

# 有效的Windows核心模式Rootkits偵測技術研究

蔡秉諭、曹偉駿

E-mail: 9806121@mail.dyu.edu.tw

## 摘要

有越來越多惡意程式結合Rootkit技術來遮掩本身的不法行為，使得系統安全的防衛面臨了極大的挑戰。我們發現先進的Rootkit技術都屬於核心模式，並且絕大部份都是以“驅動程式”的形態被載入到Windows作業系統核心中。為了能躲避偵測軟體之偵測，Rootkit技術勢必具備能隱藏其本身驅動程式的功能。因此，對系統安全來說，能偵測以驅動程式型態隱藏的Rootkit是很相當重要的。然而目前知名偵測軟體無法偵測未知型Driver-hidden Rootkit之功能。因此本研究將進一步開發具有資料探勘的新型有效Driver-hidden Rootkits之軟體，並使其具備能將所偵測到的Rootkits從作業系統中進行卸載(Unload)，以徹底去除其潛在的破壞。本偵測軟體開發完成後，也在Testbed@TWISC平台上針對Windows XP SP2及SP3此種作業系統進行實測其偵測功能。我們相信本研究所提出之偵測方法，應能激勵並提供相關研發Rootkit偵測軟體之廠商以改善其目前有關偵測未知型Windows Driver-hidden Rootkits的能力。

關鍵詞：惡意軟體、rootkit、Windows、核心模式、系統安全

## 目錄

中文摘要	iii
英文摘要	iv
誌謝辭	
v	
內容目錄	vi
表目錄	viii
圖目錄	ix
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	3
第四節 研究流程	3
第五節 論文架構	4
第二章 文獻探討	6
第一節 Rootkit的種類與隱藏技術	6
第二節 Rootkit 偵測技術	16
第三節 新型Driver-hidden Rootkit 隱藏方法	19
第四節 找出Object Drivers的方法	31
第五節 基於資料探勘之惡意軟體偵測技術	39
第三章 建構Driver-hidden Rootkits偵測機制	42
第一節 機制流程	42
第二節 機制模組設計	46
第四章 實驗設計與分析	56
第一節 實驗環境	56
第二節 偵測機制測試	56
第三節 機制可行性分析	60
第五章 結論與未來展望	65
參考文獻	67

## 參考文獻

一、中文部份陳昱成 (2008)，變形的Windows Kernel Mode Rootkit 分析研究，私立大葉大學資訊管理研究所未出版之碩士論文

。TWISC@NCKU(2007) , Testbed@TWISC介紹 [線上資料] , 來源  
[http://testbed.ncku.edu.tw/docfortestbed/20071002\\_Testbed@TWISC\\_introduction.pdf](http://testbed.ncku.edu.tw/docfortestbed/20071002_Testbed@TWISC_introduction.pdf) [2009, Jan. 10]。二、英文部份

Andreas, B. (2004). UNIX and Linux based Rootkits Techniques and Countermeasures. Papers for 16th Annual FIRST Conference on Computer Security Incident Handling. Anti Rootkit Software, News, Articles and Forums [online]. Available: <http://www.antirootkit.com> [2009, June. 14].

Badishi, G., Herzberg, A., & Keidar, I. (2007). Keeping Denial-of-Service Attackers in the Dark. *IEEE Transactions on Dependable and Secure Computing*, 4(3), pp. 194-204.

Baliga, A., Iftode, L., & Chen, X. (2008). Automated Containment of Rootkits Attacks. *Computers & Security*, 27(7-8), pp. 323-334.

Beaucamps, P. (2007). Advanced Polymorphic Techniques. *International Journal of Computer Science*, 2(3), pp. 194-205.

Beck, D., Vo, B., & Verbowski, C. (2005). Detecting Stealth Software with Strider Ghostbuster. *International Conference on Dependable Systems and Networks*, (pp. 368-377).

Bulter, J., & Honglund, G. (2004). Retrieved 6 14, 2009, from Rootkit Forum: <http://www.rootkit.com>

Bulter, J., Undercoffer, L. J., & Pinkston, J. (2003). Hidden process: the Implication for Intrusion Detection. *Proceedings of the IEEE International Workshop on Information Assurance*, (pp. 116-121).

