

KEYLOGGER : DETECTION ET TRACES LAISSEES + ETAT DE L'ART

Projet réalisé par BLANC Nathanaël et OLSZEWSKI Alan

Dans le cadre de l'obtention du M2 Informatique Sécurités des Systèmes
d'Information

SOMMAIRE

INTRODUCTION	3
ETAT DE L'ART	4
CHOIX ET PRESENTATION DE REVEALER KEYLOGGER	10
DETECTION ET TRACES LAISSEES DU KEYLOGGER	13
CONCLUSION	15

I. Introduction

Dans le cadre de l'obtention de notre Master en Informatique Spécialité Sécurité des Systèmes d'Information, il nous a été demandé de réaliser un projet en Sécurité des services et des réseaux. Le thème de ce projet étant libre, nous avons choisi de travailler sur les KeyLoggers en tant qu'Hardware.

Cependant n'ayant pas eu assez de séances, nous n'avons pas pu nous arranger avec notre intervenant pour nous en procurer. C'est pourquoi, la majeure partie de notre projet va être théorique. Nous allons essayer par la suite de trouver un outil imitant un keylogger à installer sur une clé vierge nous appartenant.

Nous allons maintenant présenter les utilités et le fonctionnement d'un keylogger.

Un keylogger (Hardware) est un composant qui espionne l'utilisateur d'un ordinateur. Il est en charge de détecter les frappes de touches du clavier de l'ordinateur cible et de les enregistrer à l'insu de l'utilisateur. De nombreux types d'enregistrements sont disponibles, certains sont capables d'enregistrer les URLs visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, et même de créer une vidéo retraçant toute l'activité de l'ordinateur. Nous allons parler de tous ces différents keyloggers quand nous retracerons l'état de l'art.

Nous allons ensuite parler du choix de notre keylogger et des détections qu'on peut effectuer.

[...]

II. Etat de l'art

Nous allons désormais vous présenter les différents modèles de KeyLogger présents sur le marché.

Tout d'abord, il faut savoir que 2 types de KeyLogger existent : le logiciel (software) ou le matériel (hardware). Dans le premier cas, il s'agit d'un processus furtif dont le rôle est d'écrire les informations captées dans un fichier caché. Dans le second cas, il s'agit d'un dispositif (un câble, une clé) qui se branche entre la prise clavier de l'ordinateur et le clavier.

Voici ci-dessous l'exemple d'un KeyLogger (hardware) :



La plupart des keyloggers présents sur le marché se présente sous cette forme :



Un simple composant qui s'insère entre l'ordinateur et le clavier qui est compatible avec les systèmes d'exploitation Windows, Linux et Mac OS. De nombreux keyloggers peuvent enregistrer quelques dizaines de mégaoctets de données, voire quelques centaines.

Ces exemplaires de base coûtent entre 40 et 70 euros.



Voici une forme différente de keylogger : le SerialGhost.

« SerialGhost est un enregistreur de frappe de RS-232 et de bus série compact avec de nombreuses fonctions telles qu' horodatage, Ethernet et Wi-Fi. Il a 8 gigaoctets de mémoire flash disponibles en mode clé USB. En plus SerialGhost Wi-Fi est doté d'un émetteur-récepteur WLAN qui permet de le connecter à un Point d'Accès Wi-Fi local et d'envoyer des rapports par E-mail. »

Ce modèle de keylogger coûte entre 74 et 104 euros.



Voici l'AirDrive Serial Logger.

L'AirDrive Serial Logger est un enregistreur série et RS-232 compact, d'une longueur de seulement 61 mm (2,4 "), accessible avec n'importe quel appareil Wi-Fi tel qu'un ordinateur, un ordinateur portable, une tablette ou un smartphone.

D'autres versions améliorées sont également disponibles sur le marché.

