

強化雲端運算環境之Rootkit惡意軟體防護技術

賴瑋倫、曹偉駿

E-mail: 382058@mail.dyu.edu.tw

摘要

隨著雲端運算日漸普及，安全議題亦隨之而來，雲端虛擬機器服務平台之安全防護將不容忽視。在Rootkit惡意軟體防護的議題中，由於各種新型Kernel Mode Rootkit對系統核心之破壞甚巨，甚至連號稱永不被病毒入侵的Apple MAC系統也淪陷，因而Rootkit受到全世界非常廣泛的注意。許多以Microsoft Windows為目標之Rootkit紛紛被製造出來，其破壞的系統也由單機延伸至雲端虛擬機器上，至於目前能偵防Windows Rootkits的各種技術中，儘管有些知名偵測軟體可以偵測一般的Rootkit，但面對變異型Rootkit卻常常無法有效偵測。本研究之貢獻為研製一款適用於雲端主機作業系統(Host OS)與虛擬機器使用者作業系統(Guest OS)上，結合特徵偵測及交叉查看技術以提升偵測能力。本機制亦加入TPM (Trusted Platform Module)嵌入式系統技術以提升Rootkit偵測能力，透過找出現有Windows Server 2008雲端作業系統與Windows 7作業系統之核心弱點，以建構雲端虛擬機器服務平台之安全基礎。

關鍵詞：Rootkit、嵌入式系統、Windows 作業系統、雲端服務、惡意軟體、系統安全

目錄

內容目錄 中文摘要	i	中文摘要	i
ii 致謝詞	iii	內容目錄	iii
iv 圖目錄	vi	表目錄	vi
vii 第一章 緒論	1	第一節 研究背景	1
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	3
4 第二章 文獻探討	6	第一節 雲端服務環境	6
6 第二節 Rootkit的種類與隱藏技術	10	第三節 Rootkit 偵測技術	17
四節 TPM技術	23	第三章 建構雲端服務之Rootkit偵測機制	28
28 第一節 整體Rootkit偵測架構	28	第二節 偵測機制	28
30 第三節 機制模組設計	32	第四章 實驗設計與分析	32
39 第一節 實驗環境	39	第二節 偵測機制測試	39
39 第三節 偵測能力與分析	42	第五章 結論	42
47 參考文獻	48		48

參考文獻

- [1] Dino A. Dai Zovi ,Advanced MAC OS X Rootkits [Online] available: http://www.hakim.ws/BHUSA09/speakers/Dai_Zovi_Mac_Rootkits/BlackHat-USA-09-Dai_Zovi-Mac-OS-X-Rootkits-wp.pdf, [Apr 18, 2013]
- [2] B. Cogswe and M. Russinovich, RootkitRevealer, [Online] available: <http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx>. [Apr 13, 2013]
- [3] R. Riley, X. Jiang and D. Xu, Guest-Transparent Prevention of Kernel Rootkits with VMM-based Memory Shadowing, Proceedings of the 11th International Symposium on Recent Advances Intrusion Detection, Volume 5230, pp. 1-20, 2008.
- [4] Cloud U-TM , Understanding The Cloud Computing Stack SaaS, PaaS, IaaS . [Online] available: http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf [Sep 18, 2012]
- [5] Research and markets, Cloud Computing – SaaS, PaaS, IaaS Market, Mobile Cloud Computing, M&A, Investments, and Future Forecast, Worldwide.
- [6] Rackspace Support, Understanding The Cloud Computing Stack SaaS, PaaS, IaaS. [Online] available: http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas [Apr 11, 2013]
- [7] S. T. King et al., SubVirt: Implementing Malware with Virtual Machines, Proceedings of the 2006 IEEE Symposium on Security and Privacy, pp.314 – 327, 2006.
- [8] C. Kruegel, W. Robertson and G. Vigna, Detecting Kernel-Level Rootkits Through Binary Analysis, Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC ' 04), pp. 91-100, 2004.