Chan, P. K., & Stolfo, S. J. (1997). On the Accuracy of Meta-Learning for Scalable Data Mining. *Journal of Intelligent Information System*, 8(1), pp. 5-28.

Chian, K., & Lloyd, L. (2007). A Case Study of the Rustock Rootkit and Spam Bot. *Proceedings of USENIX First Workshop on Hot Topics in Understanding Bonets*.

Chuvakin, A. (2003). An Overview of Unix Rootkits. iALERT White Paper, iDefense Labs, Chantilly, Virginia.

Cogswell, B., & Russinovich, M. (2005). RootkitRevealer [online]. Available: <http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx>. [2009, June. 14].

Dhamija, R., & Tygar, D. J. (2005). The Battle against Phishing: Dynamic Security Skins. *Proceedings of the 1st Symposium on Usable Privacy and Security*, (pp. 77-78).

Felten, E. W., & Halderman, J. A. (2006). Digital Rights Management, Spyware, and Security. *IEEE Security & Privacy*, 4(1), pp. 18-23.

Florio, E. (2005). When Malware Meets Rootkits [online]. Available: <http://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf> [2009, June. 14].

Geer, D. (2006). Hackers Get to the Root of the Problem. *IEEE Computer*, 39(5), pp. 17-19.

Herly, G., & Florencio, D. (2006). How to Login from an Internet Cofe without Worrying about Keyloggers. *Proceedings of the 2nd Symposium on Usable Privacy and Security*, (pp. 10-15).

Hoglund, G., & Butler, J. (2005). Rootkits: Subverting the Windows Kernel. Addison-Wesley.

Hunt, G., & Brubacher, D. (1999). Detours: Binary Interception of win32 Functions. *Proceedings of the 3rd USENIX Windows NT Symposium*, (pp. 135-143).

Jamie, B. (2004). VICE-Catch the Hookers. <http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-butler/bh-us-04-butler.pdf> [2009, June. 14].

Jazzar, M., & Jantan, A. (2008). An Approach for Anomaly Intrusion Detection Based on Causal Knowledge-Driven Diagnosis and Direction. *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, pp. 39-48.

Keong, C. (2004). Defeating Kernel Native API Hookers by Direct Service Dispatch Table Restoration [Online]. Available: <http://www.packetstormsecurity.org/hitb04/hitb04-chew-keong-tan.pdf> [2009, June. 10].

Kim, H. G., & Spafford, H. E. (1994). The Design and Implementation of Tripwire: A File System Integrity Checker. *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, (pp. 18-29).

Kim, Y. S., Jung, S. T., Suh, H. E., & Hwang, S. H. (2006). Customer Segmentation and Strategy Development Based on Customer Lifetime Value: A Case Study. *Expert Systems with Applications*, 31(1), pp. 101-107.

King, S., Chen, P., Wang, Y., Verbowski, C., Wang, H., & Lorch, J. (2006). SubVirt: Implementing Malware with Virtual Machines. *Proceedings of the IEEE Symposium on Security and Privacy*, (pp. 314-327).

King, T. S., & Chen, M. P. (2005). Backtracking Intrusions. *ACM Transactions on Computer Systems*, 23(1), pp. 51-76.

Kreibich, C., & Crowcroft, J. (2004). Honeycomb: Creating Intrusion Detection Signatures Using Honeypots. *ACM SIGCOMM Computer Communication Review*, pp. 51-56.

Kruegel, C., Robertson, W., & Vigna, G. (2004). Detection Kernel-Level Rootkits through Binary Analysis. *Proceedings of the 20th Annual Computer Security Applications Conference*.

Kumar, E. (2006). Battle with the Unseen – Understanding Rootkits on Windows. *Proceedings of the 9th AVAR International Conference*, (pp. 82-101).

Lee, W., Stolfo, S. J., & Mok, K. W. (1999). A Data Mining Framework for Building Intrusion Detection Models. *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, pp. 120-132.

Levine, J., Grizzard, J., & Owen, H. (2006). Detecting and Categorizing Kernel-level Rootkits to Aid Future Detection. *IEEE Security & Privacy*, 4(1), pp. 24-32.

