***Documentation projet Spider***

**1/ Le client**

Le client (ou infecté), est un programme en C++ pouvant enregistrer les frappes au clavier/clics à la souris effectués et les transmettre au serveur via le protocole TCP/IP. De plus, il permet de récupérer et décrypter les mots de passes de Google Chrome et de Opera grâce à la libraire SQLite3. L'envoie des données au serveur est cryptés grâce à la librairie OpenSSL avec une clé de 256 bits. Le programme modifie le registre pour pouvoir s’exécuter automatiquement à chaque redémarrage de l’ordinateur. L’architecture du client permet une adaptation simple du code sur une machine Linux.

**2/ Le serveur**

Le serveur reçoit les informations du client sous la forme de chaîne de caractères cryptés. Il les décrypte puis les stocks dans un fichier. Chaque client à son propre ficher avec comme nom : le nom de l’utilisateur infecté. Deux types de fichier existent : les « spider » contenant les touches frappées, et les « password » contenant les mots de passes des navigateurs Web des utilisateurs. Le contenu des fichiers est mis à jour en temps réel sur l’interface graphique.

Le format pour les chaines correspondant aux touches frappées est le suivant :

* Un header comprenant le nom de l’utilisateur
* L’horaire à laquelle la touche a été frappée
* Le nom de l’exécutable ayant le focus au moment où la touche a été frappée
* La chaine contenant les touches frappées

Chacune des informations du header est séparée par le charactère spécial « # ». Chaque touches frappées est séparée par le charactère spécial « [ ». Ce qui peut donner par exemple :

*anonymous#10/9/2017 23:42#chrome.exe#[j[‘[e[c[r[i[s*

Le format pour les chaines correspondant aux mots de passes des navigateurs Web est le suivant :

* Un header comprenant le nom de l’utilisateur
* Le lien du site ou le mot de passe est enregistré
* Le login de la personne
* Le mot de passe

Chacune des informations du header est séparée par le charactère spécial « # ». Ce qui peut donner par exemple :

*anonymous#https://www.facebook.com#fake@example.com#motdepassedu13*

**3/ Interface graphique**



L'interface graphique se présente sous la forme de 3 box, celle en haut à droite permet de choisir l'infecté dont nous souhaitons voir les mots de passes enregistrés pour les navigateurs Web (box inférieur droite) ainsi que les frappes au clavier / clics à la souris (box gauche).

Lorsqu'un utilisateur infecté est sélectionné, le serveur parcourt les fichiers de l'utilisateur correspondant et rempli les box grâce à ces informations, ensuite une fois l'utilisateur sélectionné, les informations arrivent en temps réel via l'envoi du serveur, les boxs de textes sont ainsi actualisés.