- [9] D. Geer, Hackers Get to the Root of the Problem, Computer, 2006.
- [10] Tripwire.
- [Online] available: <http://www.tripwire.com> [Mar. 18, 2013]
- [11] D. Molina, M. Zimmerman, G. Roberts, M. Eadie, and G. Peterson, Timely Rootkit Detection During Live Response, Proceedings of IFIP International Federation for Information Processing, vol. 285, pp. 139-148, 2008.
- [12] S. T. King and P. M. Chen, Backtracking Intrusions, ACM Transactions on Computer Systems, Vol. 37 Issue 5, pp. 223-236, 2005.
- [13] E. Kumar, Battle with the Unseen – Understanding Rootkits on Windows, Proceedings of the 9th AVAR International conference, 2000.
- [14] A. Matrosov, E. Rodionov, D. Harley and J. Malcho, Stuxnet Under the Microscope, Technical Report of ESET, 2010.
- [15] F. Daniel and P. Bravo, Rootkits Survey: A Concealment Story, Garcia Department of Informatics, University of Oviedo, 2011.
- [16] G. Hoglund and J. Butler, Rootkits: Subverting the Windows Kernel. Addison Wesley, 2006.
- [17] S. King et al., SubVirt: Implementing Malware with Virtual machines, Proceedings from the IEEE Symposium on Security and Privacy, pp. 314 – 327, 2006.
- [18] M. Myers and S. Youndt, An Introduction to Hardware-Assisted Virtual Machine (HVM) Rootkits, White Paper of Crucial Security, 2007.
- [19] D. A. D. Zovi, Hardware Virtualization Rootkits.
- [Online] Available: http://www.theta44.org/software/HVM_Rootkits_ddz_bhusa-06.pdf [Apr 18, 2013]
- [20] J. Rutkowska, Subverting Vista Kernel for Fun and Profit.
- [Online] available: <http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf> [Apr 18, 2013]
- [21] F. Wecherowski, A Real SMM Rootkit: Reversing and Hooking BIOS SMI Handlers, Phrack Magazine, 2009.
- [22] R. Wojtczuk and J. Rutkowska, Attacking SMM Memory via Intel CPU Cache Poisoning, White Paper of Invisible Things Lab., 2009.
- [23] N. Kumar and V. Kumar, Vbootkit: Compromising Windows Vista Security, Black Hat USA Conference, 2007.
- [24] L. Dufлот, Using CPU System Management Mode to Circumvent Operating System Security Functions, CanSecWest Applied Security Conference, 2006.
- [25] E. Florio and K. Kasslin, Your Computer is Now Stoned (Again!): the Rise of MBR Rootkits, Technical Report of Symantec, 2008.
- [26] J. Heasman, Implementing and Detecting a PCI Rootkit, White paper of Next Generation Security Software Ltd., 2007.
- [27] J. Heasman, Implementing and Detecting An ACPI BIOS Rootkit, White paper of Next Generation Security Software Ltd., 2006
- [28] Keisuke Takemori, Adrian Perrig, Ning Qu, Yutaka Miyake, Remote Attestation for HDD Files using Kernel Protection Mechanism, IEEE Communications Society, 2010.
- [29] W. J. Tsaur, S. R. Wu and J. X. Wu, Windows Rootkits Stealth Technologies in Cloud Computing, Proceedings of CISC, Taiwan, 2012.
- [30] H. David, TDL4 rebooted, [Online] available: <http://blog.eset.com/2011/10/18/tdl4-rebooted> [Apr 14, 2013]
- [31] M. Davis, S. Bodmer, and A. LeMasters. Hacking Exposed: Malware and Rootkits. New York: McGraw-Hill, 2009.
- [32] Microsoft Security Essentials [Software] Available: http://www.microsoft.com/security_essentials [Sep 29, 2012]
- [33] Kaspersky Internet Security [Software] Available: <http://www.kaspersky.com/> [Apr 21, 2013]
- [34] MalwareBytes Anti-Malware [Software] Available: <http://www.malwarebytes.org/mbam.php> [Apr 12, 2013]
- [35] G. Jacob, H. Debar, and E. Filiol, Behavioral Detection of Malware: from A Survey Towards An Established Taxonomy, Journal Computer Virology, 2008.
- [36] D. Wagner, Mimicry Attacks on Host-Based Intrusion Detection Systems, Proceedings of the 9th ACM conference on computer and communications security, 2002.
- [37] N. L. Petroni, J. Timothy, F. Aaron, W. William and A. Arbaugh, An Architecture for Specification-Based Detection of Semantic Integrity Violations in Kernel Dynamic Data, Proceedings of the USENIX Security Symposium, 2006.
- [38] F. Gadaleta, N. Nikiforakis, Y. Younan and W. Joosen, Hello Rootkitty: A Lightweight Invariance-Enforcing Framework, Information Security, 2011.
- [39] M. D. Ernst, J. H. Perkins, P. J. Guo, S. McCamant, C. Pacheco, M. S. Tschantz and C. Xiao, The Daikon System for Dynamic Detection of Likely Invariants, Science of Computer Programming, 2007.
- [40] F. Gadaleta, N. Nikiforakis, J. Muhlberg and W. Joosen, Hyperforce: Hypervisor-Enforced Execution of Security-Critical Code, Information Security and Privacy, 2011.
- [41] A. Baliga, V. Ganapathy and L. Iftode, Detecting Kernel-Level Rootkits Using Data Structure Invariants, Proceedings of IEEE Transactions on Dependable and Secure Computing, 2011.
- [42] M. Carbone, W. Lee, W. Cui, M. Peinado, L. Lu and X. Jiang, Mapping Kernel Objects to Enable Systematic Integrity Checking, Proceedings of ACM Conference on Computer and Communications Security, 2009.
- [43] G. Hoglund, Rootkits: Subverting the Windows Kernel, Addison-Wesley, 2005.
- [44] Microsoft, Kernel Patch Protection: Frequently Asked Questions [Online] available: <http://msdn.microsoft.com/en-us/windows/hardware/gg487353> [Apr 19, 2013]
- [45] M. Russinovich and D. Solomon, Windows Internals. Microsoft, 5th edition, 2009.
- [46] J. Rutkowska, Rootkits vs. stealth by design malware, [Online] available: <https://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Rutkowska.pdf> [Apr 28, 2013]
- [47] Z. Wang, X. Jiang, W. Cui and P. Ning, Countering Kernel Rootkits with Lightweight Hook Protection, Proceedings of ACM Conference on Computer and Communications Security, 2009.