Martignoni, L., Stinson, E., Fredrikson, M., Jha, S., & Mitchell, J. C. (2008). A Layered Architecture for Detecting Malicious Behaviors. *Lecture Notes in Computer Science*, 5230, pp. 78-97.

McAfee. (2006). Retrieved 6 14, 2009, from Rootkits, Part 1 of 3: The Growing Threat: [http://www.mcafee.com/us/local\\_content/white\\_papers/threat\\_center/wp\\_akapoor\\_rootkits1\\_en.pdf](http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf)

Mirkovic, J., & Reiher, P. (2005). D-word: A Source-end Defense against Flooding Denial-of-Service Attacks. *IEEE Transactions on Dependable and Secure Computing*, 2(3), pp. 216-232.

Molina, D., Zimmerman, M., Roberts, G., Eaddie, M., & Peterson, G. (2008). Timely Rootkit Detection During Live Response. *IFIP International Federation for Information Processing*, 285, pp. 139-148.

Monastyrsky, A., Saponov, K., & Monastyrsky, Y. (2005). Kaspersky Lab [Online]. Available: <http://www.vi-ruslist.com/en/analysis?pubid=168740859>[2009, June 25].

Oh, S. J., & Kim, J. S. (2005). A Hierarchical Clustering Algorithm for Categorical Sequence Data. *International Journal of Information Technology & Decision Making*, 4(1), pp. 81-96.

Petroni, N. L., Fraser, T., Molina, J., & Arbaugh, W. A. (2004). Copilot-a Coprocessor-based Kernel Runtime Integrity Monitor. *Proceedings of the 13th Usenix Security Symposium*, (pp. 179-194).

Quinlan, R. J. (1993). C4.5: Programs for Machine Learning. San Francisco: Morgan Kaufmann.

Quinlan, R. J. (1986). Induction on Decision Tree. *Machine Learning*, 1(1), pp. 82-106.

Rabek, J., Khazan, R., Lewandowski, S., & Cunningham, R. (2003). Detecting of Injected, Dynamically Generated, and Obfuscated Malicious Code. *Proceedings of the ACM Workshop on Rapid Malcode*, (pp. 76-82).

Ramakrishna, P., & Maarof, M. A. (2002). Detecting and Prevention of Active Sniffing on Routing Protocol. *Student Conference on Research and Development*, pp. 498-501.

Ronald, R. (1995). Retrieved 6 14, 2009, from MD5 [Online]. Available:

<http://en.wikipedia.org/wiki/MD5> [2009, June 25].Schultz, M. G., Eskin, E., Zadok, E., & Stolfo, S. J. (2001). Data Mining Methods for Detection of New Malicious Executables. *IEEE Symposium on Security and Privacy*, (pp. 39-49).Shaw, J. M., Subramaniam, C., Tan, W. G., & Welge, E. M. (2001). Knowledge Management and Data Mining for Marketing. *Decision Support Systems*, 31(1), pp. 127-137.Shih, H. D., Chiang, S. H., & Lin, B. (2007). A Generalized Associative Petri Net for Reasoning. *IEEE Transactions on Knowledge and Data Engineering*, 19(9), pp. 1241-1251.Sobh, T. S. (2006). Wired and Wireless Intrusion Detection System: Classifications, Good Characteristics and State-of-the-art. *Computer Standards & Interfaces*, 28(6), pp. 670-694.Spitzner, L. (2003). The HoneyNet Project: Trapping the Hackers. *IEEE Security & Privacy*, 1(2), 15-23.Sy, B. K. (2009). Integrating Intrusion Alert Information to Aid Forensic Explanation: An Analytical Intrusion Detection Framework for Distributive IDS. *Information Fusion*, 10(4), pp. 325-341.Tsaur, W. J., Chen, Y. C., & Tsai, B. Y. (2009). A New Windows Driver-hidden Rootkit Based on Direct Kernel Object Manipulation. *Lecture Notes in Computer Science*, 5574, pp. 202-213.Ye, Y., Wang, D., Li, T., & Ye, D. (2007). IMDS: Intelligent Malware Detection System. *The 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, (pp. 1043-1047).