L'AirDrive Serial Logger Pro qui est une version améliorée de l'AirDrive Serial Logger, avec des options de connectivité supplémentaires. Il fonctionne à la fois comme un point d'accès Wi-Fi et comme un appareil Wi-Fi, permettant des fonctionnalités telles que les rapports Email, l'horodatage et le streaming de données.

Enfin l'AirDrive Serial Logger Max qui est l'enregistreur de données le plus avancé de la gamme AirDrive Serial Logger, avec toutes les fonctionnalités de la version Pro, enrichie d'une mémoire interne de 8 Go disponible comme clé USB haute vitesse (480Mbps).

D'autres équipements sont également disponibles :



Voici le MorphStick Keyboard Tap 2 Ethernet. C'est un périphérique réseau compact, capable de convertir des données de clavier, de lecteur de code-barres ou de souris USB en paquets Ethernet. Il se branche sur une connexion USB entre l'ordinateur et le périphérique USB, capture les trames de données transmises et les envoie en tant que datagrammes UDP dans un format configurable par l'utilisateur.

Comme le modèle précédent, il existe des versions avancées.

Le MorphStick Keyboard Host 2 Ethernet est une variante de la version Tap, qui ne nécessite pas d'ordinateur pour que le clavier ou le lecteur de code-barres fonctionne. Il contient un hôte USB intégré, qui interroge le périphérique USB connecté pour les données, simplifiant ainsi la configuration et réduisant le nombre de câbles. Le clavier MorphStick Ethernet 2 fonctionne dans le sens opposé, simulant un clavier USB ou une souris USB à partir de données UDP entrantes via Ethernet. La source des données UDP peut être un MorphStick Keyboard 2 Ethernet ou des données générées à partir d'un périphérique réseau ou d'un ordinateur.



KeyGrabber Wi-Fi Premium est un keylogger sans fil et est équipé de la technologie la plus récente : deux microprocesseurs performants, pile TCP/IP complète, transceiver WLAN et 8 gigaoctets de mémoire Flash. Ce modèle possède la fonction de connexion Internet à distance. Ce keylogger sans fil se connecte à un Point d'Accès Wi-Fi local et il envoie des E-mails contenant les données de frappe enregistrées. En plus, grâce à TCP/IP, on peut se connecter à ce keylogger à tout moment et à distance pour voir le fichier journal enregistré.



Ce « keylogger » réalise des captures d'écran en mode furtif et les sauvegarde comme fichiers JPEG dans une mémoire flash de 8 gigaoctets. Ce vidéo-logger se branche à la sortie DVI, VGA ou HDMI de la carte graphique. Il commencera alors automatiquement à réaliser des captures d'écran presque toutes les secondes. L'attaquant passe alors au mode clé USB pour voir les captures enregistrées. L'appareil s'affichera alors comme disque amovible contenant des fichiers JPEG. Cet équipement est l'unique appareil de ce type disponible sur le marché.



« Ce keylogger matériel modulaire [...] est destinée à être installée à l'intérieur d'un clavier. Profil bas et connecteurs universels 2.5 mm garantissent la compatibilité avec tout clavier USB et PS/2. Après l'installation à l'intérieur du clavier, cet enregistreur de frappe est complètement invisible pour les yeux et pour des logiciels. »

Voici ci-dessous un schéma pour montrer où se place cet équipement :



Et enfin, il y a le KeyGrabber MultiLogger :



