Abstract

Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Security analysts extensively use virtual machines to analyse sample programs and study them to determine if they contain any malware. Malware detection is again a crucial
aspect of software security. This paper is intended to help organizations understand the threats posed by malware and mitigate the risks associated with malware incidents. In addition to providing background information on the major categories of malware, this paper majorly focuses on Analysis Aware Malware also called as Split Personality Malware which checks for the presence of Malware Analysis tools and behaves in a benign manner thus escaping detection.

References

- Efficient Detection of Split Personalities in Malware”. In the Proceedings of 17th Annual Network and Distributed System Security Symposium (NDSS 2010), San Diego, February 2010

Index Terms

Computer Science Engineering and Technology

Keywords