



Les keylogger ou enregistreur de frappes clavier

Les keylogger (enregistreur de frappes clavier en français) sont des logiciels ou équipements matériels qui permettent d'enregistrer les frappes claviers.

Puis ces dernières sont ensuite transmises au pirate.

Le but étant d'obtenir des informations comme les mots de passe durant la saisie sur vos applications telles que [les navigateurs WEB](#).

Cet article explique un peu le fonctionnement et donne quelques programmes de protection contre les keylogger (Anti-Keylogger).



Principe des keyloggers

Les keylogger sont donc des dispositifs qui permettent d'enregistrer les frappes claviers.

Nous distinguerons les keyloggers logiciels, matériels.

Keyloggers de type logiciel

Il existe divers keyloggers, comme des keyloggers commerciaux , c'est à dire des logiciels vendus par des sociétés.

Mais aussi des keylogger liés à des malwares.

N'importe qui peut en acheter... un patron qui souhaite

surveiller son employé, ou un mari/femme.

Et puis, il y a [les logiciels malveillants](#).

En règle générale, [les trojans](#) de type Stealer, qui souhaite voler des données et autres informations contenues dans l'ordinateur possède des fonctionnalités de keylogger.

Ainsi, la plupart des [Trojans RAT](#) proposent ces fonctionnalités.

Par exemple, l'article suivant décrit un de ces keylogger : [iSpy Keylogger](#)

La vidéo suivante montre un Trojan RAT en action et la partie keylogger :

Fonctionnement des keyloggers logiciels

En général, le keylogger enregistre les frappes claviers dans un journal.

Ce journal peut-être récupérés par le pirate ou être envoyé automatiquement.

Enfin, le pirate peut interroger le keylogger en temps réel.

Il existe différentes méthodes de fonctionnement des keyloggers sur [Windows](#) pour récupérer les frappes claviers.

Ce qu'il faut comprendre avant tout, c'est que Windows gère les frappes, puisque le système d'exploitation offre une interface entre la partie logicielles et le matériel.

Un keylogger peut placer un hook, c'est à dire un crochet sur des fonctions de clavier, ainsi, les frappes claviers passeront par le keylogger qui pourra les enregistrer avant de les transmettre « normalement ».

Le but est d'intercepter les appels de fonctions Windows de

clavier afin que celles-ci passent par le keylogger.

Ce hook peut se faire de manière globale ou injecter tous les processus afin de les surveiller.

Enfin il est aussi possible de modifier l'adresse de certaines fonctions (API) de librairie user32.dll.

Ainsi quand un processus appelle ce dernier, c'est en réalité le keylogger qui sera contacté.

Ce dernier peut alors falsifier les résultats.

Enfin une dernière méthode différente des crochets consistent à appeler à intervalles réguliers et très courts qui donnent le statut des touches.

Il est alors possible de savoir quand une touche est pressée.

Ce sont ici des méthodes au niveau userland, c'est à dire au niveau des processus de [Windows](#).

il est aussi possible de créer des keylogger kernel-mode, c'est à dire à des niveaux plus bas de [Windows](#).

Cela nécessite de charger [un driver \(fichier .sys\)](#), là aussi afin de placer des hooks sur des fonctionnalités de Windows (API).

On peut aussi modifier (patch) un drivers légitime de Windows afin d'altérer son fonctionnement et enregistrer les appels claviers.

Exemple de Keylogger

Voici un exemple d'enregistreur de frappes clavier.

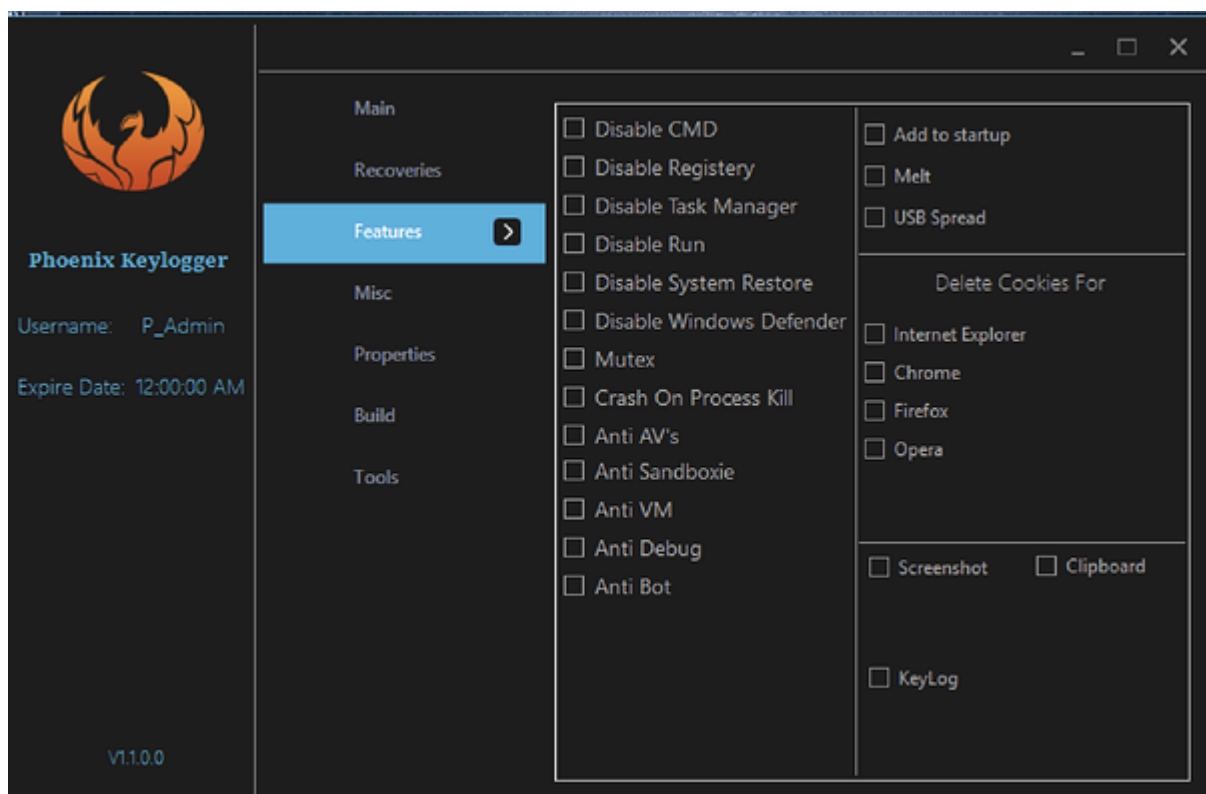
Il s'agit ici de bien comprendre qu'un keylogger possède souvent d'autres fonctions pour voler des données.