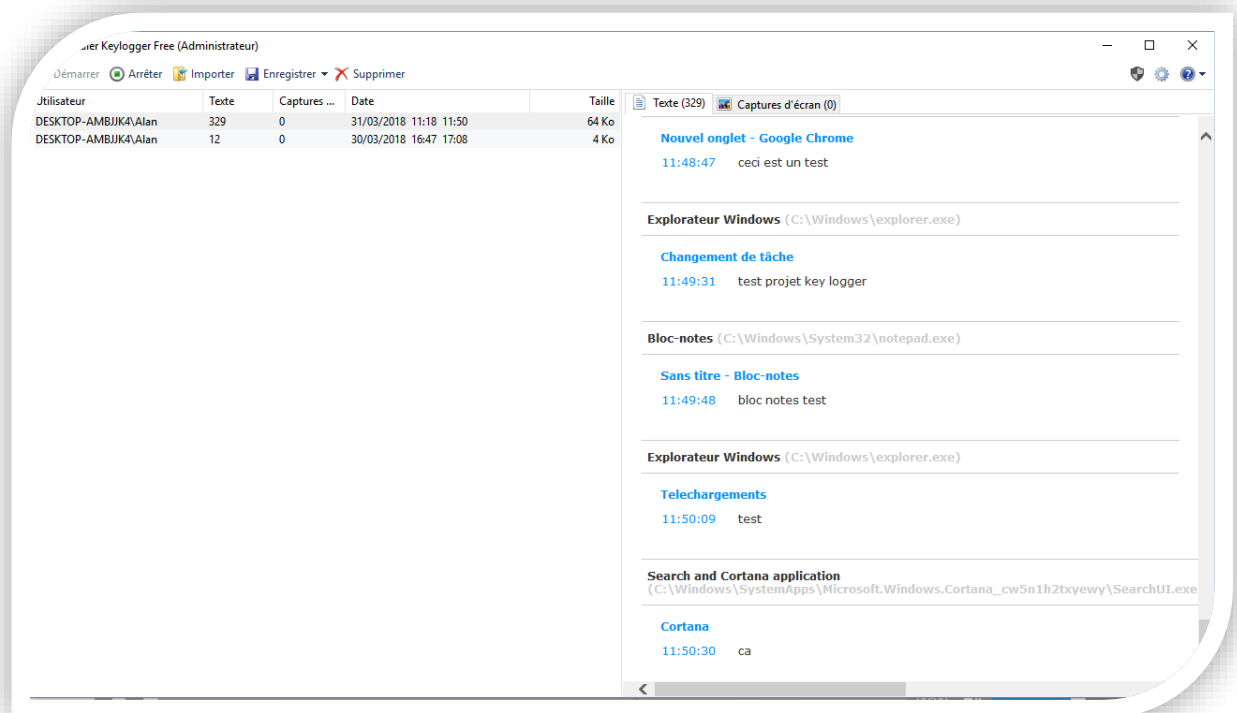
C'est un enregistreur de frappe multicanal. Il peut surveiller jusqu'à 8 claviers et enregistrer les données dans la mémoire flash incorporée. Les données enregistrées peuvent être envoyées en flux continu en temps réel via Ethernet à toute adresse IP souhaitée. Il ne requiert ni pilote ni logiciel.

Voilà un petit résumé de tous les différents keyloggers qui sont présents sur le marché. Leur prix varie beaucoup cependant le bas de gamme reste très abordable pour tout débutant (une cinquantaine d'euros). Ceci est une liste non exhaustive, il en existe encore de nombreux modèles tels que des câbles mais

