Abstract

Now a days thousands of malware samples are received by anti-malware companies on daily basis. And these large numbers are send for analysis by a number of automated analysis tools. These tool automatically execute a program in a controlled environment and generate a report describing the program’s behaviour.

This research paper is a contribution towards the Dynamic Malware analysis. The aim is to provide the general malware features found in recent malware by performing dynamic malware analysis using cuckoo sandbox executed on Windows XP (SP3). This paper also discusses the detailed information about techniques & tools used in dynamic malware analysis.

References

12. Ulrich Bayer, Imam Habibi, Davide Balzarotti, Engin Kirda, and Christopher Kruegel “A View on Current Malware Behaviors”.

Index Terms

Computer Science Security

Keywords

Malware, Sandbox, Malicious.