A Study on Effective Technology for Detecting Windows Kernel Mode Rootkits

蔡秉諭、曹偉駿

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

ABSTRACT

More and more malicious programs are combined with rootkits to shield their illegal activities, and the result makes information security defense encounter a great challenge. It can be observed that most sophisticated kernel mode rootkits are implemented to execute hiding tasks through drivers in Windows Kernel. Thus, for the purpose of system security, the role of a detector for detecting Windows driver-hidden rootkits is becoming extremely important. However, we have verified currently well-known detecting software that it can not successfully avoid a variety of driver-hidden rootkit. Therefore, we propose a countermeasure to effectively detect Windows driver-hidden rootkits. Furthermore, we will also develop an effective scheme to unload the detected driver-hidden rootkit from Windows to achieve higher system security, in order to clearly remove the destructions from the system. After the proposal detecting scheme have been developed, we will test it on the Testbed@TWISC platform by Windows XP SP2 and SP3. We affirm our efforts will be extremely useful for improving the current techniques of detecting unknown Windows driver-hidden rootkits.

Keywords : malware、rootkit、Windows、kernel mode、system security

Table of Contents

REFERENCES

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 [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.comBulter, 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 Honypots. 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.pdfMirkovic, 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., Sapronov, 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.Spitizner, 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).