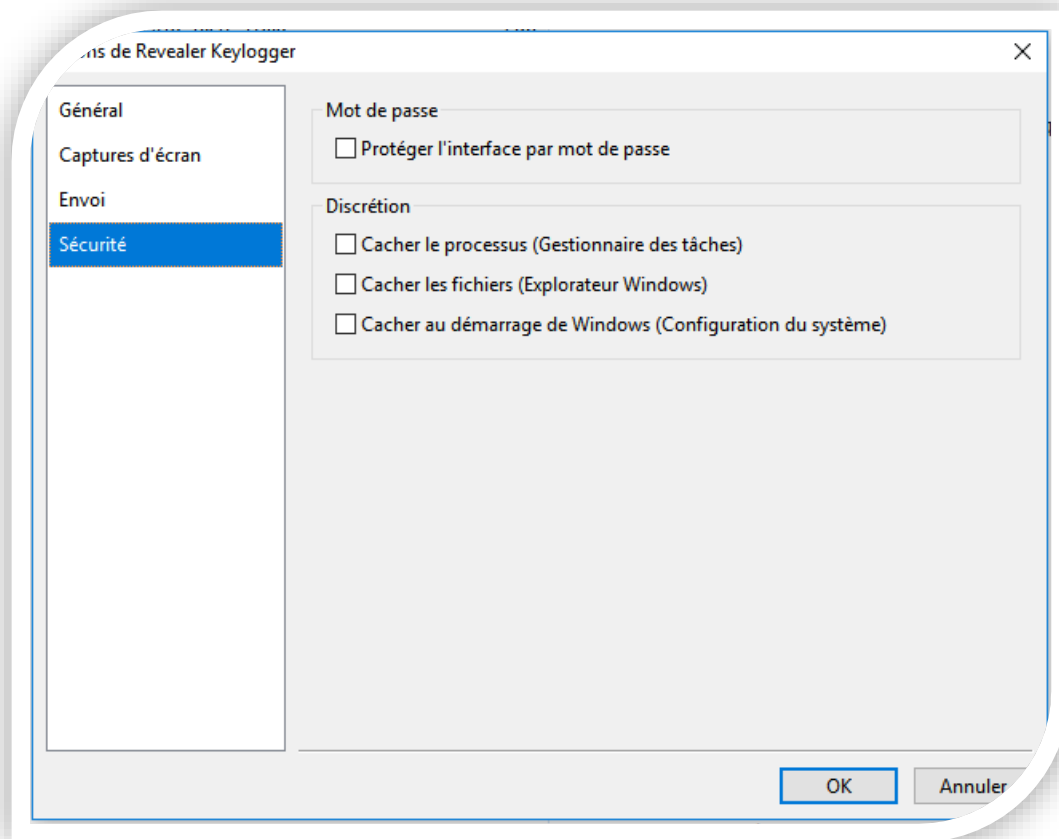
III. Choix et présentation de Revealer Keylogger

Comme dit dans l'introduction, nous avons cherché un moyen pour créer notre propre keylogger. Pour ce faire, nous avons essayé beaucoup d'outils à installer sur notre propre clé USB. Nous avons fini par nous pencher sur l'outil Revealer Keylogger.

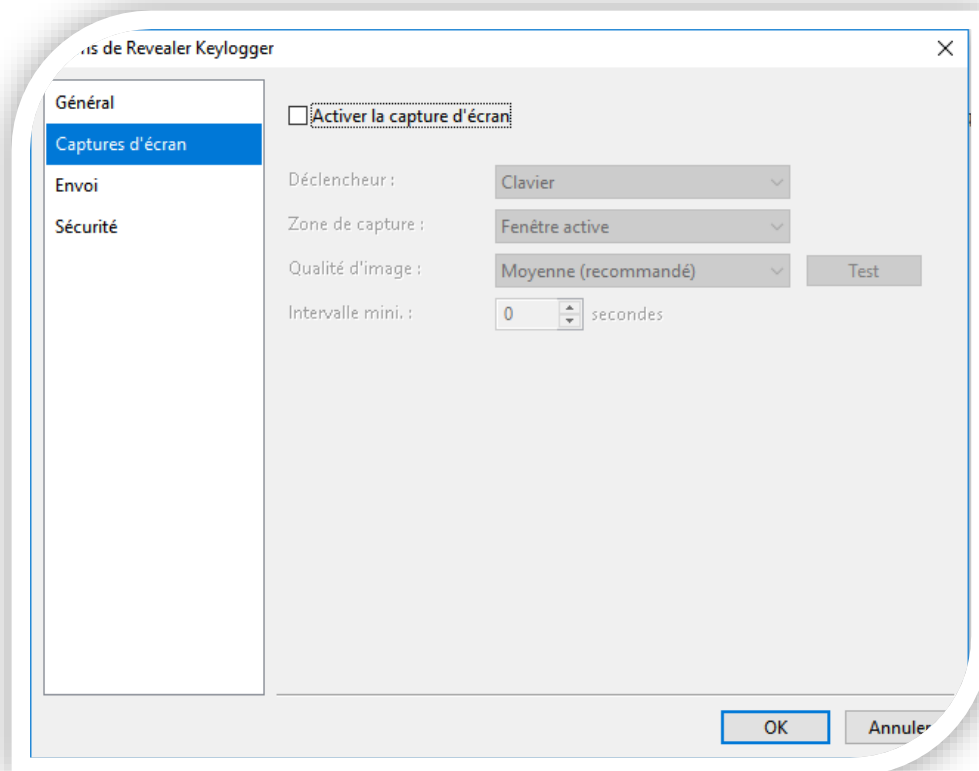
Revealer Keylogger est payant mais possède une version gratuite. La version payante contient des fonctionnalités très intéressantes que la version gratuite ne propose pas.



