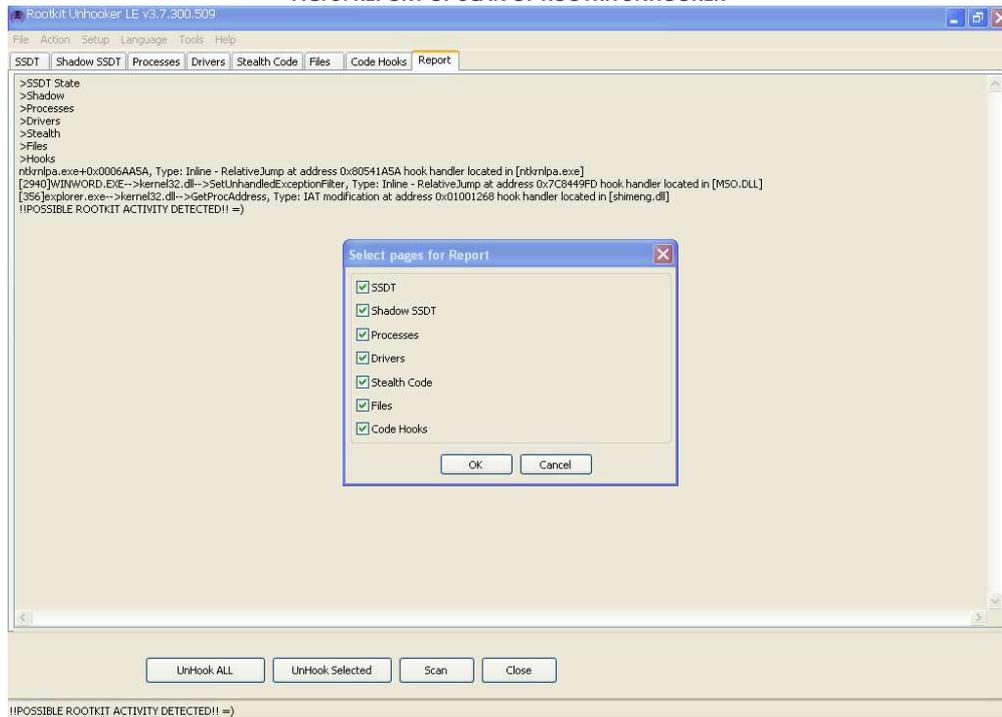


FIG. 9: REPORT OF SCAN OF ROOTKITUNHOOKER



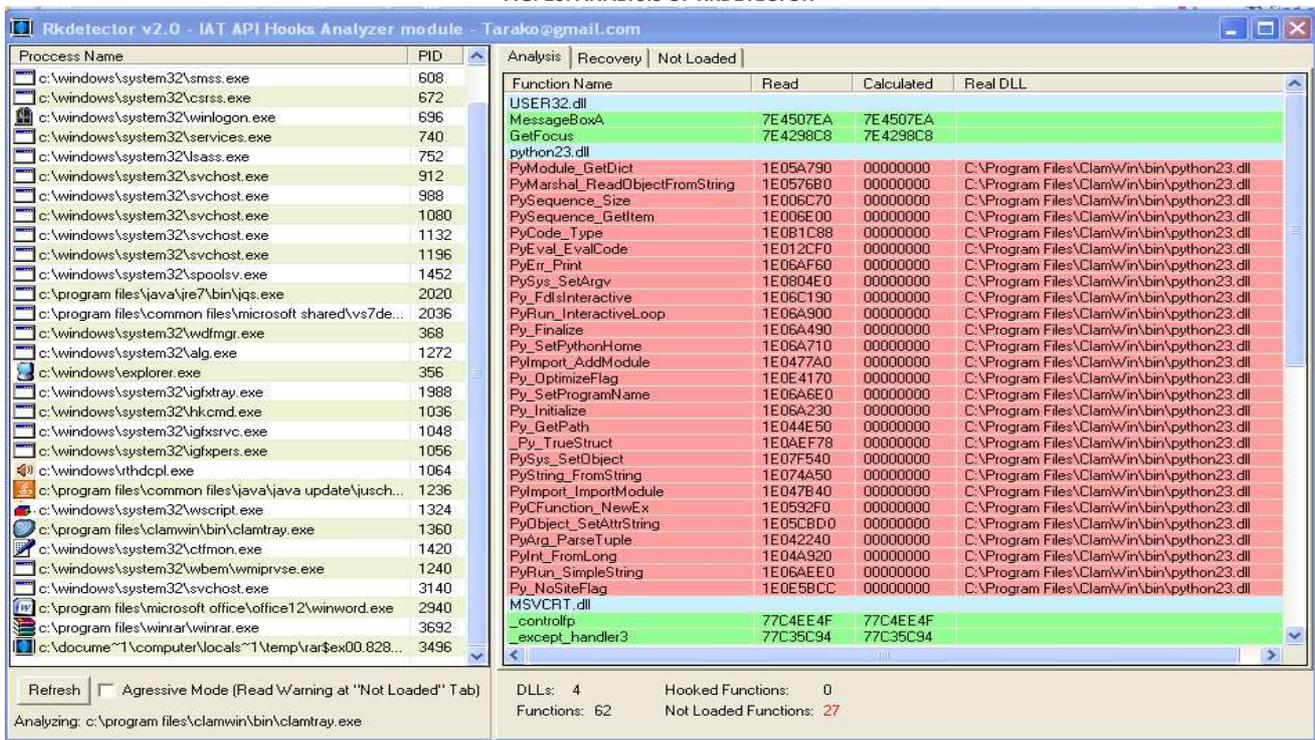
FEATURES

- It scans for SSDT, shadow SSDT, processes, drivers, stealth code, files, code hooks, and provides 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.
- It creates a report with log activity and provides options for exporting it to file for further evaluation.
- User can change the background and text colors, show only hooked functions, hide grid lines, and use standard Disk I/O.
- 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.

3.1.7 RKDETECTOR

RKDetector is a diagnostic tool that provides information about hidden process and services hooked by an NT rootkit such as Hacker Defender. After hidden handles are identified, RKDetector will try to kill those