雲端服務環境之程序隱藏型Rootkit偵測機制研究

杞承樺、曹偉駿

E-mail: 387178@mail.dyu.edu.tw

摘 要

雲端服務發展日趨成熟，其雲端之優點也提供了駭客便利的途徑，使其發展出複雜而細膩的攻擊手法。而這些手法不難發現皆有Rootkit的蹤跡，其中又以木馬型Rootkit危害最為嚴重。這種結合Rootkit隱藏的技術中，以移除雙向鏈結與使用系統服務表最難以偵測，因此常常令使用者不自覺的下載，並開啟檔案使其逐漸擴散於鄰近的系統與網路。且潛伏等待時機發動攻擊，其攻擊的發起方式是由遠端伺服器控制，傳達指令後透過偽裝成正常程序或執行緒的木馬，再經由網路傳輸回送給攻擊者，以竊取重要資料。這種手法一般又稱之為 APT (Advanced Persistent Threat)，其對於雲端環境有強大的威脅。雖然有知名偵測軟體亦能偵測出隱藏於程序型的Rootkit，但面對混合型Rootkit時，卻常常無法有效偵測。 因此，本研究將於雲端作業系統上開發出 Process-hidden Rootkit 偵測機制，目的在於能夠有效偵測出利用移除雙向鏈結與使用系統服務表做 Rootkit 隱藏的混合型木馬程式，進而達到防範雲端之 APT 攻擊手法的一環，並可協助防毒軟體與雲端系統服務商，建構出完整防禦Rootkit攻擊機制。

關鍵詞 : Rootkit、木馬程式、雲端服務、Windows作業系統、進階持續性攻擊

目錄

參考文獻

[1] Trend Labs, “ 2013資安關鍵十大預測:多元平台挑戰數位生活安全 , APT攻擊和雲端隱私成為企業雙重隱憂 ”, Internet: http://blog.trendmicro.com.tw/?p=3883 [Jan. 15, 2013] [2] ?良斌, “ ??木?程序??技?, ” Journal of nantongvocational & Techcicalshippingcollege, pp. 56-58, Mar, 2005.

[3] 沈經, “ 駭客指控德國政府使用木馬程式監控網路通訊 ”, Internet: http://www.ithome.com.tw/itadm/article.php?c=70192 [May.1, 2013] [4]陳啟川, “ 惡意程式的隱形斗蓬－Rootkit ”, Internet: http://www.runpc.com.tw/content/content.aspx?id=103730 [May.15, 2013] [5]董元昕, “ 雲端運算的安全議題 ”, Internet: http://newsletter.certcc.org.tw/epaper/201111/report3_1.html [May.1, 2013] [6] A. K Sood and R. J Enbody, “ Targeted Cyber Attacks: A Superset of Advanced Persistent Threats, ” IEEE Security & Privacy, p. 1, July 2012.

[7] B. Blunden, The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, Jones & Bartlett Learning, April 2012.

[8] D. A. D. Zovi, “ Hardware Virtualization Rootkits, ” Available: http://www.theta44.org/software/HVM_Rootkits_ddz_bhusa-06.pdf [May.15,2013] [9] E. Messmer, “ Intel/McAfee: What's the Future of Security?, ” Internet: http://www.computerworld.com.au/article/429666/intel_mcafee_what_future_security_/?fp=4&fpid=804870237 [May.15,2013] [10] E. Florio and K. Kasslin, “ Your Computer is Now Stoned (Again!): the Rise of MBR Rootkits, ” Technical Report of Symantec, 2009.

[11] E. U. Kumar “ User-mode Memory Scanning on 32-bit & 64-bit Windows, ” Journal in Computer Virology, vol. 6, no. 2, pp. 123-141, May 2010.

