A Study on Registry-hidden Rootkit Detection Mechanism in Cloud Service Environments

曾淑婷、曹偉駿

E-mail: 387218@mail.dyu.edu.tw

ABSTRACT

In considerations of international big factories such as Google, Microsoft, Amazon, IBM, Dell, Sun, HP and so on entering the territory of cloud computing, application of cloud and virtualization technology has led to better desktop software using experiences in the Personal Computer area. As a result, the malware hiding in cloud virtual machine, particularly spywares and rootkits, have become the key preventive objects in the computer security territory. Regarding malware development, possessing certain degree of hiding function has been becoming a trend. Under Microsoft Windows systems, the existence and operation of malwares cannot be independent of related information registry in the system. Additionally, malwares often hide in the registry, so it is difficult to delete them completely. Consequently, how to effectively detect rootkits that hide in the registry has been becoming especially important. Although there are famous detection tools that can detect rootkits that hide in the registry, they often fail to detect new types of rootkits. In order to detect rootkits that hide in operating systems based on tampering registry file, this research analyzes the rootkit hiding technology in registry and related rootkit detection technologies. After analyzing the registry file format and operation controlling flow, this research designs a new type of registry based rootkit hiding technology, and then develops rootkit detection mechanism based on the experiences of designing the new type of rootkit. By the flow of virtualizing registry and registry key value flow at bottom tier in the Win 32 system, the actually valid registry key can be obtained, which can effectively detect hinding rootkits in cloud environments.

Keywords : Cloud services、Malware、Rootkit、Registry Virtualization、Windows operating systems

Table of Contents

REFERENCES

[1] S. Gold, “Protecting the cloud: attack vectors and other exploits,” Network Security, no. 12, pp. 10-12, 2010.

[2] D. Molina, M. Zimmerman, G. Roberts, M. Eaddie and G. Peterson, “Timely Rootkit Detection During Live Response,” Proceedings of IFIP International Federation for Information Processing, vol. 285, pp. 139-148, 2008.

[3] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali, “Cloud computing: Distributed Internet computing for IT and scientific research,” Internet Computing, IEEE, vol. 13, no. 5, pp. 10-13, 2009.

[4] 任雲韜, 李毅超, 曹躍, “基於註冊表Hive檔案的惡意程序隱藏檢測方法,” 電子科技大學學報, vol. 36, no. 3, pp. 621-624, 2007.

[5] 李冠儀, “以Windows Registry 為基礎之使用者行為異常偵測方法,” 中央大學資訊管理學系學位論文, pp. 1-54, 2006.

[6] 李偉斌, 王華勇, 羅平, “通過註冊表監控實現木馬檢測,” 計算機工程與設計, vol. 27, no. 12, pp. 2220-2222, 2006.

[7] 李錦, “Rookit 木馬的隱藏機理與檢測技術剖析,” 遼寧師範大學學報: 自然科學版, vol. 6, no. 2, pp. 176-178, 2009.

[8] D. J. Farmer,“ A Windows Registry Quick- Reference for the Everyday Examiner, ”, pp. 1-14, 2007.
[9] 楊彥, 黃皓,“ Windows Rootkit 隱藏技術研究, ” 計算機工程, vol. 34, no. 12, pp. 152-156, 2008.
[10] 劉?, 張家旺,“ Rootkit 木馬隱藏技術分析與檢測技術綜述, ” 資訊安全與通信保密, no. 11, pp. 61-65, 2010.
[11] 陳啟川,“ 惡意程式的隱形鬥蓬－Rootkit, ” Internet: http://www.runpc.com.tw/content/content.aspx? id=103730 [May 18, 2013].
[12] 蘇建郡, 方鵬喜,“ Snort 於網站管理之應用, ” 第三屆離島資訊技術與應用研討會, pp. 334-340, 2003.
[13] 申文迪, 羅克露,“ 輕量級虛擬機系統資源保護層研究, ” 計算機工程, vol. 36, no. 14, pp. 127-128, 2010.
[14] 王繼偉, 王嘉偉， 許家維， 謝續平,“ 基於虛擬機器外部觀察與映像檔比對的惡意程式分析, ” 第二十屆資訊安全會議, pp. 69-74, 2010.
[15] M. Christodorescu and S. Jha,“ Testing Malware Detectors, ” Proceedings of the ACM SIGSOFT international symposium on Software testing and analysis, vol. 29, no. 4, pp. 34-44, 2004.
[16] E. Kumar,“ Battle with the Unseen- understanding Rootkits on Windows, ” Proceedings of International Conference on the 9th (AVAR), pp.82-97, 2006.
[17] 張登銀, 高德華, 李鵬,“ 一種新的註冊表隱藏Rootkit 檢測方案, ” 江蘇大學學報: 自然科學版, vol. 31, no. 3, pp. 328-333, 2010.
[18] W. J. Tsaur, S. R. Wu and J. X. Wu,“ Windows Rootkits Stealth Technologies in Cloud Computing, ” Proceedings of Cryptology and Information Security Conference (CISC), Taiwan, 2012.
[19] J. Zhang, S. Liu, J. Peng and A. Guan ,“ Techniques of User-mode Detecting System Service Descriptor Table, ” Proceedings of the 13th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 96-101, 2009.
[20] R. James, Butler II,“ Detecting Compromises of Core Subsystems and Kernel Functions in Windows NT/2000/XP, ” M.S. thesis, University of Maryland, Baltimore County, 2002.
[21] D. Fu, S. Zhou, and C. Cao,“ A Windows Rootkit Detection Method Based on Cross-view, ” Proceedings of International Conference on E-product E-service and E-entertainment (ICEEE), pp. 1-3, 2010.
[22] A. Pauna,“ Improved self Adaptive Honeypots Capable of Detecting Rootkit Malware, ” Proceedings of the 9th International Conference on Communications (COMM), pp. 281-284, 2012.
[23] Z. Lu, G. Gan and J. Jiang,“ Analysis and research on hidden technology based on kernel-level Rootkit process, ” Proceedings of International Conference on Internet Technology and Applications (iTAP), pp. 1-4, 2011.
[24] W. J. Tsaur and Y. C. Chen,“ Exploring Rootkit Detectors Vulnerabilities Using a New Windows Hidden Driver Based Rootkit, ” Proceedings of International Conference on Social Computing (SocialCom), IEEE, pp. 842-848, 2010.
[25] W. Q. Wang, Z. G. Wu and S. X. Li,“ Perfect Solution of Windows Registry Concealment Detection, ” Computer Engineering, vol. 38, no. 14, pp. 106-108, 2012.