

Le Keylogger

Pré-Requis

Une machine virtuelle Debian9

Avoir des connaissances de base dans l'utilisation du langage Python.

- Il ne s'agit pas d'un cours de Python !

Ce programme n'est qu'une base de travail que vous pourrez par la suite enrichir à votre convenance.

Il est interdit d'utiliser ce type de programme sur un système dont vous n'êtes pas propriétaire ou pour lequel vous n'avez pas reçu les autorisations.

Qu'est-ce qu'un KeyLogger ?

Un keylogger, c'est un " enregistreur de touches «

Autrement dit, un spyware capable de détecter les frappes sur le clavier de votre ordinateur et de les mémoriser. Le tout, sans que vous le sachiez.

Il permet donc à des cyber-criminels de mettre à jour vos identifiants et codes d'accès sur vos comptes privés ou professionnels.

Les keyloggers matériels

Se présentent sous forme de petit dispositif (câble, boîtier, adaptateur, etc...) intercalé entre le clavier et l'ordinateur.

Facilement détectable !



Les keyloggers logiciels

Programme exploitant une fonction du système pour surveiller toutes les frappes du clavier.

Certains peuvent même aller jusqu'à s'attaquer au noyau du système, gérant les communications entre les logiciels et les périphériques.

Ils peuvent intercepter toutes les informations en provenance du clavier mais également de la souris.

De plus, ils sont programmés pour être invisibles, indétectables et se lancer pendant le démarrage du système d'exploitation.

Zeus, un keylogger tristement célèbre

L'un des keyloggers les plus célèbres s'appelle " Zeus ".

Il était paramétré pour s'activer dès que l'ordinateur accédait à un site appartenant à une liste prédéfinie dont faisaient partie de grands noms comme eBay, PayPal, Amazon, etc.

Il enregistrerait alors les noms des utilisateurs, les mots de passe, les numéros de compte et toutes les informations sensibles.

Plusieurs millions de dollars auraient ainsi été détournés.

S'en prémunir !

Contrairement à ce qu'on pense, ils sont très souvent installés sur les ordinateurs « publics » comme dans les aéroports, les cybercafés, les hôtels, etc...

Evitez d'installer des logiciels dont vous ne connaissez pas la provenance.

Maintenez constamment à jour tous vos logiciels et votre système d'exploitation.

Notre code

Le code que nous allons créer va nous permettre de capturer toutes les touches tapées au clavier par l'utilisateur sur un système Linux Debian.

Les touches capturées seront stockées dans un fichier de log préalablement défini.

Nous utiliserons pour ce faire le module : **pyxhook**.

- http://pyhook.sourceforge.net/doc_1.5.0/