{tag} {/tag}

IJCA Special Issue on Communication Security

comnetcs - Number 1

Year of Publication: 2012

Authors:

Saurabh Chamotra

Rakesh Kumar Sehgal

Raj Kamal

{bibtex}comnetcs1007.bib{/bibtex}

Abstract

Malware analysis is a process of determining the intent and modus operandi of a given malware sample. It is the first step in process of developing any preventive or defensive measure against a malware attack. The work presented in this paper is focused on the dynamic malware analysis. Dynamic malware analysis is one of the malware analysis techniques, in which the malware sample is executed in a controlled environment called sandbox and the effects of the execution at different levels of system abstractions (I.e. operating system, network, or kernel) are captured, stored and processed. In this paper we are presenting the design details of a

malware execution environment named as Honeysand. The presented solution is specifically designed for catering the needs of performing dynamic analysis for a class of malwares known as bot. Bot is a class of mwalre that have the ability to coordinate among themselves and create a network of infected systems which is under the control of a single machine called command & control server [18] .Based upon the proposed system design we have developed a prototype system using the honeypot technology as a base with some other open source tools configured over it and used this prototype to demonstrate the effectiveness of the proposed solution.

References

- anubis.iseclab.org
- www.cwsandbox.org
- www.norman.com
- www.joebox.org
- netscty.com/malware-tool
- Shinsuke miwa,Toshiyuki miyiachi, Masashi eto, Masashi “Design and Implementation of an Isolated Sandbox with Mimetic Internet used to Analyze Malwares”
- Gérard Wagener • Radu State • Alexandre Dulaunoy “Malware behaviour analysis” Spinger-Verlag France 2007
- Andreas Moser, Christopher Kruegel, and Engin Kirda. “Limits of Static Analysis for Malware Detection”. In Proceedings of the 23rd Annual Computer Security Applications Conference(ACSAC), 2007
- Min Gyung Kang, Pongsin Poosankam, and Heng Yin. Renovo: “A Hidden Code Extractor for Packed Executables”. In Proceedings of the 5th ACM Workshop on Recurring Malcode (WORM), 2007.
- Lorenzo Martignoni, Mihai Christodorescu, and Somesh Jha. “OmniUnpack: Fast, Generic,and Safe Unpacking of Malware. In Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC), 2007.
- Boris Lau and Vanja Svajcer. Measuring virtual machine detection in malware using DSD tracer. Journal in Computer Virology, 6(3), 2010.
- Thomas Raffetseder, Christopher Kruegel, and Engin Kirda “Detecting System Emulators”
- Vasudevan, Yerraballi,”Cobra: Fine-grained Malware Analysis using Stealth Localized-Executions”. In: IEEE Symposium on Security and Privacy. (2006)
- Bayer, Kruegel,Kirda, “TTAnalyze: A Tool for Analyzing Malware”.In: 15th Annual Conference of the European Institute for Computer Antivirus Research (EICAR). (2006)
- Xu Chen, Jon Andersen, Zhuoqing Morley Mao, Michael Bailey, and Jose Nazario. “Towards an Understanding of Anti-Virtualization and Anti-Debugging Behavior in Modern Malware”. In Proceedings of the 38th Annual IEEE International Conference on Dependable Systems and Networks (DSN), 2008.
- Katsunari Yoshioka, Yoshihiko Hosobuchi, Tatsunori Orii, and Tsutomu Matsumoto. “Your Sandbox is blinded: Impact of Decoy Injection to Public Malware Analysis Systems”. Journal of Information Processing, 19, 2011.
- Manuel,EgeleTheodoor,ScholteEngine Survey on Automated Dynamic Malware Analysis

Techniques and Tools”

- Honeynet Project & Research Alliance. “Know your Enemy: Tracking Botnets”.
- MichaelBailey,JonOberheide,JonAndersen,Z. Morley Mao, Farnam Jahanian,Jose Nazario. “Automated Classification and Analysis of Internet Malware”
- T. Dullien and R. Rolles. “Graph-based comparison of Executable Objects”. In Symposium sur la S´ecurit´e des Technologies de l’Information et des Communications (SSTIC), June 2005.
- M. Christodorescu and S. Jha. Static “Analysis of Executables to Detect Malicious Patterns”. In Usenix Security Symposium, 2003.
- C. Linn and S. Debray. “Obfuscation of executable code to improve resistance to static disassembly”. In CCS ’03: Proceedings of the 10th ACM conference on Computer and communications security, pages 290–299, New York, NY, USA, 2003. ACM.
- F. Guo, P. Ferrie, and T.-C. Chiueh.” A study of the packer problem and its solutions”. In RAID ’08: Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection, pages 98–115, Berlin, Heidelberg, 2008. Springer-Verlag.
- M. Christodorescu, S. Jha, S. Seshia, D. Song, and R. Bryant. “Semantics-aware Malware Detection”. In IEEE Symposium on Security and Privacy, 2005.
- J. Kinder, S. Katzenbeisser, C. Schallhart, and H. Veith. “Detecting Malicious Code by Model Checking”. In Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2005.
- C. Kruegel, W. Robertson, and G. Vigna. “Detecting Kernel-Level Rootkits through Binary Analysis”. In Annual Computer Security Application Conference (ACSAC), 2004.
- http://en.wikipedia.org/wiki/Botnet

Index Terms

Computer Science

Keywords

Tracking