Abstract

The subject of this work is the domain of automated malware analysis. Malware analysis can be done with two techniques: static analysis and dynamic analysis; the focus of this paper is the dynamic behaviour of malware.

Malware is any software which is designed specifically to cause damage to a computer or computer network. Numerous types of malware are developed every day causing a lot of damage to users, organizations or companies, therefore a need for automated applications which makes the analysis better and easier is essential.

In the first chapter we begin with a summary of information security and three of most of the important characteristics of information, continuing with the importance of cyber security and most common threats. The second chapter debut with a short history of malware and common types of malware. In the following chapter discusses three types of malware analysis: static, dynamic or behavioral and automated, which is a combination of the static and dynamic analysis. The fourth chapter presents applications already exploring the automated analysis of malware behaviour.

An original aspect of the thesis consists in developing and implementing the framework making possible the analysis of malware within a virtual environment. This application consists of a few tools which are examining malware behaviour by monitoring registry key and disk files changes.

This work is the result of my own activity. I have neither given nor received unauthorized assistance on this work.

OANCEA ALIN-ANDREI