

雲端運算服務平台之Windows Rootkits偵測機制

黃奕璽、曹偉駿

E-mail: 343857@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，目前資安研究者多著墨於資料安全防護，包括資料隱私性與保密性之研究。然而，雲端虛擬機器服務平台之安全防護亦不容忽視。現今雲端服務架構皆以虛擬化技術為基礎並建構在雲端作業系統之上，一旦雲端作業系統遭受惡意程式破壞，則建構在雲端作業系統上的虛擬機器亦將隨之崩潰，因此雲端作業系統之安全防護就顯得格外重要。目前有越來越多惡意程式結合Rootkit技術來遮掩本身的不法行為，使得雲端作業系統安全的防衛面臨了極大的挑戰。就我們所知，目前相關文獻皆在探討雲端運算環境中的使用者端作業系統(Guest OS)防護，並無針對雲端主機作業系統(Host OS)安全議題進行探討，因此本研究將是首先嘗試於Windows 雲端主機作業系統中，開發能偵測未知型Kernel Mode Rootkits之技術，以建構雲端虛擬機器服務平台之安全基礎。本研究首先發展出一新型且有能力躲避現有知名偵測軟體的Windows 雲端作業系統Driver-hidden Rootkit，以指出這些知名偵測軟體的缺失，接著則進一步開發能有效偵測各種Windows雲端作業系統Driver-hidden Rootkits之機制，包括亦能偵測本研究所研製之新型Rootkit，亦即將建構出Windows 雲端作業系統Driver-hidden Rootkits偵測技術，尤其能夠偵測未知型Driver-hidden Rootkits，能提供雲端作業系統對Kernel Mode Rootkits完善的偵測能力。透過實驗測試與分析，在偵測率、偵測時間、CPU佔用率、I/O使用率方面，本機制相較國際知名防毒軟體大廠ESET、AVAST及趨勢科技的Rootkit偵測軟體，皆勝出許多，因此我們堅信本機制具有極高的實用價值。

關鍵詞：雲端運算、雲端運算安全、惡意程式、Rootkit、系統安全、Windows作業系統、核心模式

目錄

中文摘要	iii	英文摘要	iii
	v	誌謝辭	v
	vi	內容目錄	vi
	viii	表目錄	viii
	x	圖目錄	x
第一章 緒論	1	1.1 研究背景	1
		1.2 研究動機與目的	1
		1.3 研究流程	1
第二章 文獻探討	3		
2.1 雲端運算技術	7	2.1.1 雲端運算定義	7
		2.1.2 雲端運算之分類	7
		2.2 雲端運算安全議題	7
		2.3 Windows Rootkits 的種類與隱藏技術	8
		2.3.1 Rootkit的種類與隱藏技術	14
		2.3.2 Rootkit的種類	14
		2.3.3 Rootkits 的隱藏的技術	15
		2.4 隱藏技巧	18
		2.5 新型Windows Rootkits偵測技術探討	25
		2.5.1 定義搜尋記憶體範圍	34
		2.5.2 尋找Object Drivers的方法	34
第三章 適用雲端運算之Windows Rootkit偵測機制	43	3.1 新型Windows Rootkits隱藏技術	43
		3.2 新型Windows Rootkits偵測技術	43
第四章 實驗設計與分析	47		
		4.1 系統建置	51
		4.2 隱藏能力之實驗設計與分析	51
		4.2.1 Rootkit載入前置作業	52
		4.2.2 隱藏能力測試與分析	52
		4.3 偵測能力之實驗設計與分析	54
		4.3.1 Anti-rootkit 載入與偵測器測試	54