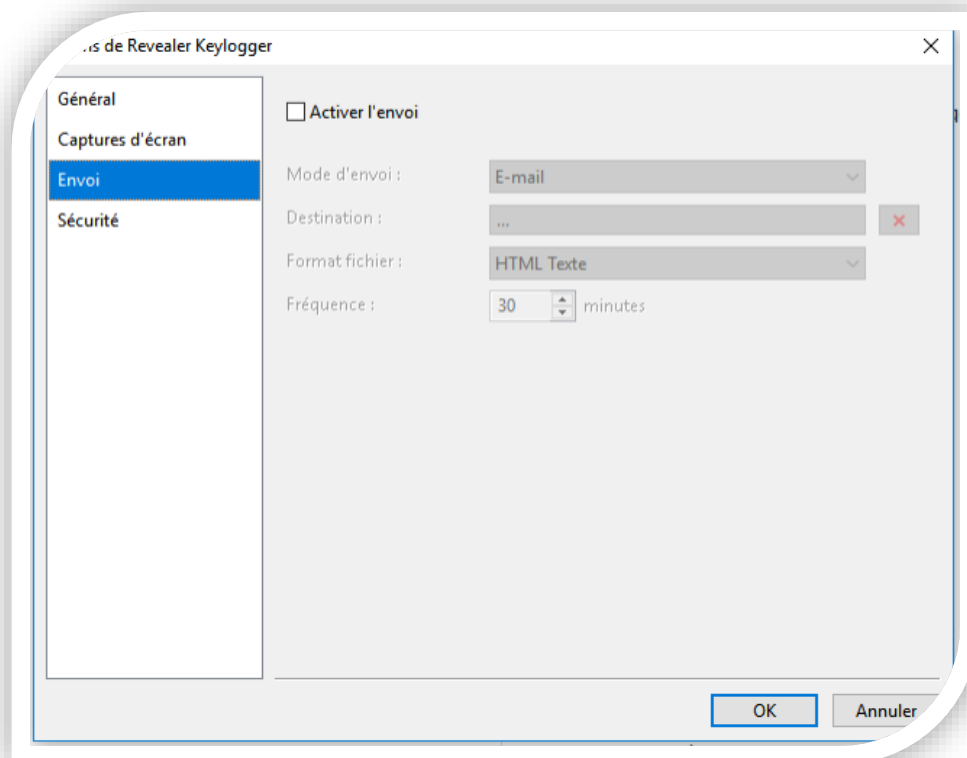
Voici la manière dont l'interface de l'outil se présente. Sur la partie de gauche, plusieurs journaux se présentent, ce sont plus précisément les différentes sessions d'enregistrement du keylogger. Le détail du journal choisi se trouve sur la droite. Il se découpe par ordre chronologique et dans lequel on peut voir l'application utilisée et les touches sur lesquelles l'utilisateur a appuyé.



