Observation de l'activité de l'outil de prise de contrôle à distance JSpy avec Sysmon

projet réalisé par

Aurélien MANGIN
Hugo CZEKALA

dans le cadre du Master 2 Sécurité des Systèmes d'Information

SOMMAIRE

Table des matières

INTRODUCTION

Dans le cadre du cours sur les malwares, nous avons décidé de nous attarder de manière plus précise sur les chevaux de Troie.

Nous avons donc réalisé une étude sur ce type de menace, et plus précisément sur un outil de prise de contrôle à distance qui s'appelle **JSpy**. Nous voulions à la base utiliser **Back Orifice**, cependant, ce dernier étant connu de tous les antivirus actuels, il n'est plus nécessaire de s'attarder dessus. Nous en parlerons tout de même car il s'agit d'un outil de prise de contrôle à distance qui a été très en vogue dans les années 2000.
A travers cette étude, nous allons donc voir comment JSpy fonctionne, et quel est son impact sur un système Windows. Afin d'étudier le fonctionnement d'un tel outil, nous l'avons installé sur une machine virtuelle Windows, et avons étudié son comportement grâce à l'outil de monitoring **Sysmon**.

Ce document se présente en plusieurs parties :

- le contexte : présentation théorique de Back Orifice, JSpy et de Sysmon
- la pratique frauduleuse : utilisation de JSpy
- le monitoring : observation de l'activité de JSpy avec Sysmon

Nous espérons, à travers cette étude, montrer comment se défendre face à de tels outils et rendre la compréhension des chevaux de Troie plus accessible à tous.

PRÉSENTATION DES OUTILS

Définitions

Référence : “Hacker’s guide” 5e édition, écrit par Éric CHARTON

Un cheval de Troie est un logiciel furtif et difficilement détectable, qui donne accès aux ressources d’un ordinateur cible à travers le réseau Internet.

Celui-ci est composé d’un serveur (installé sur la machine cible) capable de réaliser certaines opération. Nous pouvons citer des opérations “banales”, sans réel danger, telles que : lister le contenu d’un répertoire, déplacer des fichiers, inverser l’écran, changer le curseur de la souris, etc… Le cheval de Troie est également capable d’effectuer des opération dangereuses, qui peuvent nuire à la machine infectée. Par exemple, détruire le contenu des mémoires de masse.
Ce serveur est associé à un client qui prend le contrôle du serveur à distance. Pour résumer, le troyen fonctionne comme un outil de prise de contrôle à distance. Il se différencie uniquement par sa furtivité.

Le cheval de Troie est qualifié de virus justement à cause de cette difficulté à le détecter, mais également parce que les manipulations qu’il autorise peuvent être le fait d’un hacker. Le cheval de Troie est développé par des individus indépendants, et non pas par de grandes entreprises. C’est la raison pour laquelle il est considéré comme dangereux pour un ordinateur. Le troyen est également considéré comme destructeur, puisque certaines de ses fonctionnalités permettent de porter atteinte à l’intégrité des données stockées sur un PC.

https://www.bitdefender.com/site/VirusInfo/browseVirusEnciclopedia
Cette page contient tous les troyens répertoriés, explique leurs actions, leurs signatures et leurs caractéristiques.

De manière légale, le concept du cheval de Troie n’existe pas. Il n’existe techniquement aucune différence entre l’outil d’administration à distance Windows, ou Telnet, et le troyen Back Orifice. Il s’agit avant tout d’un outil d’administration à distance, uniquement, avec un serveur et un client.

Côté sécurité, on pourrait croire qu’un troyen présente plusieurs lacunes, puisque nombre d’entre eux donnent accès librement à la machine cible. Mais ce n’est plus le cas aujourd’hui. En effet, certains troyens proposent des accès sécurisés par mot de passe.

Question détectabilité, maintenant, il est vrai que le troyen ne manifeste pas sa présence dans le menu Démarrer de Windows. En revanche, pour pouvoir fonctionner, celui-ci doit écouter sur un port IP du PC cible. Il faut donc moins d’une seconde pour détecter sa présence avec un scanner digne de ce nom (SuperScan 3.0 par exemple).

