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
- Thomas Raffetseder, Christopher Kruegel, and Engin Kirda “Detecting System Emulators”
- Manuel,EgeleTheodoor, ScholteEngine 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