[12] F. Li, A. Lai and D. Ddl, “ Evidence of Advanced Persistent Threat: A Case Study of Malware for Political Espionage, ” 6th International Conference on Malicious and Unwanted Software (MALWARE), pp. 102-109, Oct 2011.
[13] F. Wecherowski, “ A Real SMM Rootkit: Reversing and Hooking BIOS SMI Handlers, ” Phrack Magazine, vol. 13, no. 66, 2009.
[14] G. Bonfa, “ Step-by-step Reverse Engineering Malware: ZeroAccess / Max++ / Smiscer Crimeware Rootkit ” , Internet: http://resources.infosecinstitute.com/step-by-step-tutorial-on-reverse-engineering-malware-the-zeroaccessmaxsmiscer-crimeware-rootkit/ [May.20, 2013] [15] G. Hoglund and J. Butler, “ Rootkits: Subverting the Windows Kernel. Addison Wesley, ” Boston, 2006.
[16] N. Villeneuve, “ The Trends in Targeted Attacks of 2012 ” , Internet: http://blog.trendmicro.com/trendlabs-security-intelligence/the-trends-in-targeted-attacks-of-2012/ [May.29, 2013] [17] H. Gao, Q. Li, Z. Yu, W. Wei and Z. Li, “ Research on the Working Mechanism of Bootkit, ” Proceedings of 8th International Conference on Information Science and Digital Content Technology (ICIDT), pp. 476-479, June 2012.
[18] I. Seo, I. Kim, J. Yoon and J. Ryou, “ Detection of Unknown Malicious Codes Based on Group File Characteristics, ” Proceedings of the 5th International Conference on Ubiquitous Information Technologies and Applications (CUTE), pp. 1-6, Dec 2010.
[19] J. Zhang, S. Liu, J. Peng and A. Guan, “ Techniques of User-mode Detecting System Service Descriptor Table, ” Proceedings of 13th International Conference on Computer Supported Cooperative Work in Design (CSCWD 2009), pp. 96-101, April 2009.
[20] K. L. Steven, “ Trusted Platform Module Basics: Using TPM in Embedded Systems, ” Technology & Engineering, 2006.
[21] L. Zeyong, G. Gang and J. Jun, “ Analysis and Research on Hidden Technology Based on Kernel-Level Rootkit Process, ” Proceedings of 2011 International Conference on Internet Technology and Applications (iTAP), pp. 1-4, Aug. 2011.
[22] M. Laureano, C. Maziero and E. Jamhour, “ Protecting Host-based Intrusion Detectors Through Virtual Machines, ” Computer Networks, 2007 [23] P. Bravo and D. F. Garcia, “ Rootkits Survey A Concealment Story, ” Architecture.
[24] R. S. Montero, “ Building IaaS Clouds and the Art of Virtual Machine Management, ” Proceedings of International Conference on High Performance Computing and Simulation (HPCS), pp. 573-573, 2012.
[25] TDL4 rebooted, http://blog.eset.com/2011/10/18/tdl4-rebooted [May 27, 2013] [26] W. J. Tsaur and Y. C. Chen, “ Exploring Rootkit Detectors' Vulnerabilities Using a New Windows Hidden Driver Based Rootkit, ” Proceedings of IEEE Second International Conference on Social Computing (SocialCom), pp. 842-848, Aug. 2010.
[27] 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.
[28] Waggener Edstrom STB Private Cloud Team, “ Microsoft on Cloud Computing ” , Internet: http://www.microsoft.com/en-us/news/presskits/cloud/default.aspx [May.5, 2013] [29] X. Li, Y. Wen, M. Huang and Q. Liu, “ An Overview of Bootkit Attacking Approaches, ” Proceedings of Seventh International Conference on Mobile Ad-hoc and Sensor Networks (MSN), pp. 428-431, Dec, 2011.
[30] Y. Wang, D. Gu, W. Li, J. Li and M. Wen, “ Virus Analysis on IDT Hooks of Rootkits Trojan, ” Proceedings of International Symposium on Information Engineering and Electronic Commerce (IEEC'09), pp. 224-228, May 2009.
[31] Y. Huang, “ Windows Rootkits Detection Technologies for Service Platforms in Cloud Computing, ” Master Thesis, Da-Yeh University, 2011.