الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

RAPPORT DU PROJET DE FIN D'ÉTUDES

Pour l'obtention du diplôme de

Poste Graduation Spécialisée en Sécurité Informatique

Etude sur l'analyse et la détection des malwares

Réalisé par:

- MEHENNAOUI Saber
- NAILI Ali

Devant le Jury :

Président :

- Mr HADJER Samir

- **Examinateurs :**

- Mr BOULEMTAFES Amine
- Mlle ZEGHACHE Linda

L'Encadreur

- Mr AMIRA Abdelouahab

Co-encadreur

- Mr DJEDJIG Nabil

Année Universitaire : 2017 /2018

Abstract

The malware is software that is deployed with a malicious intent, and designed to perform actions harmful to an information system and without the knowledge of its user. A malware can also be used to carry out attacks ranging from fraudulent access to a system, to its complete destruction, and can even generate profit. To counter this kind of threat, it becomes important to understand the behavior of malwares, their methods of infection and spread, their camouflage techniques, their malicious actions and their communications with the outside world. It is also very important to have the right tools and environments to perform and facilitate the analysis.

In this work, we are interested in the tools and techniques of analysis and detection of malwares. We present a state of the art of different types of malware, their methods of diffusion, dissimilarity and persistence. We present the different techniques used to analyze the functioning of malware, namely: static, dynamic and hybrid analysis, as well as malware detection techniques used to prevent infection of computer systems. In addition, we present the most used tools in the analysis of malware, classified by categories of analysis: static, dynamic or hybrid, and: manual or automatic, citing their advantages and disadvantages.

Also, we conducted an experimental part exploiting the "Cuckoo" sandbox to perform the automatic hybrid analysis of the famous Ransomware Wannacry. Finally, the analysis of the generated report shows that the information obtained reflects the behavior and malicious actions of this Ransomeware.

Sommaire