L'étude porte sur [Phoenix par CyberReason](#).

Les fonctionnalités du keylogger :

- Enregistre les frappes clavier + voler les données du presse papier de Windows
- Effectue [des captures d'écran](#)
- Vol les mots de passe de logiciel comme : [navigateurs WEB](#), client mails, client FTP, logiciel de discussions.
- Envoie les données par SMTP, FTP et Telegram
- Possibilité de télécharger et installer d'autres malwares
- Fonction pour tuer les antivirus
- Peut se propager par médias amovibles « [Virus USB](#) »
- Anti-debugging et Anti-VM Features. Il s'agit de détecter la présence d'une [machine virtuelle](#) et interdire l'installation du malware pour une étude par des chercheurs en sécurité.

Phoenix utilise une méthode commune de raccordement des événements de clavier (hook) pour son enregistrement au clavier. Il utilise une fonction API Windows SetWindowsHookExA pour mapper les touches sur lesquelles vous avez appuyé, puis les associe au processus correspondant.




Ainsi, le malware possède des fonctions de stealer puisqu'il peut voler les mots de passe.

En outre il peut servir de tremplin pour installer d'autres malwares.

Il est vendu sur des forums privés avec une documentation et un support.


Voici les prix.




Illusion
Whatever you are, be a good one
55




Posts:	314
Threads:	18
B Rating:	39 0 0
Popularity:	178
Bytes:	1,089
Game XP:	564



1 MONTH
SUBSCRIPTION \$14.99



3 MONTHS
SUBSCRIPTION \$34.99



LIFETIME
SUBSCRIPTION \$78.99

PACKAGE INCLUSION




Any packages you choose will be included all of this awesome benefits.

Documentation

All Future Updates

Unlimited Stub Build

PAYMENT METHODS



Keylogger matériel

Les keyloggers matériel se présentent sous la forme d'une prise USB entre le clavier et l'ordinateur, ainsi, le petit boîtier peut intercepter les frappes claviers. Celui-ci peut être récupérés ultérieurement par le pirate ou les données peuvent être transmises par clé USB.



Anti-Keylogger

Il existe des programmes dit Anti-Keylogger avec des approches différentes.

Bien entendu, on parle ici d'Anti-Keylogger pour [Windows](#).

Vous trouverez un aperçu d'anti-keylogger gratuit sur la page suivante : [Les anti-Keylogger pour se protéger des keyloggers](#)

Pensez que cela ne protège pas de tout car comme l'explique cet article, les keylogger ont souvent des fonctions pour voler les mots de passe.

Ainsi même si vous protégez des frappes claviers, l'attaquant peut récupérer les mots de passe de vos navigateurs WEB ou autres.

Conclusion

Les keyloggers sont des menaces permanentes puisqu'ils font parti de l'arsenal utilisés par les [les trojans](#) de type Stealer.

Vous pouvez installer, si vous le souhaitez un anti-Keylogger qui fait le boulot.

Personnellement, je ne suis pas pour les protections spécifiques (anti-exploit, anti-keylogger, [anti-ransomware](#)).

Le plus simple étant de ne pas infecter l'ordinateur, ce qui n'est pas très compliqué au final.

En effet si on est un tant soit peu sérieux sur la toile et si on suit quelques recettes pour sécuriser son ordinateur.

De manière générale, pour sécuriser ses comptes en ligne, vous pouvez lire ce tuto : [Comment protéger ses comptes internet](#)

A lire : [Comment sécuriser son ordinateur ?](#)