Comparative Performance Study of Antimalware Tools on TDL-4 Rootkit

S.O. SUBAIRU, A.O. ISAH, J.K. ALHASSAN
Cyber Security Science, Federal University of Technology, Minna, Nigeria
lanrezubair@yahoo.com

Abstract

Researchers and security expert has been vigorously on the study of malwares, great interest has been drawn to rootkits. Rootkits are a notably dangerously type of malware with the ability to cover their presence on the compromised host operating system and allow malicious recreation via spyware and other more obvious types of malware undetected. Once a rootkit gained access to a system, it can be very tough to track and do away with them. In this research, various antimalware tools were critically analyzed and studied to ascertain their effectiveness in combating a deadly malware called tdl-4. An analytical model developed was used to obtain all experimental results and findings which are documented for further work.

Index terms: Rootkit, TDL-4, Antimalware, Malware, Detector

References:

[1]. Chris, R. (2006). Inside Windows Rootkits. Vigilantmind Inc. Retrieved from http://repo.hackerzvoice.net/depot_madchat/vxdevl/library/Inside%20Windows%20Rootkits.pdf, 1-18.

[2]. Probert, D. (2008). Architecture of the Windows kernel. Microsoft Corporation. Retrieved from http://www.cs.fsu.edu/~zwang/files/cop4610/Spring2015/windows.pdf

[3]. Ashwin, R. (2008, September 2). Detecting kernel rootkits. Master's Thesis Proposal Dartmouth Computer Science Technical Report TR2008-627. Retrieved fromhttp://www.ists.dartmouth.edu/library/409.pdf, 2-5.

[4]. McAfee Labs Threats Report (November, 2014). Retrieved from http://www.mcafee.com/ca/resources/reports/rp-quarterly-threat-q3-2014.pdf

[5]. Microsoft Security Intelligence Report Volume 17 | January through June, (2014). Retrieved from http://www.emc.com/collateral/guide/11455-customer-faq.pdf.

[6]. Kaspersky labs

[7]. Rehman, R., Hazarika, D., Chetia, G. (2011). Malware Threats and Mitigation Strategies: A Survey. Journal of Theoretical and Applied Information Technology. Vol. 29 No.2 ISSN: 1992-8645, 69-72.

[8]. Rehman, R., Hazarika, D., Chetia, G. (2011). Malware Threats and Mitigation Strategies: A Survey. Journal of Theoretical and Applied Information Technology. Vol. 29 No.2 ISSN: 1992-8645, 69-72.

[9]. Bits. (2011). Malware Risks and Mitigation Report. Retrieved from http://www.nist.gov/itl/upload/BITS-Malware-Report-Jun2011.pdf

[10]. You, I., Yim, K. (2010). Malware Obfuscation Techniques: A Brief Survey. International Conference on Broadband, Wireless Computing, Communication and Applications, 297-300.