En définitive, ce qui différencie le troyen d'un logiciel d'accès à distance légal, c'est simplement le fait qu'un troyen est installé à l'insu d'un utilisateur. Ce qui le fait entrer dans la catégorie des virus, c'est donc l'utilisation que l'on va en faire.

Certains chevaux de Troie procèdent à des opérations illégales. Par exemple, nous pouvons citer les suivants :

- EPS (Email Password Sender) : vole les mots de passe des systèmes et les expédie par email.
- Rasmin : utilise toute la mémoire et plante le PC régulièrement. Attaque par déni de service.
- The Thief : vole les mots de passe et les envoie par email.
- Droid Dream Light (a été retiré du Google Play Store) : après avoir identifié les identifiants uniques d'une tablette, il peut télécharger de nouvelles acceptations et accéder au périphérique en mode root.

Le **monitoring** est un mot anglais pour désigner la surveillance. En informatique, le monitoring se fait essentiellement par l'examination des données et des événements. Ces événements sont présents sous forme de logs (enregistrements datés et classés, détaillant l'activité interne d'un processus et ses interactions avec son environnement).

Le monitoring, dans une société, est géré par un SIEM (Security Information & Event Management). Une solution SIEM collecte toute les données liées à la sécurité d'un système d'information complet (ordinateurs, périphériques réseau…).

Sous Windows, le journal des événements permet le même type de fonctionnalités, avec les événements locaux. Il collecte et enregistre tous les événements générés par les processus.

Back Orifice

Back Orifice est le plus connu des chevaux de Troie. Il est désormais detecté par la totalité des antivirus, ce qui le rend assez inoffensif et plutôt pratique pour réaliser des expériences. Sa dernière mise à jour date de 2007. Ce troyen est de la famille des rootkits (il peut être installé au niveau le plus sensible du système). Son installation ne prend que quelques secondes, puis il se dissimule.

Back Orifice est dit "neutre". C'est à dire pas de malveillance, pas d'attaque, c'est un logiciel silencieux. A un détail près : il installe des fonctions d'administration système (effacer, copier…) via le protocole IP, donc à travers Internet.
L'intrusion de Back Orifice est donc généralement l'oeuvre d'un tiers. Ce troyen figure en général sur une disquette de programme en apparence anodine (jeu, accessoire, driver, pièce-jointe à un email…).

Aujourd'hui, les chevaux de Troie sont plutôt difficiles à implanter. Les techniques de propagation de ces virus relèvent plus de l'espionnage et de l'intrusion sauvage que de la propagation active à travers des fichiers.
Le vrai danger du cheval de Troie est son efficacité, dans le cadre de l'espionnage industriel par exemple. Nous pouvons aussi citer la violation de la vie privée.

Voici la liste des fonctions autorisées par Back Orifice 2K :

- sniffing de clavier
- exploration du contenu du disque dur via un explorateur HTTP
- prise de contrôle du système de partage de fichiers de Microsoft
- édition directe dans la base des registres
- gestion et transfert de fichiers
- amélioration par plugin
- installation, mise à jour et désinstallation à distance
- sniffing des communications TCP/IP
- accès aux consoles via Telnet
- capture vidéo/audio
- backdoor pour contourner les mots de passe
- gestion des processus actifs
- capture et affichage des messages de l'interface graphique
- compression des fichiers
- redémarrage à distance
- résolutions des noms de domaine

En résumé, Back Orifice est un super-outil d'administration à distance.

JSpy

JSpy est un outil de prise de contrôle à distance développé en Java. Il permet un certain nombre de fonctions, telles que :

- des fonctions réseau
- des fonctions de surveillance (webcam par exemple)
- exploration de dossiers
- copie des dossiers, fichiers
- lancement de commandes Windows
- des fonctions plus drôles ("crazy mouse")

Nous détaillerons ces fonctionnalités plus en détail dans la partie pratique.

JSpy permet de générer un .jar, qui, une fois exécuté sur la machine distante, nous donne accès à toutes ces fonctionnalités. Il serait donc facile de piéger un utilisateur lambda en renommant ce fichier "Java Update". Il serait tenté de cliquer dessus, et nous prendrions alors le contrôle de son ordinateur.

