

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur de la Recherche Scientifique
Centre de Recherche en Information Scientifique et Technique



**Mémoire pour l'obtention du diplôme
de Post-Graduation Spécialisée en Sécurité Informatique**

Thème

Développement d'un Keylogger logiciel

Elaboré par:

HADIBY Walid

LEKAEL Hamza

Encadré par :

Mme. BENMEZIANE Souad

Soutenu devant le jury :

- **Mr. Dr. O. Nouali, Président**
- **Mr. Dr. D. Tandjaoui, Examineur**
- **Mr. A. Amira, Examineur**

- Février 2014 -

Remerciements

Nous remercions le bon dieu

Ce mémoire est le fruit d'un travail acharné au sein du CERIST et comme un tel travail nécessite la contribution de plusieurs personnes, nous profitons de cette occasion pour les remercier à travers ces quelques phrases.

Nous tenons tout d'abord à remercier notre promotrice Mme BENMEZIANE Souad pour la confiance qu'elle nous a témoignée en nous proposant ce sujet, sa disponibilité tout au long du projet, ses encouragements et sa patience, ses remarques et ses suggestions nous ont permis de finaliser ce document.

Nous exprimons toute notre profonde gratitude et nous remercions le personnel du service formation du CERIST, sans oublier tous les enseignants qui ont assuré notre formation.

Nous remercions aussi les membres du jury pour avoir bien voulu juger notre travail.

Sommaire

Introduction générale.....	01
----------------------------	----

Chapitre I Attaques informatiques

I.1 Introduction.....	03
I.2 Notions de sécurité informatique.....	03
I.2.1 Définition des concepts de sécurité.....	03
I.2.2 Enjeux de la sécurité des systèmes informatiques.....	04
I.3 Attaques informatiques.....	05
I.3.1 Définition d'une attaque.....	05
I.3.2 Motivations d'une attaque.....	05
I.3.3 Etapes d'une attaque.....	05
I.4 Classifications des attaques.....	06
I.4.1 Attaques actives.....	06
I.4.1.1 Craquage de mots de passe.....	06
I.4.1.2 Déni de service (DOS).....	06
I.4.1.3 Détournement de session (Spoofing).....	08
I.4.1.4 Débordement de tampon.....	09
I.4.1.5 Codes malveillants: Malwares.....	09
I.4.2 Attaques passives.....	11
I.4.2.1 Ecoute réseau (Sniffing).....	11
I.4.2.2 Scanning.....	11
I.4.2.3 Ingénierie sociale (Social-engineering).....	12
I.4.2.4 Hameçonnage (Phishing).....	12
I.4.2.5 Bounces de découverte.....	13
I.4.2.6 Enregistreurs de frappe (Key loggers).....	13
I.5 Conclusion.....	13

Chapitre II Keyloggers

II.1 Introduction.....	14
II.2 Définition d'un Keylogger.....	14
II.3 Usage d'un Keylogger.....	14
II.4 Dangers d'un Keylogger.....	15
II.5 Types des Keyloggers.....	16
II.5.1 Keyloggers Matériels.....	16
II.5.1.1 Avantages du Keylogger matériel.....	17
II.5.1.2 Inconvénient du Keylogger matériel.....	17
II.5.2 Keyloggers Logiciels.....	17
II.5.3 Comparaison entre Keylogger logiciel et Keylogger matériel.....	17

II.6	Mode de fonctionnement d'un Keylogger.....	18
II.7	Modes de diffusion d'un Keylogger..	18
II.8	Classes de propagation des frappes	18
II.9	Différentes zones d'insertion des Keyloggers.....	20
II.10	Principes de construction des Keyloggers.....	22
II.10.1	Installation d'un Browser Helper Object (BHO) avec Internet Explorer	22
II.10.2	Requête cyclique sur toutes les touches clavier et les cliques souris.....	22
II.10.3	Hooking	22
II.10.3.1	L'API Hooking : attaque en mode utilisateur (user-mode).....	23
II.10.3.2	SSDT Hooking : attaque en mode noyau (Kernel-mode).....	23
II.11	Méthodes de protection contre les Keyloggers	23
II.12	Conclusion.....	24

Chapitre III Conception du Keylogger

III.1	Introduction.....	25
III.2	Description du CFN-Keylogger +.....	25
III.3	Schéma conceptuel.....	26
III.4	Modules du CFN-Keylogger +.....	26
III.4.1	Module Enregistreur de Frappes.....	27
III.4.2	Module Capture.....	27
III.4.2.1	Capture d'écran, Webcam.....	27
III.4.2.2	Capture audio.....	27
III.4.3	Module Chiffrement.....	27
III.4.3.1	Chiffrement du fichier log	27
III.4.3.2	Chiffrement des fichiers images.....	28
III.4.4	Module Compression.....	28
III.4.5	Module Envoi	29
III.4.5.1	Envoi par email.....	29
III.4.5.2	Envoi par FTP	29
III.4.5.3	Envoi vers une Clé USB.....	29
III.4.6	Module Dissimulation	30
III.4.7	Module Auto destruction.....	30
III.5	Fichiers utilisés par le CFN-Keylogger+.....	31
III.5.1	Fichier DLL.....	31
III.5.1	Fichier de configuration.....	31
III.6	Fichiers générés par le CFN-Keylogger+.....	32
III.6.1	Fichier log.....	32
III.6.2	Fichiers de captures (écran, Webcam, audio).....	33
III.6.3	Fichier compressé à envoyer.....	34
III.7	Description du CFN-Keylogger+ Generator	34
III.8	Principe de fonctionnement du CFN-Keylogger +.....	35
III.9	Technique utilisée pour réaliser le CFN-Keylogger +.....	35
III.10	Conclusion.....	37

Chapitre IV Implémentation du Keylogger

IV.1 Introduction.....	38
IV.2 Outils et langage de programmation.....	38
IV.3 Présentation du CFN-Keylogger +.....	38
IV.3.1 Paramétrage du CFN-Keylogger+.....	38
IV.3.1.1 Paramètres Généraux.....	38
IV.3.1.2 Paramètres Visuels.....	41
A. Capture d'écran.....	41
B. Capture Webcam.....	42
IV.3.1.3 Paramètres Audio.....	42
IV.3.1.4 Paramètres Email.....	43
IV.3.1.5 Paramètres FTP.....	45
IV.3.1.6 Paramètres USB.....	46
IV.3.1.7 Paramètres Mot de passe.....	47
IV.3.1.8 Paramètres Camouflage.....	49
IV.3.1.9 Paramètres Destruction automatique.....	50
IV.3.1.10 Paramètres Log.....	51
IV.3.2 Génération du programme d'installation du CFN-Keylogger+	52
IV.3.3 Préparation et installation du CFN-Keylogger+.....	54
IV.3.4 Traitement, envoi et réception et des fichiers log et différentes captures	55
IV.3.5 Auto-destruction du CFN-Keylogger+.....	55
Conclusion générale.....	56
Bibliographie.....	57