hidden tasks and rescan the service database in order to detect hidden services installed by hackers and hidden regkeys (Run, Runonce...). Another feature is that RKDetector have their own internal MD5 database with signatures about known rootkits, exploits and hacking tools that are used to identify malware running in your system. Rkdetector was the first new generation rootkit detector tool, offering same features as the most known sysinternals Rootkit revealer software

FIG. 10: ANALYSIS OF RKDETECTOR



FEATURES

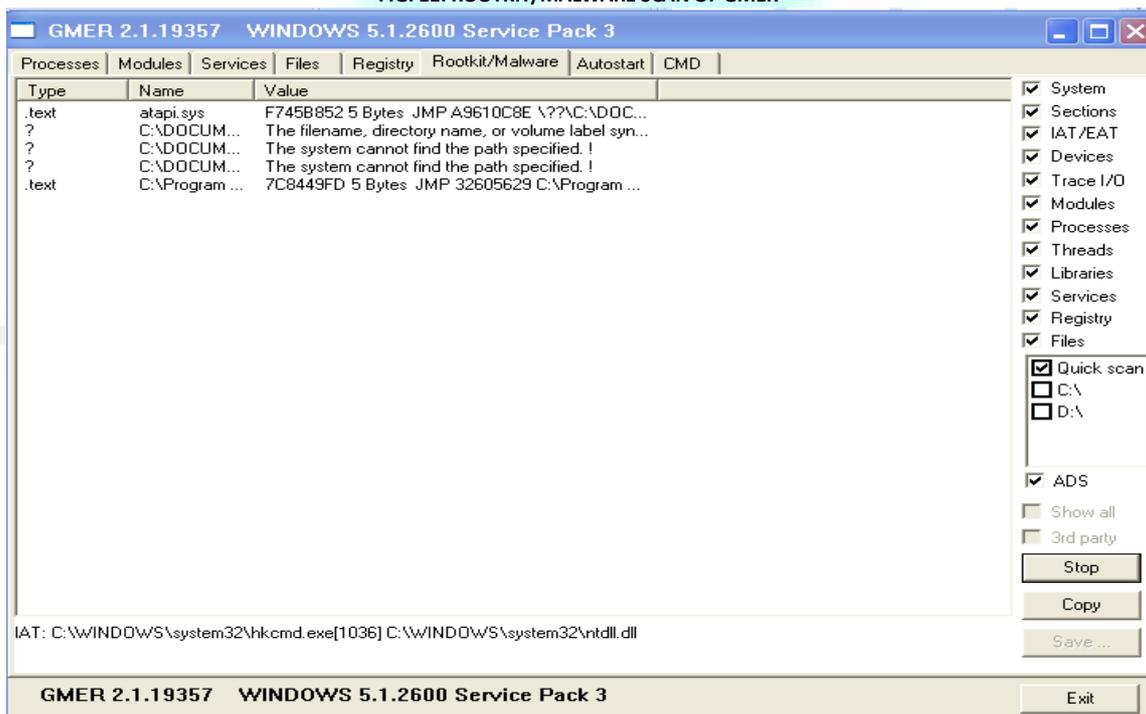
- Hidden file detection.
- Hidden registry keys detection.
- ADS (Alternate Data Streams) detection.
- Rootkit deletion by wiping the used binary files and rebooting the system.
- Data recovery for both FAT32 and NTFS file system.
- File system browser.

