Guide d'utilisation de la RubberDucky

Auteurs :
Liam COURSODON
Mathis LEJEUNE
Kamel LOUNIS
Mohammed Amine MAFTOUH

Mai 2023

1 Présentation

Ce projet a été réalisé par 4 étudiants d'IMT Atlantique Brest sous l'encadrement de VINCENT Johanne, LOHR Christophe, VATON Sandrine et SAILHAN Françoise, enseignants à l'IMT. Ce guide d'utilisation détaille l'architecture et le fonctionnement de la RubberDucky pour Ubuntu et complète le *readme* associé à ce projet.

2 Contenu de l'archive

Dans cette archive se trouve plusieurs fichier :

- README.md : description du répertoire et consignes d'utilisation
- client : dossier faisant office de l'ordinateur cible. On y retrouve le script cle.py qui simule l'insertion de la clé dans l'ordinateur.
- serveur : dossier contenant le code du virus qui doit être hébergé sur le serveur ainsi qu'un fichier python serveur.py qui sert à simuler un serveur en local. On retrouve aussi les fichiers suivant :
- data.txt : fichier de configuration du virus détaillé dans la partie 4
- download.py : 1er fichier téléchargé par la clé usb dont le role consiste à télécharger le reste de façons plus rapide et optimal.
- sousvirusU.py, virus.py, compteur.py et popup.py sont les script du virus téléchargé par download.py. virus.py étant le script principal.

3 Installation

En se plaçant dans le répertoire du projet :

- Pour télécharger le projet via github:

```
git clone https://github.com/LiamCrsd/RubberDucky
cd RubberDucky
git checkout serveur
```

- Pour télécharger et installer les librairies et le logiciel :

```
sudo pip install -r requirements.txt
```

- Configurer l'url du serveur

Dans le dossier serveur il faut veillez à modifier le variable "url" dans le fichier "download.py" afin qu'elle correpsonde à l'url du serveur. Si le serveur est hébérgé localement l'url est :

```
localhost:8000
```

4 Utilisation

4.1 Lancement du serveur

En se plaçant dans le répertoire du projet :

- Pour lancer le serveur :

```
cd serveur
python3 serveur.py
```

4.2 Lancement du virus

- Avec la clé :

Branchez la clé
Attendez
Si rien ne se passe essayez de changer la clé de port
Recommencez jusqu'à que le virus s'éxécute

- Avec cle.py :

```
python3 client/cle.py
```

Ce script simule la cle.

4.3 Arrêter le virus

- Dans le fichier data.txt :

Dans le répertoire à partir du quel le virus est éxécuté, retrouvez le fichier "data.txt" et modifier la 1ere ligne de sorte à avoir "virus actif : 0" Vous pouvez aussi l'ouvrir dans un des invité de commande ouvert en faisant :

```
nano data.txt
```

modifier "virus actif : 0" et sauvegarder en faisant

```
Ctrl + X
Y // et appuyer sur entrer
```

- En forcant l'arret du processus originel :

Retrouvez la premiere fenetre ouverte, et forceant l'arret Cela arretera le virus et fermera toutes les autres fenetres.

- Avec le "mot de passe" :

En regardant dans data.txt on peut aussi remarquer qu'il existe un mot de passe (dans notre cas "motdepass")// De plus en regardant le code on remarque qu'il verifie si mdp.txt correspond au mot de passe il suffit de faire cette commande pour arreter le virus :

```
echo motdepasse > mdp.txt
```

4.4 Parametre le virus

Dans le fichier data.txt il est possible de faire varier de nombreux parametre du virus pour l'adapter à votre utilisation

- Virus actif :

Vérifie simplement si le virus est actif avec un boolean (1 = true, 0 = false)

- Nb terminaux :

Détermine le nombre de terminaux à ouvrir au démérage du virus (le nombre de fenetre)

- Compteur :

Cette variable permet de suivre l'avancement du compteur simulant un hack

- Tic compteur :

Correspond au nombre de seconde entre chaque tic d'avancement du compteur celui ci prennant 40 tic pour se completer.

- Mdp :

Mot de passe du virus à ecrire dans mdp.txt pour l'arreter.