- [48] H. Yin, P. Poosankam, S. Hanna and D. Song, Hookscout: Proactive Binary-Centric Hook Detection, Proceedings of the 7th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, 2010.
- [49] McAfee deepsafe.
- [Online] available: <http://www.mcafee.com/us/solutions/mcafee-deepsafe.aspx> [Mar 18, 2013]
- [50] A. Seshadri, M. Luk, N. Qu and A. Perrig, Secvisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity For commodity OSes, 2007.
- [51] Gmer [Online] available: <http://www.gmer.net/> [Apr. 18, 2013]
- [52] B. Blunden, The Rootkit Arsenal, Wordware Publishing, 2009.
- [53] B. Cogswell and M. Russinovich, Rootkitrevealer [Online] available: <http://technet.microsoft.com/en-us/sysinternals/bb897445> [Apr. 14, 2013]
- [54] M. Russinovich, Rootkit Revealer [Online] available: <http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx> [Apr. 18, 2013]
- [55] IceSword [Online] available: <http://www.softpedia.com/get/System/System-Info/IceSword.shtml> [Apr. 23, 2013]
- [56] Rootkit Unhooker [Online] available: <http://www.antirootkit.com/software/RootKit-Unhooker.htm>, 2012.
- [Apr. 12, 2013]
- [57] P. Gmerek, [Online] available: <http://www.gmer.net/> [Apr. 13, 2013]
- [58] U.S. Patent No. 11/271327. Washington, DC: U.S., Patent and Trademark Office, 2010.
- [59] Burdach M., Finding Digital Evidence in Physical Memory, Proceedings for Black Hat Federal Conference, 2006.
- [60] G. Garcia, Forensic Physical Memory Analysis: An Overview of Tools and Techniques, Proceedings for TTK T-110.5290 Seminar on Network Security, 2007.
- [61] Hbgary responder pro, <http://www.hbgary.com/responder-pro-2> [Apr. 12, 2013]
- [62] A. Walters, The volatility framework: Volatile memory artifact extraction utility framework, [Online] available: <https://www.volatilitysystems.com/default/volatility>, 2012.
- [Apr. 18, 2013]
- [63] Volatility malware plugins, [Online] available: <http://code.google.com/p/malwarecookbook>, 2012.
- [Apr. 18, 2013]
- [64] A. Schuster, Pool Allocations as an Information Source in Windows Memory Forensics, Pool Allocations as an Information Source in Windows Memory Forensics, 2006.
- [65] A. Schuster, Searching for Processes and Threads in Microsoft Windows Memory Dumps, Digital Investigation, 2006.
- [66] IBM Provisioning User Guide [Online] available: http://pic.dhe.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.tivoli.tpm.scenario.doc/tpm_user_guide.pdf [Apr. 12, 2013]
- [67] Total Productive Maintenance, [Online] available: <http://www.ame.org/sites/default/files/TPM-introduction-AME.pdf> [Mar. 1, 2013]
- [68] Trusted Platform Module (TPM) Quick Reference Guide [Online] available: http://downloadmirror.intel.com/15034/eng/DQ965CO_TPM_QuickRefGuide03.pdf [Apr. 4, 2013]
- [69] Smart TPM [Online] available: http://download.gigabyte.ru/manual/motherboard_manual_smart-tpm_c.pdf [Apr. 6, 2013]
- [70] TWCERT [Online] available: http://newsletter.certcc.org.tw/epaper/201109/tech2_2.html [Apr. 13, 2013]
- [71] IntelR Trusted Execution Technology (IntelR TXT) [Online] available: <http://download.intel.com/technology/security/downloads/315168.pdf> [Apr. 15, 2013]
- [72] W. Huang, Windows Rootkits Detection Technologies for Service Platforms in Cloud Computing, Master thesis, Da-Yeh University, 2011.