Sysmon

Référence : https://docs.microsoft.com/

Sysmon, pour **Sys**tem **Mon**itor, est un service système Windows qui permet, une fois installé, de surveiller et d'enregistrer l'activité du système dans le journal des événements. Il fournit des indications précises et détaillées sur les différents processus, les informations réseau et les modifications apportées sur les fichiers. Il est donc possible grâce à cet outil de détecter une activité malveillante ou suspecte et de comprendre le fonctionnement de celle-ci.

Sysmon est capable de fournir un certain nombre de fonctionnalités, en voici une liste détaillée :

- création de logs
- enregistrer le hachage des fichiers image de processus en utilisant des algorithmes comme SHA1, MD5, SHA256 ou IMPHASH
- plusieurs hashs peuvent être utilisés en même temps
- inclut un processus de session dans chaque événement pour permettre la corrélation des événements même lorsque Windows réutilise les identifiants de processus
- enregistre les connexions réseau, y compris le processus source de chaque connexion, les adresses IP, les numéros de port, les noms d'hôtes et les noms de ports
- indique les changements dans le temps de création de fichier pour comprendre quand un fichier a été créé. La modification des fichiers "create timestamp" est une technique fréquemment utilisée par les malwares pour masquer leurs traces
- rechargement automatique de la configuration si le registre change
- règles pour inclure ou exclure certains événements de façon dynamique
- génère des événements depuis le début du processus de démarrage pour capturer l'activité réalisée par des logiciels malveillants

MISE EN PRATIQUE

Nous avons installé Sysmon sur un ordinateur portable, tournant sous Windows 10.
Tout d'abord, nous devons télécharger l'outil sur le site de Microsoft.

Sysmon v7.01

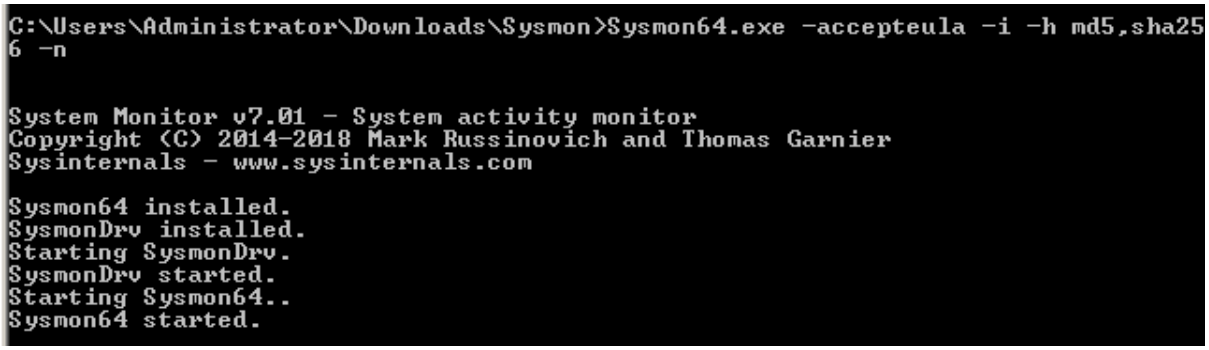
05/22/2017 • 12 minutes to read • Contributors

By Mark Russinovich and Thomas Garnier

Published: January 5, 2018

Download Sysmon (1.4 MB)

Une fois téléchargé et décompressé, il faut ouvrir un terminal en mode administrateur, et taper la commande suivante :



Nous avons installé Sysmon en lignes de commandes (voir figure ci-dessus). L'option **-i** permet d'installer le service et le driver. L'option **-h** (hash) permet de spécifier les algorithmes de hachage utilisés pour l'identification de l'image. Sysmon supporte plusieurs algorithmes en même temps. L'option **-n** (network) permet de spécifier que l'on souhaite récupérer les logs des connexions réseau.

Une fois installé, Sysmon va placer ses logs dans l'Observateur d'événements Windows.