.....	58 4.3.2 偵測能力測試與分析
.....	60 第五章 結論與未來展望
.....	72 參考文獻	74

參考文獻

- [1]A. Rosenthal, et al., " Cloud computing: A new business paradigm for biomedical information sharing, " Journal of Biomedical Informatics, vol. 43, no. 2, pp. 342-353, 2010.
- [2]S. Paquette, et al., " Identifying the security risks associated with governmental use of cloud computing, " Government Information Quarterly, vol. 27, no. 3, pp. 245-253, 2010.
- [3]Z. Liang-Jie and Z. Qun, " CCOA: Cloud computing open architecture, " Proceedings of IEEE International Conference on Web Services (ICWS 2009), pp. 607-616, 2009.
- [4]L. Liu, et al., " GreenCloud: A new architecture for green data center, " Proceedings of the 6th International Conference Industry Session On Autonomic Computing and Communications Industry Session(ICAC-INDST '09), pp. 29-38, 2009.
- [5]Flavio Lombardi, Roberto Di Pietro, " Secure virtualization for cloud computing, " Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1113-1122, 2011.
- [6]Amazon Elastic Computer Cloud (Amazon EC2), <http://aws.amazon.com/ec2/>, November 9, 2010.
- [7]C. Keong, " Defeating Kernel Native API Hookers by Direct Service Dispatch Table Restoration, " Technical Report, SIG2 G-TEC Lab, October, 2004.
- [8]G. Hunt and D. Brubacker, " Detours: Binary Interception of Win32 Functions, " Proceedings of the Third USENIX Windows NT Symposium, pp. 135-143, 1999.
- [9]VICE, http://www.rootkit.com/board_project_fused.php?did=proj20, 2010.
- [10]A. Baliga, L. Iftode, X. Chen, " Automated containment of rootkits attacks, " Computers & Security, vol. 27, no. 7-8, pp. 323-334, 2008.
- [11]R. Sherstobitoff and P. Bustamante, " You Installed Internet Security on Your Network: Is Your Company Safe?, " Information Systems Security, vol. 16, pp. 188-194, 2007.
- [12]Insu Park, R. Sharman, H.R. Rao, S. Upadhyaya, " Short Term and Total Life Impact analysis of email worms in computer systems, " Decision Support Systems, vol. 43, no. 3, pp. 827-841, 2007.
- [13]M. Armbrust, et al., " A view of cloud computing, " Communications of the ACM, vol. 53, no. 4, pp. 50-58, 2010.
- [14]M. Fouquet, et al., " Cloud computing for the masses, " Proceedings of the 1st ACM workshop on User-provided networking: challenges and opportunities, pp. 31-36, 2009.
- [15]Google App Engine, <http://code.google.com/intl/en/appengine>, November 9, 2010.
- [16]Microsoft Azure, <http://www.microsoft.com/azure>, November 9, 2010.
- [17]S. Subashini and V. Kavitha, " A survey on security issues in service delivery models of cloud computing, " Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.
- [18]R. Buyya, et al., " Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, " Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616, 2009.
- [19]Mcloud, <http://www.microsoft.com/taiwan/Mcloud/>, November 9, 2010.
- [20]A. Schuster, " The impact of Microsoft Windows pool allocation strategies on memory forensics, " Digital Investigation, vol. 5, no. 1, pp. S58-S64, 2008.
- [21]MmIsAddressValid Routine, [http://msdn.microsoft.com/en-us/library/ff554572\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ff554572(v=vs.85).aspx), May 3, 2011.
- [22]James Okolica, " Gilbert L. Peterson, Windows operating systems agnostic memory analysis, " Digital Investigation, Vol 7, PP. S48-S56, 2010.
- [23]B. Andreas, " UNIX and Linux based Rootkits Techniques and Countermeasures, " DFN-CERT Services GmbH, 2004.
- [24]G. Hoglund and J. Butler, Rootkits: Subverting the Windows kernel, Addison-Wesley, 2005.
- [25]D. Molina, M. Zimmerman, G. Roberts, M. Eaddie, and G. Peterson, " Timely rookit detection during live response, " Proceedings of IFIP International Federation for Information Processing, vol. 285, pp. 139-148, 2008.
- [26]T. Woei-Jiunn and C. Yuh-Chen, " Exploring Rootkit Detectors' Vulnerabilities Using a New Windows Hidden Driver Based Rootkit, " Proceedings of the 2010 IEEE International Conference on Information Privacy , Security, Risk and Trust (PASSAT 2010), pp. 842-848, 2010.
- [27]A. Chuvakin, An Overview of Unix Rootkits, iALERT White Paper, iDefense Labs, Chantilly, Virginia, 2003.
- [28]S. T. King and P. M. Chen, " Backtracking intrusions, " ACM Transactions on Computer Systems, vol. 23, no. 1, pp. 51-76, 2005.
- [29]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.
- [30]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.

[31]D. Geer, " Hackers get to the root of the problem, " Computer, vol. 39, no. 5, pp. 17-19, 2006.

[32]Tripwire, <http://www.tripwire.com>, 2008, November 9, 2010.

[33]Y. Yanfang, W. Dingding, L. Tao, Y. Dongyi, J. Qingshan, " An intelligent PE-malware detection system based on association mining, " Journal in Computer Virology, vol.4, no.4, pp. 323-334, 2008.

[34]J. Bulter, J. L. Undercoffer, and J. Pinkston, " Hidden process: the implication for intrusion detection, " Proceedings of the IEEE International Workshop on Information Assurance, pp. 116-121, 2003.

[35]L. Stevenson and N. Altholz, Rootkits for Dummies, Wiley Publishing, 2007.

[36]Kumar, Eric, " Primary Title: User-mode memory scanning on 32-bit & 64-bit windows, " Journal in Computer Virology, Vol. 6, no.5, 2010.

[37]Lobo, D. Watters, P. Xinwen Wu , " RBACS: Rootkit Behavioral Analysis and Classification System, " Proceedings of the Third International Conference on Knowledge Discovery and Data Mining (WKDD '10) , pp.75-80, 2010.

[38]TDL3: The Rootkit of All Evil?, <http://www.eset.com/us/resources/white-papers/TDL3-Analysis.pdf>, Jul 3, 2011.

[39]TDSS part 1: The x64 Dollar Question, <http://resources.infosecinstitute.com/tdss4-part-1/>, Jul 3, 2011.

[40]Trendmicro, <http://tw.trendmicro.com/tw/support/tech-support/board/tech/article/20110301065025.html>, Jun. 3, 2011.

[41]T. Fawcett, " An introduction to ROC analysis, " Pattern Recognition Letters, vol. 27, no. 8, pp. 861-874, 2006.