Windows Rootkits detection technologies for service platforms in cloud computing

黃奕璽、曹偉駿

E-mail: 343857@mail.dyu.edu.tw

ABSTRACT

With the growing popularity of cloud computing, the security issues in cloud computing also emerge. Currently, information security researchers are focusing on cloud data security, including cloud data privacy and confidentiality. However, the security protection of the virtual-machine service platform in cloud computing is also crucial. The service architectures in cloud computing are based on the virtualization technology, which can achieve rapid deployment, resources flexibility, rapid disaster recovery, cost reduction, and so on. But even though the virtualization technology has the advantages mentioned above, it still has to be constructed based on cloud operating systems. And once the cloud operating systems suffer the attack of malware, the virtual machines constructed using the cloud operating systems will collapse. Therefore, the security protection of cloud operating systems is particularly critical. Nowadays, 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. To the best of our knowledge, existing literatures are mainly aimed at exploring protective measures for the Guest OS, while there are few researches involved in the security issues of the Host OS. Therefore, this thesis will firstly try to develop a technology for detecting unknown kernel-mode rootkits in Windows host operating systems for cloud compiting, and thus build the security infrastructure for the virtual-machine service platform in cloud computing. As for the research procedure, we will firstly develop a new-typed driver-hidden rootkit for Windows host operating systems. The proposed rootkit has the ability of escaping a wide variety of famous detecting software, and can be used to indicate the weakness of those well-known detecting software. Afterwards, we have developed an effective mechanism for detecting driver-hidden rootkits, including the proposed new-typed Rootkit threat and other existing rootkits. Through experimental test and analysis, we have found that, in the aspects of detection rate, detection time, CPU usage rate and I/O usage rate, the proposed mechanism is much more superior to the existing rootkit detection software developed by famous domestic and foreign anti-virus software manufacturers like ESET, AVAST and Trend Micro. Thus, we affirm that the proposed mechanism is extremely practical in the real world.

Keywords : Cloud Computing、Cloud Computing Security、Malware、Rootkit、System Security、Windows Operating System 、Kernel Mode

Table of Contents

REFERENCES

[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 , 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.