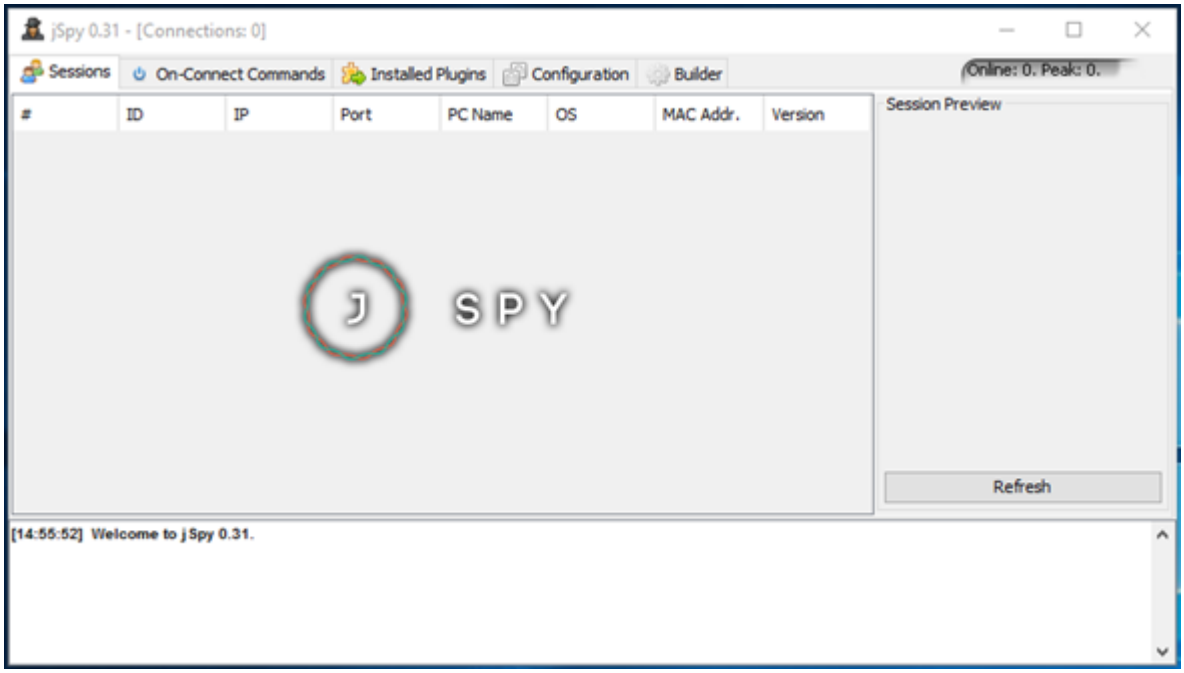
Il faut donc ouvrir l'observateur d'événements (Win+R et taper "eventvwr").

Il faut ensuite sélectionner le chemin suivant :

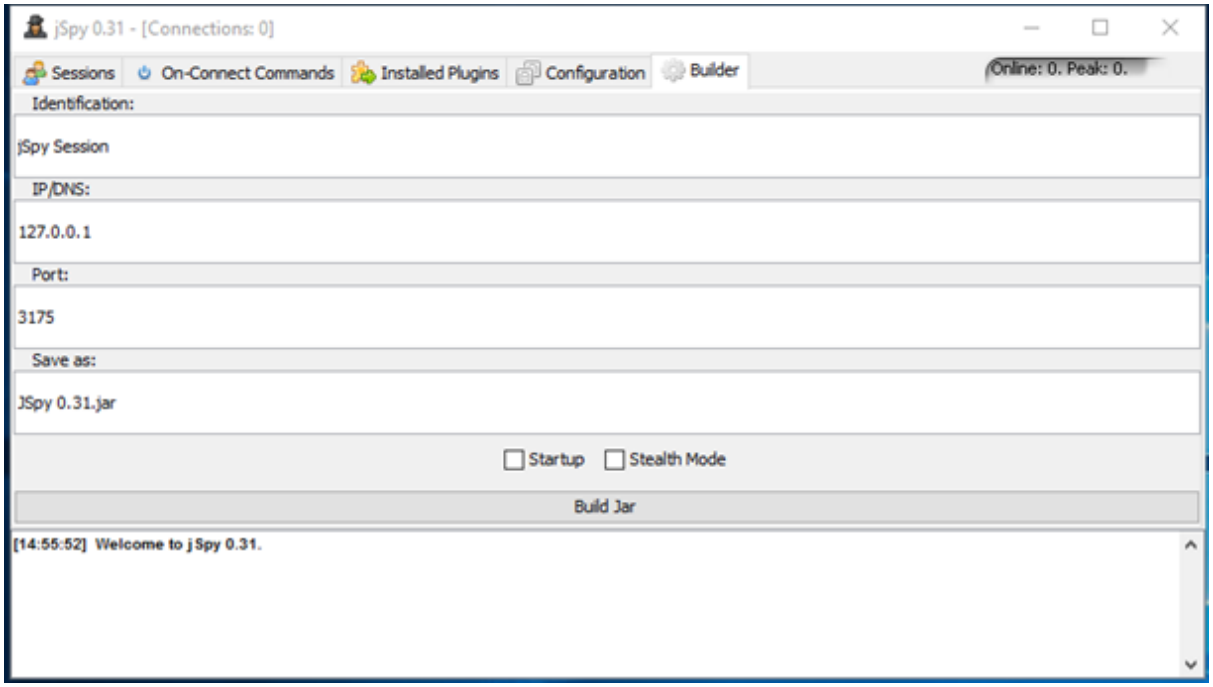
→ Applications and Services Logs/Microsoft/Windows/Sysmon/Operational