Voici les options du keylogger. Dans l'onglet sécurité, plusieurs méthodes s'offrent à nous pour que le keylogger soit presque invisible. Ces méthodes ne concernent que la version payante, nous n'avons malheureusement pas pu les essayer. Nous verrons par la suite qu'un keylogger n'est pas invisible, il laisse des traces qu'un utilisateur peut voir.



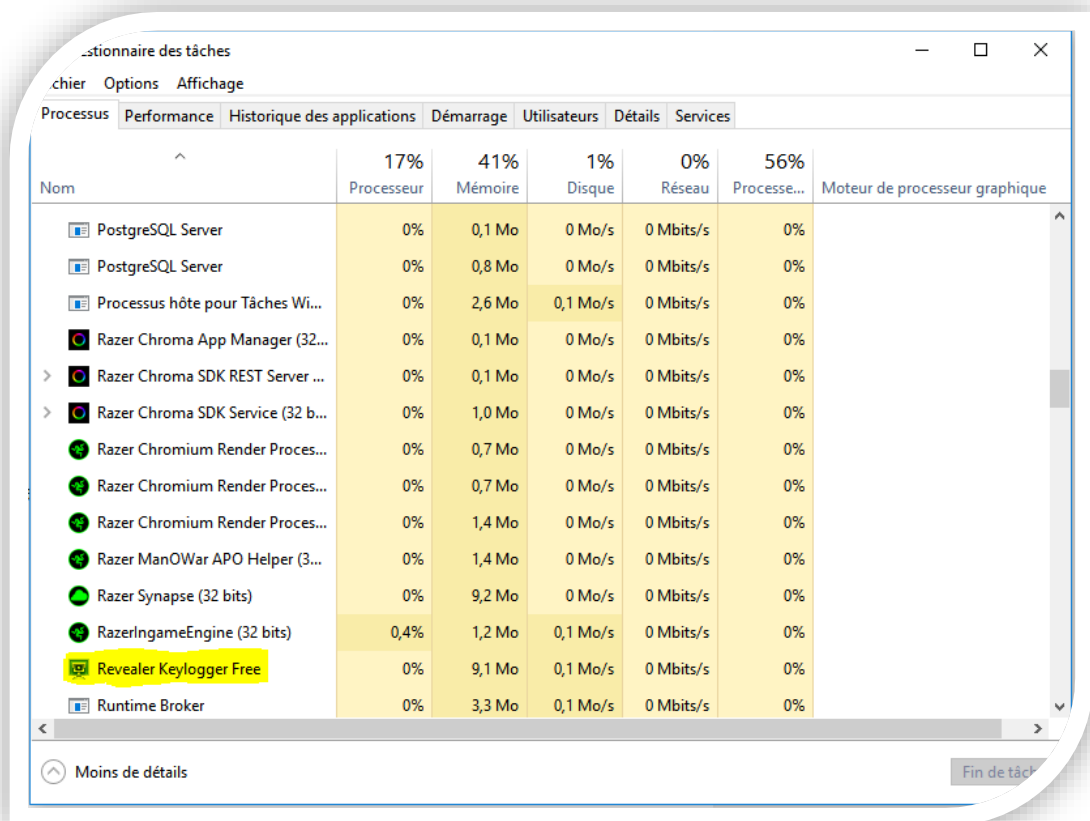
D'autres options sont également disponibles dans la version payante telles que les captures d'écran à tout moment ou encore l'envoi des enregistrements par mail.



IV. Détection et traces laissées du KeyLogger

1. Gestionnaire des tâches

Tout d'abord, tout simplement nous pouvons distinguer le keylogger dans les processus en arrière-plan dans le gestionnaire des tâches. Même si le keylogger n'est pas ouvert et n'est pas visible aux yeux de l'utilisateur, celui-ci est visible dans les processus.



