

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

杞承樺、曹偉駿

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

## ABSTRACT

Since cloud service's development becomes mature, the advantages of cloud service also give hackers easy way to create complicated and exquisite techniques of attacks. Rootkit always be used in these techniques and exquisite one is Trojan-based rootkits. In this rootkit-combined technique, "removing double linked list" and "using system services" are very hard to detect, which is why it always let users download data unconsciously and spread to contiguous systems and networks gradually by opening files. The way of attack is hiding to wait opportunities, and is controlled by a remote server. And pretends to be proper procedures or threads after conveying instructions, and steals important information by network transfer back to the attacker. The above-mentioned trick is called the technique of "APT" (Advanced Persistent Threat) which becomes a big menace to cloud services. Although famous anti-virus software can detect process-hidden rootkits, they still cannot work when confronting to mixed rootkits. Therefore, this research will develop a mechanism for detecting process-hidden rootkits in cloud operating systems to avoid APT attacks on clouds, which can effectively detect mixed rootkits of "removing double linked list" and "using system services". Moreover, the proposed mechanism can help anti-virus software and cloud systems service provider develop a complete protection mechanism against rootkit attacks.

Keywords : Rootkit、Trojans、Cloud Services、Windows OS、Advanced Persistent Threat

## Table of Contents

中文摘要	iii	英文摘要	iii
iv 誌謝辭	vi	內容目錄	ii
表目錄	iii	圖目錄	iv
第一章 緒論	1	第一節 研究背景	1
第二節 研究動機與目的	2	第三節 研究限制	2
3 第四節 研究流程	3	第五節 論文架構	5
第二章 文獻探討	6	第一節 雲端服務環境安全技術	6
基於程序的Rootkit隱藏技術	10	第三節 基於程序的Rootkit偵測技術	21
基於Windows雲端之Process-hidden Rootkit偵測機制	31	第三章 建構基於Windows雲端之Process-hidden Rootkit偵測機制	31
Rootkit偵測架構	31	第一節 Rootkit偵測架構	31
偵測機制	34	第二節 偵測機制	34
機制模組設計	36	第三節 機制模組設計	36
第四章 實驗設計與分析	43	第一節 實驗環境	43
第一節 實驗環境	43	第二節 偵測機制測試	43
第二節 偵測機制測試	43	第三節 偵測能力與分析	47
第三節 偵測能力與分析	47	第五章 結論與未來展望	53
第五章 結論與未來展望	53	參考文獻	54

## REFERENCES

- [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 & Techicalshippingcollege, 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, "惡意程式的隱形斗篷 - 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](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](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](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/tld4-rebooted> [May 27, 2013]
- [26] W. J. Tsauro 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. Tsauro, 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.