A partir de là, nous aurons accès à tous les événements reportés par Sysmon.

Attardons-nous maintenant sur JSpy, l'outil de prise de contrôle à distance.
Après avoir cliqué sur l'application, nous arrivons sur la fenêtre principale (voir figure ci-après).

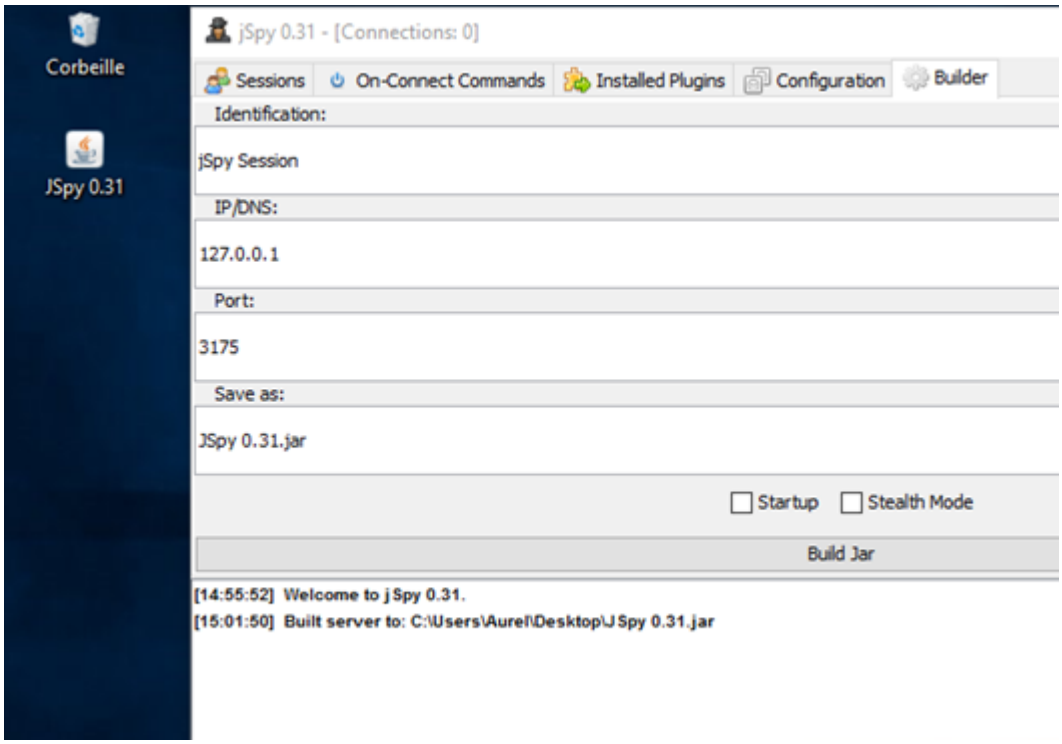


La première étape est de créer le fichier .jar "serveur", qui va devoir être implanté sur le PC à infecter. Pour ce faire, nous allons dans l'onglet **Builder**.