3.1.8 GMER

GMER is an application that detects and removes root kits.

It scans for hidden processes, hidden threads, hidden modules, hidden services, hidden files, and hidden disk sectors (MBR), hidden Alternate Data Streams, hidden registry keys, drivers hooking SSDT, drivers hooking IDT, drivers hooking IRP calls, inline hooks. GMER also allows monitoring the following system functions: processes creating, driver's load, libraries loading, files functions, registry entries, TCP or IP connections.

FIG. 11: ROOTKIT/MALWARE SCAN OF GMER



FEATURES

- Intuitive environment

- Scan the computer for malware
- Monitor processes and TCP/IP connections
- Evaluation and conclusion

3.1.9 Vba32 AntiRootkit

Vba32 AntiRootkit is designed to analyze the computer for the anomalies that arise due to the presence of malware in the system. Due to this, you will be able to detect and neutralize both the known and unknown viruses that are present in your system in active state. This program is a good assistant in the work of a specialist struggling with complicated infections.

FIG. 12: KERNEL MODULE SCAN OF VBA32



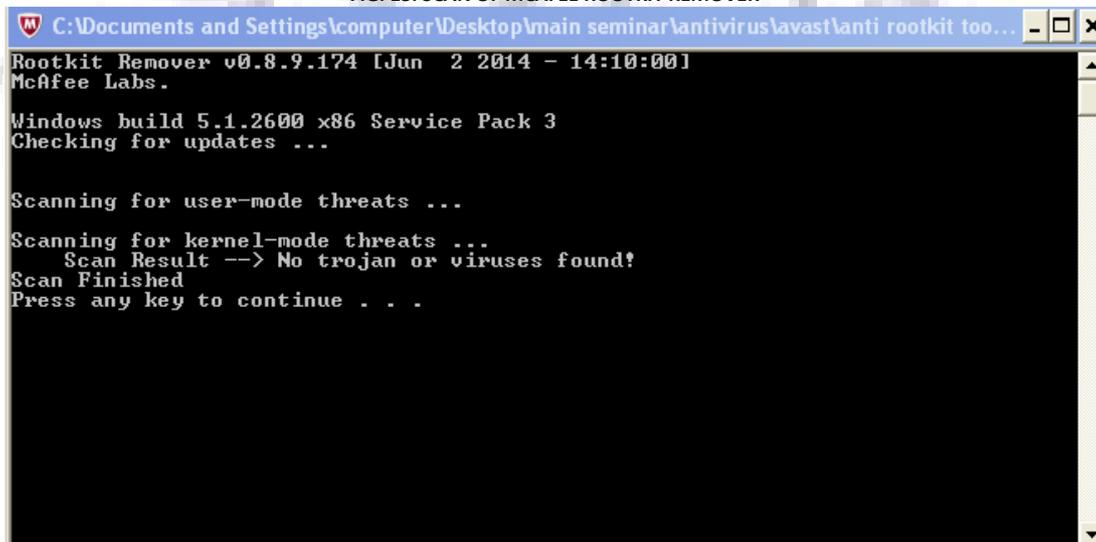
FEATURES

- Free of charge
- Does not require installation
- Can be used with any antivirus software installed on your computer
- Uses a unique feature of the detection of "clean" files
- Can be used in several modes
- Supports the maintenance of a system status report in html format
- Treatment of the system may be done using a scripting language
- Supports Windows 7 XP VISTA
- Help files in Russian and English languages
- Part of Vba32 Personal and Vba32 Check

3.1.10 McAfee Rootkit Remover

McAfee Rootkit Remover is a 538kb standalone freeware 'command-prompt-look-alike' tool that can be used to detect and remove complex rootkits and associated malware. Currently it can detect and remove ZeroAccess, Necurs and TDSS family of rootkits. McAfee Labs plans to add coverage for more rootkit families in future versions of the tool.