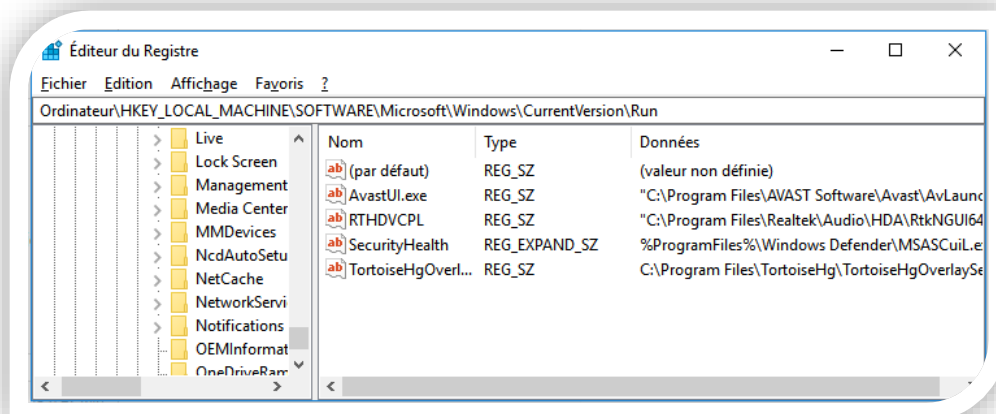
The screenshot shows the Windows Task Manager window with the 'Performance' tab selected. The window title is 'Gestionnaire des tâches'. The 'Processus' tab is active, showing a list of running processes. The columns are: Nom, 17% Processeur, 41% Mémoire, 1% Disque, 0% Réseau, 56% Processeur graphique, and Moteur de processeur graphique. The process 'Revealer Keylogger Free' is highlighted in yellow.

Nom	17% Processeur	41% Mémoire	1% Disque	0% Réseau	56% Processeur graphique	Moteur de processeur graphique
PostgreSQL Server	0%	0,1 Mo	0 Mo/s	0 Mbits/s	0%	
PostgreSQL Server	0%	0,8 Mo	0 Mo/s	0 Mbits/s	0%	
Processus hôte pour Tâches Wi...	0%	2,6 Mo	0,1 Mo/s	0 Mbits/s	0%	
Razer Chroma App Manager (32...	0%	0,1 Mo	0 Mo/s	0 Mbits/s	0%	
> Razer Chroma SDK REST Server ...	0%	0,1 Mo	0 Mo/s	0 Mbits/s	0%	
> Razer Chroma SDK Service (32 b...	0%	1,0 Mo	0 Mo/s	0 Mbits/s	0%	
Razer Chromium Render Proces...	0%	0,7 Mo	0 Mo/s	0 Mbits/s	0%	
Razer Chromium Render Proces...	0%	0,7 Mo	0 Mo/s	0 Mbits/s	0%	
Razer Chromium Render Proces...	0%	1,4 Mo	0 Mo/s	0 Mbits/s	0%	
Razer ManOWar APO Helper (3...	0%	1,4 Mo	0 Mo/s	0 Mbits/s	0%	
Razer Synapse (32 bits)	0%	9,2 Mo	0 Mo/s	0 Mbits/s	0%	
RazerIngameEngine (32 bits)	0,4%	1,2 Mo	0,1 Mo/s	0 Mbits/s	0%	
Revealer Keylogger Free	0%	9,1 Mo	0,1 Mo/s	0 Mbits/s	0%	
Runtime Broker	0%	3,3 Mo	0,1 Mo/s	0 Mbits/s	0%	

2. Provenance d'un keylogger

Si le keylogger est de type client/serveur et est connecté en TCP, nous pouvons analyser l'entête des trames envoyées depuis le pc de l'utilisateur. Si l'envoi des captures se fait par mail, il se peut que nous puissions voir seulement l'adresse de messagerie du serveur auquel est envoyée l'information. Pour cette méthode, nous pouvons utiliser un simple analyseur de trames tel que WireShark.