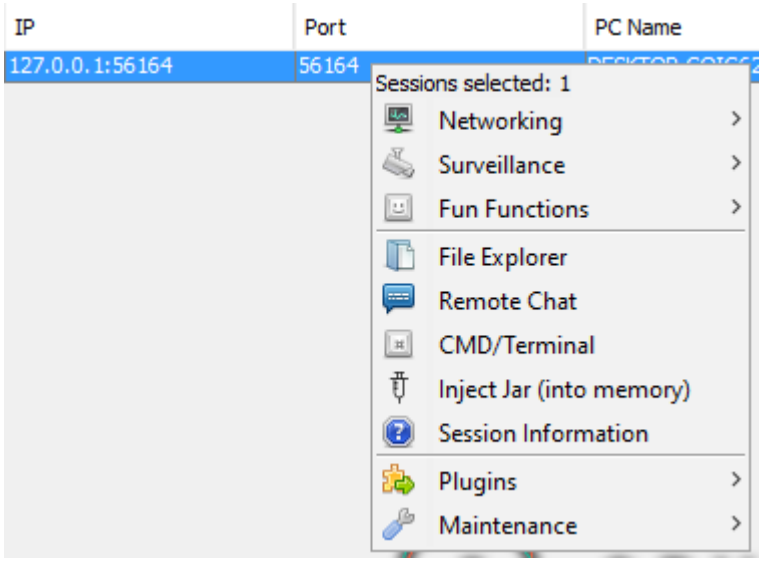


Nous allons infecter notre propre PC, par souci de légalité. Ainsi nous configurons l'IP avec l'adresse locale (127.0.0.1). Nous laissons le port proposé par défaut, et nous appelons notre fichier jar "JSpy 0.31.jar", puis nous générons le jar en cliquant sur "build Jar".

Nous enregistrons ce dernier sur le Bureau, pour le retrouver facilement, comme le montre la figure suivante.

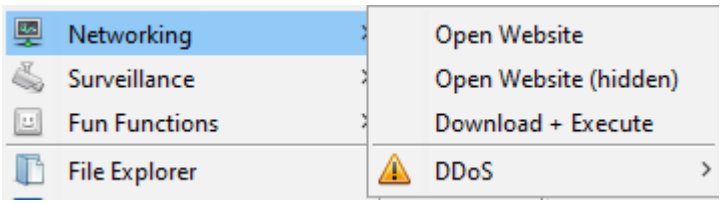


Pour que le PC soit infecté, il faut donc que ce fichier soit exécuté. Il suffit de double-cliquer dessus, et le tour est joué.
JSpy le détecte automatiquement, et une nouvelle session s'ouvre.
Nous avons désormais le contrôle du PC infecté.



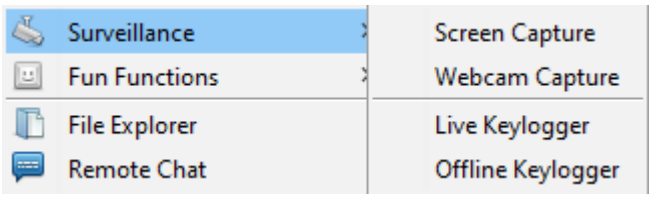
JSpy permet d'effectuer un certain nombre d'opérations, comme le montre la figure ci-dessus.

