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 malware 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 miyachi, 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
  Extractor for Packed Executables”. In Proceedings of the 5th ACM Workshop on Recurring
  Malcode (WORM), 2007.
- Lorenzo Martignoni, Mihai Cristodorescu, and Somesh Jha. “OmniUnpack: Fast,
  Applications Conference (ACSAC), 2007.
- Boris Lau and Vanja Svajcer. Measuring virtual machine detection in malware using DSD
- Thomas Raffetseder, Christopher Kruegel, and Engin Kirda “Detecting System
  Emulators”
- Vasudevan, Yerraballi, “Cobra: Fine-grained Malware Analysis using Stealth
- Bayer, Kruegel, Kirda, “TTAnalyze: A Tool for Analyzing Malware”. In: 15th Annual
- 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”.
- Manuel, Egele Theodoor, Scholte Engine Survey on Automated Dynamic Malware Analysis
Techniques and Tools
- Honeynet Project & Research Alliance. “Know your Enemy: Tracking Botnets”.
- Michael Bailey, Jon Oberheide, Jon Andersen, Z. Morley Mao, Farnam Jahanian, Jose Nazario. “Automated Classification and Analysis of Internet Malware”

Index Terms

Computer Science

Keywords

Tracking