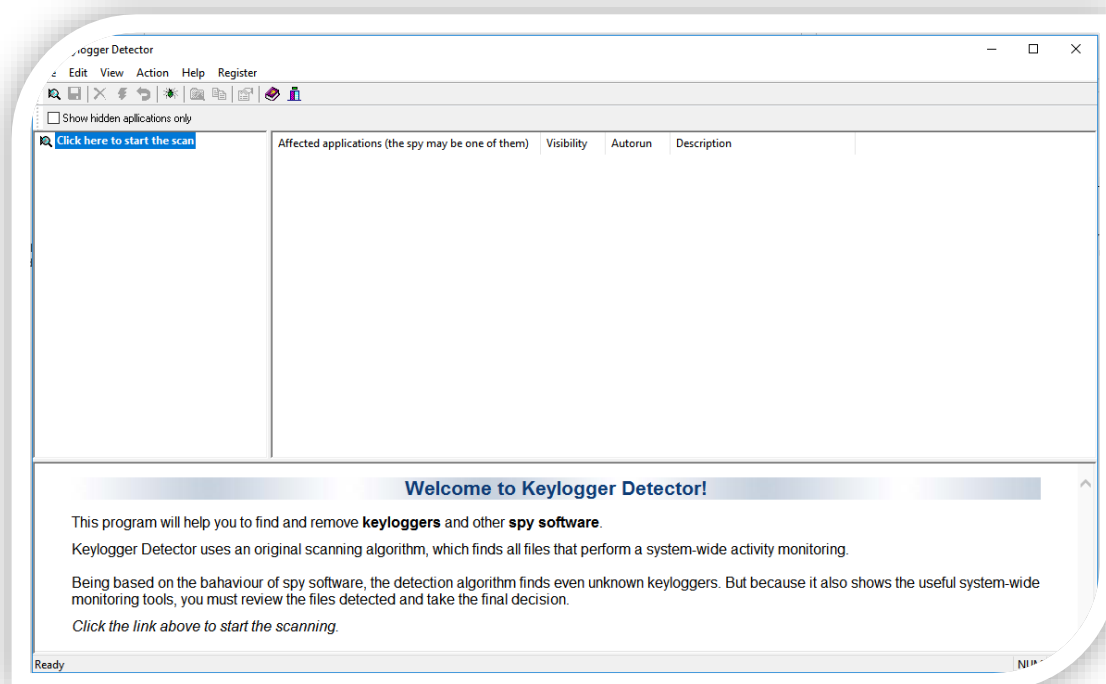
3. Vérification des registres



Dans l'éditeur de registre, nous pouvons retrouver les différents programmes s'exécutant au démarrage de Windows. Le chemin HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run nous montre ces différents programmes. Si un keylogger s'exécute au démarrage de l'ordinateur, il pourrait être affiché ci-dessus.

4. Logiciel de détection de keylogger

Il existe également des logiciels qui permettent de vérifier l'existence de keylogger et de les supprimer. On peut citer par exemple l'application Keylogger Detector qui repère les keyloggers. Si le logiciel (keylogger) est récalcitrant à la désinstallation, on peut forcer la désinstallation avec l'application IOBit Installer.



V. Conclusion

Pour conclure, on peut remarquer qu'il existe énormément de modèles différents de keyloggers. Nous n'avons pas réussi à tous les répertorier. Il existe également des anti-keyloggers qui « cryptent » les touches avant que le keylogger y ait accès. Ces programmes sont malheureusement lourds et peu utilisés. Parmi ceux-là on peut noter le fameux Keyscrambler.

De nombreuses méthodes existent pour « contrer » (détecter) ces keyloggers. Nos recherches, étant théoriques que pratiques, n'ont fait affaire que de quelques méthodes puisque nous n'avons pas réussi à nous procurer un réel keylogger.

Ce projet a été très intéressant pour nous, puisque nous avons réussi à étendre nos connaissances sur le sujet.