Réseau



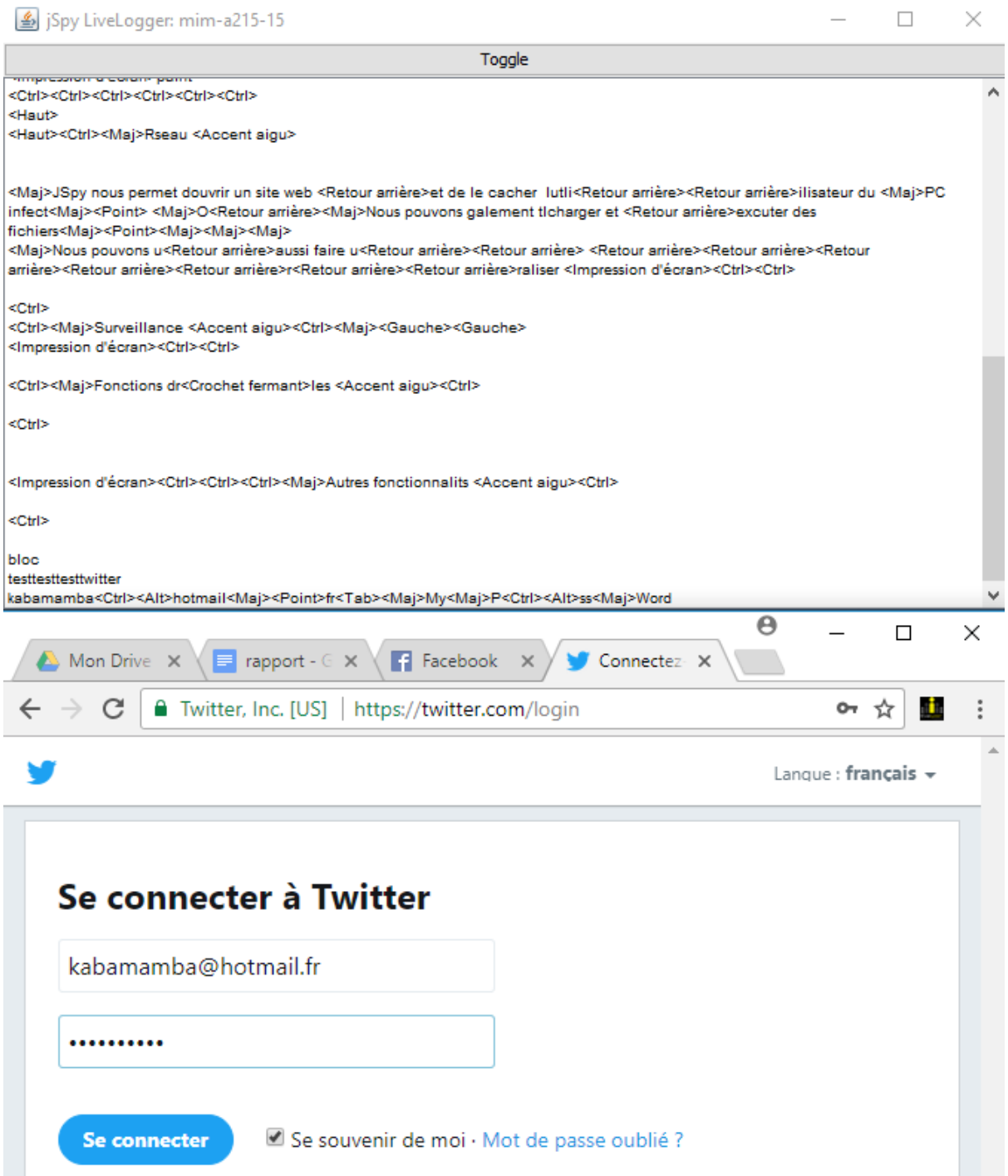
JSpy nous permet d'ouvrir un site web et de le cacher à l'utilisateur du PC infecté. Nous pouvons également télécharger et exécuter des fichiers.
Nous pouvons aussi réaliser des attaques de type déni de service, mais pour des raisons évidentes (nous avons exécuté le serveur sur notre propre machine), nous n'avons pas testé cette fonctionnalité.
De plus, il existe des outils DDoS très puissants sous KaliLinux qui ne nécessitent pas un contrôle d'accès à distance. (Ettercap et l'ARP poisoning, Hping3, etc…)

Surveillance



Comme on peut le voir sur l'impression d'écran ci-dessus, JSpy possède la fonctionnalité d'être utilisé en tant que Keylogger, nous avons le choix entre deux modes, à savoir, le mode live et le mode offline. (Voir les détails ci-après)

