

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

• Examineurs :

- 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 Ransomware.

Sommaire

Résumé.....	4
Introduction générale.....	5
Chapitre I : Etat de l’art sur les différents types de malwares	
I.1 Introduction.....	8
I.2 Définition.....	8
I.3 Les Types de malwares.....	9
I.3.1 Les virus.....	9
I.3.2 Les chevaux de Troie.....	9
I.3.3 Les vers.....	10
I.3.4 Les publiciels (Adwares).....	10
I.3.5 Les portes dérobées (Backdoor).....	10
I.3.6 Les enregistreur de frappe (Keylogger).....	11
I.3.7 Les rançongiciels (Ransomwares).....	11
I.3.8 Les espionlogiciels (Spywares).....	11
I.3.9 Les rootkits.....	11
I.3.10 Les rogues.....	12
I.3.11 Les spams.....	12
I.3.12 Les bots.....	13
I.3.13 Les exploits.....	13
I.3.14 Les wabbits.....	13
I.3.15 Les hijackers.....	13
I.4 Méthodes de diffusion des malwares.....	14
I.4.1 Installation physique.....	14
I.4.2 La navigation sur des sites web mal conçus.....	14
I.4.3 Infections par supports amovibles.....	15
I.4.4 Les cracks et les keygens.....	15
I.4.5 Les faux codecs.....	15
I.4.6 Email et l’exécution d’une pièce jointe.....	16
I.4.7 Vulnérabilités logicielles.....	16
I.4.8 Les Roguewares, Les Faux Logiciels De Sécurité.....	16
I.4.9 Les Canulars ou Hoax.....	17
I.4.10 Les logiciels gratuits adwares.....	18
I.5 Méthodes de dissimulation et persistance.....	18
I.5.1 Persistance.....	18
I.5.2 Dissimulation.....	20
I.6 Conclusion.....	21
Chapitre II : Etat de l’art sur les différentes méthodes d’analyse et de détection des malwares	
II.1 Introduction.....	22
Objectif de l’analyse des malwares.....	22
II.2 Les methodes d’analyse des malwares.....	23
II.2.1 Analyse statique.....	23
II.2.1.1 Technique D'analyse Statique.....	24
II.2.1.2 Avantages De L’analyse Statique.....	28
II.2.1.3 Limites de l’analyse statique.....	29
II.2.2 Analyse Dynamique.....	29
II.2.2.1 Les techniques de l’analyse dynamiques des malwares.....	29
II.2.2.2 Environnements d’exécution de l’analyse dynamique.....	31
II.2.2.3 Avantages de l’analyse dynamique.....	32
II.2.2.4 limites de l’analyse dynamique.....	32

II. 2.3 Analyse hybride	32
II.3 Les méthodes de détection des malware	32
II.3.1 Méthode de détection par signature	32
II.3.2 Méthode de détection par Heuristique.....	33
II.3.3 La détection basée sur le comportement	33
II. 4 Les méthodes d’obfuscation des malwares	33
II.4.1 Obfuscation des chaines de caractères	33
II.4.2 Les Packers	33
II.4.3 Anti-virtualization	34
II.4.4 Anti Débogage	34
II.4.5 Obfuscation du code	34
II. 5 Conclusion	37
Chapitre III : Recensement et comparaison des outils d’analyse et de détection des malwares	
III.1 Introduction.....	38
III.2 Outils d’analyse statique.....	38
III.2.1 Détecteurs des Packers / Crypte.	38
III.2.1.1 PeiD	38
III.2.1.2 NPE File Analyzer.....	39
III.2.1.3 Detect It Easy.....	40
III.2.1.4 StudPE	41
III.2.1.5 CFF Explorer.....	41
III.2.1.6 PE Explorer.....	42
III. 2.2 Désassembleurs/Débogueurs.....	43
III.2.2.1 Les Désassembleurs.....	44
III. 2.2.2 Les Débogueurs.....	45
III.3 Outils d’analyse dynamique	49
III.3.1 Le Monitoring Du Malware Sur Un Ordinateur.....	49
III.3.1.1 La Surveillance Des Processus.....	50
III.3.1.2 Surveillance Du Registre.....	52
III.3.1.3 Le Monitoring Des Changements.	53
III.3.1.4 La Surveillance Du Réseau.	55
III.4 Outils d’analyse hybride.....	60
III.4.1 Le Bac a Sable Cuckoo(CuckooSandbox).....	61
III.4.2 Le Bac a Sable REMnux (REMnux Sandbox).....	62
III.4.3 Le Bac a Sable Limon (Limon Sandbox).....	64
III.4.4 Le Bac a Sable ZeroWine (ZeroWine Sandbox).....	65
III.4.5 FLARE VM (FlareVmware).....	66
III.4.6 Analyse Automatique en ligne	67
III.5 Conclusion.....	67
Chapitre IV : Expérimentation	
IV.1 Introduction.....	68
IV.2 Méthodologie Adoptée.....	68
IV.2.1 Description De La Méthode Et Le Choix De L’outil... ..	68
IV.2.1.1 le choix de l’environnement d’analyse.....	68
IV.2.1.2 2 Description du bac a sable Cuckoo.....	68
IV.2.1.3 Architecture et principe de fonctionnement.....	69
IV.2.1.4 Déroulement de l’analyse.....	70
IV.2.2 Description Du Malware Etudié.....	71
IV.2.2.1 malware Wannacry.....	71
IV.2.2.2 Mode de fonctionnement du Wannacry.....	71
IV.2.2.3 Comportement du ransomwarewannacry.....	72
IV.2.2.4 Statistiques sur le ransomware WannaCry.....	74
IV.3 Test Et Expérimentation.....	74

IV.3.1 L'environnement de l'analyse.....	74
IV.3.2 Installation Et Configuration Du Bac à Sable CUCKO	75
IV.3.2.1 La machine de base (hôte).....	75
IV.3.2.2 La Machine invité (Guest).....	79
IV.3.2.3 Configuration du Cuckoo.....	82
IV.4 Déroulement de l'analyse.....	84
IV.5 Analyse du rapport de l'analyse	88
IV.5.1 Analyse statique.....	88
IV.5.2 Analyse dynamique.....	92
IV.5.2.1 La surveillance des processus.....	93
IV.5.2.2 Points de démarrage automatique.....	94
IV.5.2.3 Activités au niveau du système de fichier.....	94
IV.5.2.4 Activités au niveau de la base des registres.....	95
IV.5.2.5 Trafic réseau.....	96
IV.5.2.6 Image mémoire.....	96
IV.5.2.7 Installation de Tor.....	96
IV.6 Conclusion.....	98
Conclusion générale & Perspectives.....	99