FIG. 13: SCAN OF MCAFEE ROOTKIT REMOVER



FEATURES

- Scans, detects and removes rootkits
- Works alongside your existing antivirus
- Open source

4. COMPARATIVE ANALYSIS

On the basis of comparison of the tools following is the table:

TABLE 1

Anti-Rootkit tools	Version	Active	Memory Scanning	Register Scan	Driver Scan	SSDT Scan	Scan Time(min)	Hooking detection	Removal	Best Features
aswMBR	1.0.1.2252	Yes	Yes	No	No	No	0.23	No	yes	Memory Scan
RootRepeal	1.3.5.0	Yes	Yes	No	Yes	Yes	0.50	No	Yes	All Scans
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
RKDetector	2.0	Yes	No	No	No	No	1.00	No	Yes	Hooking
GMER	2.1.19357	Yes	Yes	Yes	Yes	Yes	9.05	Yes	Yes	Removal
Vba32 AntiRootkit	3.12.5.4	Yes	Yes	No	No	No	12.05	Yes	No	Hooking
McAfee Rootkit Remover	0.8.9.174	Yes	Yes	No	No	No	1.00	No	Yes	Removal

As per the above table we identified the best tools to be used for detecting rootkits. They will fall under two categories:

FOR NAÏVE USERS

For the beginners or naïve users who does not have any knowledge related to hooking and various types of scan such as SSDT, SPYDLLRemover and GMER are the best tools to work with as they does not include complex terms like hooking and SSDT kernel modules which are not user friendly and user is easily able to view processes, modules, files in the system.

FOR PROFESSIONALS

For the 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.

5. CONCLUSIONS

Cyber security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. In the report various anti Rootkit tools are studied and analyzed on the basis of different parameters and reached to the conclusion that for the beginners or naïve users who does not have any knowledge related to hooking and various types of scan such as SSDT, 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. By focusing on dynamic behavior, it is likely that an ARK developer will keep up with the latest threats and provide better overall security.

REFERENCES

1. Anoop Kumar Verma Aman Kumar Sharma "Cyber Security Issues and Recommendations" Volume 4, Issue 4, April 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering
2. Ateeq Ahmad ,Int.J.Computer Technology & Applications,Vol 3 (2), 750-752 ISSN:2229-6093 "Type of Security Threats and It's Prevention"
3. Azeez Nureni Ayofe, Barry Irwin "CYBER SECURITY: CHALLENGES AND THE WAY FORWARD" Computer Science and Telecommunications 2010|No.6(29) ISSN 1512-1232 56
4. Dan Boneh, John C. Mitchell Senior Member IEEE, , Steven M. Bellovin, Susan Landau, Member IEEE, and Michael E. Lesk, Carl Landwehr Member IEEE "Privacy and Cybersecurity: The Next 100 Years",
5. Dr. Ibikunle Frank "APPROACH TO CYBER SECURITY ISSUES IN NIGERIA: CHALLENGES AND SOLUTION" *International Journal of Cognitive Research in science, engineering and education Vol. 1, No.1, 2013.*
6. G.Nikhita Reddy1 G.J.Ugander Reddy2 "A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies" International Journal of Engineering and Technology Volume 4 No. 1, January, 2014 ISSN: 2049-3444 © 2014 – IJET Publications UK. All rights reserved. 48
7. Hussain A.H. Awad and Fadi M. Battah "Enhancing Information Systems Security in Educational Organizations in KSA through proposing security model" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011 ISSN (Online): 1694-0814
8. Ravi Sharma International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 "Study of Latest Emerging Trends on Cyber Security and its challenges to Society"
9. Saeed S. Basamh, Hani A. Qudaih, Jamaludin Bin Ibrahim "An Overview on Cyber Security Awareness in Muslim Countries" Volume 4 No. 1, January 2014 ISSN 2223-4985 International Journal of Information and Communication Technology Research

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail infoijrcm@gmail.com for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals

