# A Study on Polymorphic Windows Kernel Mode Rootkit

**陳昱成、曹偉駿**

E-mail: 9707374@mail.dyu.edu.tw

## ABSTRACT

More and more malicious programs are combined with rootkits to shield their illegal activities and the result makes security products face a challenge. It can be observed that most sophisticated kernel mode rootkits are implemented to execute hiding tasks through drivers in Windows Kernel. Therefore, the role of a detector for detecting Windows driver-hidden rootkits is becoming extremely important. In this thesis, we first develop a new Windows driver-hidden rootkit with five tricks based on Direct Kernel Object Manipulation, and have verified that it can successfully avoid well-known rootkit detectors. And we then propose a countermeasure to detect it. We affirm our efforts will be extremely useful for improving the current techniques of detecting Windows driver-hidden rootkits.

Keywords : malware ; windows ; rootkit ; kernel mode ; system security

## Table of Contents

## REFERENCES

Badishi, G., Herzberg, A., & Keidar, I. (2007). Keeping denial-of-service attackers in the dark. IEEE Transactions on Dependable and Secure Computing, 4(3), 194-204. Beaucamps, P. (2007). Advanced polymorphic techniques. International Journal of Computer Science, 2(3), 194-205. Bulter, J., & Honglund, G. (2004). Rootkit Forum [online]. Available : http://www.rootkit.com [2008, Febryary 15]. Bulter, J., Undercoffer, J. L., & Pinkston, J. (2003). Hidden process: the implication for intrusion detection. Proceedings of the IEEE International Workshop on Information Assurance, (pp. 116-121), USA: New York. Chian, K., & Lloyd, L. (2007). A case study of the rustock rootkit and spam bot. Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Bonnets (pp. 10-18), USA: Cambridge Cogswell, B., & Russinovich, M. (2005). RootkitRevealer [online]. Available: http://technet.microsoft.com/en-us/sysinternals/bb8 97445.aspx [2008, March 11]. Dhamija, R., & Tygar, J. D. (2005). The battle against phishing: dynamic security skins. Proceedings of the First Symposium on Usable Privacy and Security (pp. 77-88), USA: Pittsburgh. Felten, E. W., & Halderman, J. A. (2006). Digital rights management, spyware, and security. IEEE Security & Privacy, 1(4), 18-23. Florio, E. (2005). When Malware Meets Rootkits [online]. Available: http://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf [2008, March 2]. Herly, C., & Florencio, D. (2006). How to login from an internet cofe without worrying about keyloggers. Proceedings of the Second Symposium on Usable Privacy and Security (pp. 10-15), USA: Pittsburgh. Hoglun, G., & Bulter, J. (2005). Rootkits: Subverting the Windows Kernel. California: Addison-Wesley. Hunt, G., & Brubacher, D. (1999). Detours: binary interception of win32 functions. Proceedings of the Third USENIX Windows NT Symposium (pp. 135-143), USA: Washington. 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 [2008, March 9]. Kim, G. H., & Spafford, E. H. (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), USA: Virginia. Kreibich, C., & Crowcroft, J. (2004). Honeycomb: creating intrusion detection signatures using honeypots. ACM

SIGCOMM Computer Communication Review, 34(1), 51-56. McAfee. (2006). Rootkits, Part 1 of 3: The Growing Threat [Online]. Available: http://www.mcafee.com/us/local_content/white_pap ers/threat_center/wp_akapoor_rootkits1_en.pdf [2008, April 22]. 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), 216-232. 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), USA: Washington. Ramakrishna, P., & Maarof, M. A. (2002). Detecting and prevention of active sniffing on routing protocol. Student Conference on Research and Development (pp. 498-501), Malaysia: Shah Alam. Rutkowska, J. (2006). Introducing Stealth Malware Taxonomy [Online]. Available: http://www.invisilethings.org/papers/malw are-taxonom.pdf [2008, Fabruary 7]. Schreiber, S. (2001). Undocumented Windows 2000 Secrets: A Programmer ’ s Cookbook. California: Addison-Wesley. Schuster, A. (2006). Searching for processes and threads in microsoft windows memory dumps. The International Journal of Digital Forensics & Incident Response, 3(1), 10-16. Spitzner, L. (2003). The honeynet project: trapping the hackers. IEEE Security & Privacy, 1(2), 15-23. Wang, Y. M., & Beck, D. (2005). Fast user-mode rootkit scanner for the enterprise. USENIX Proceedings of LISA Nineteenth Systems Administration Conference (pp. 23-30), USA: San Diego. Xianghe, L., Liancheng, Z., & Shuo, L. (2006). Kernel rootkits implement and detection. Wuhan University Journal of Natural Sciences, 11(6), 1473-1476.