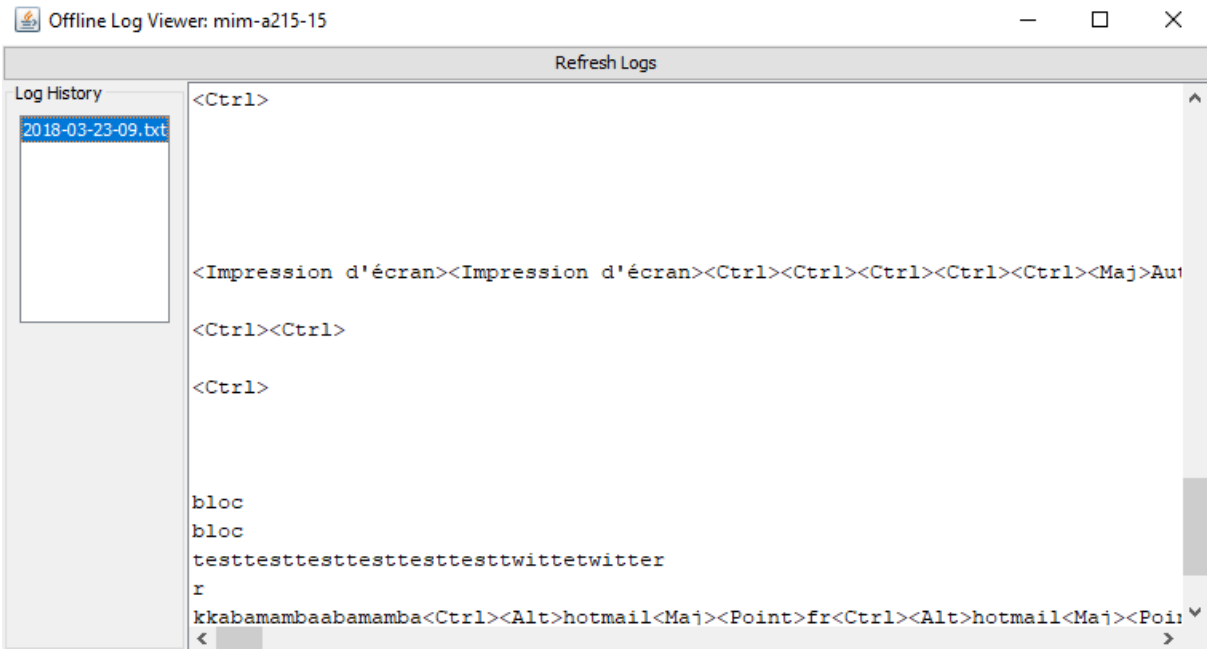
1. Live Keylogger



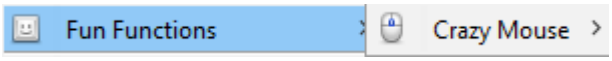
Comme on peut le voir sur le screen ci-dessus, le live keylogger nous permet de récupérer toutes les informations que l'utilisateur saisit au clavier. Après avoir essayé de nous connecter à Twitter, on peut voir que le keylogger a réussi à récupérer notre mot de passe (MyPassWord).

2. Offline Keylogger

Le mode offline garde un historique des précédents logs utilisés, on peut donc les re-visualiser.

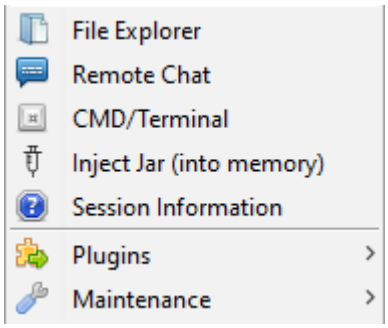


Fonctions “drôles”



Cette fonctionnalité n’est présente que pour le fun, et ne représente rapporte strictement rien à l’attaquant. Elle n’est présente que pour embêter l’utilisateur du PC infecté.
Elle consiste à faire changer le curseur de position sur l’écran une fois par seconde. Ainsi, il est difficile (voir presque impossible) de cliquer là où on le voudrait, par manque de temps.

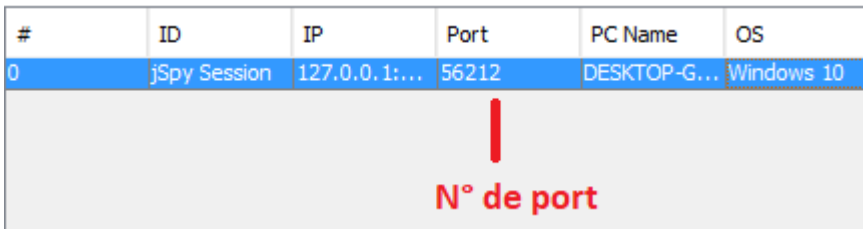
Autres fonctionnalités



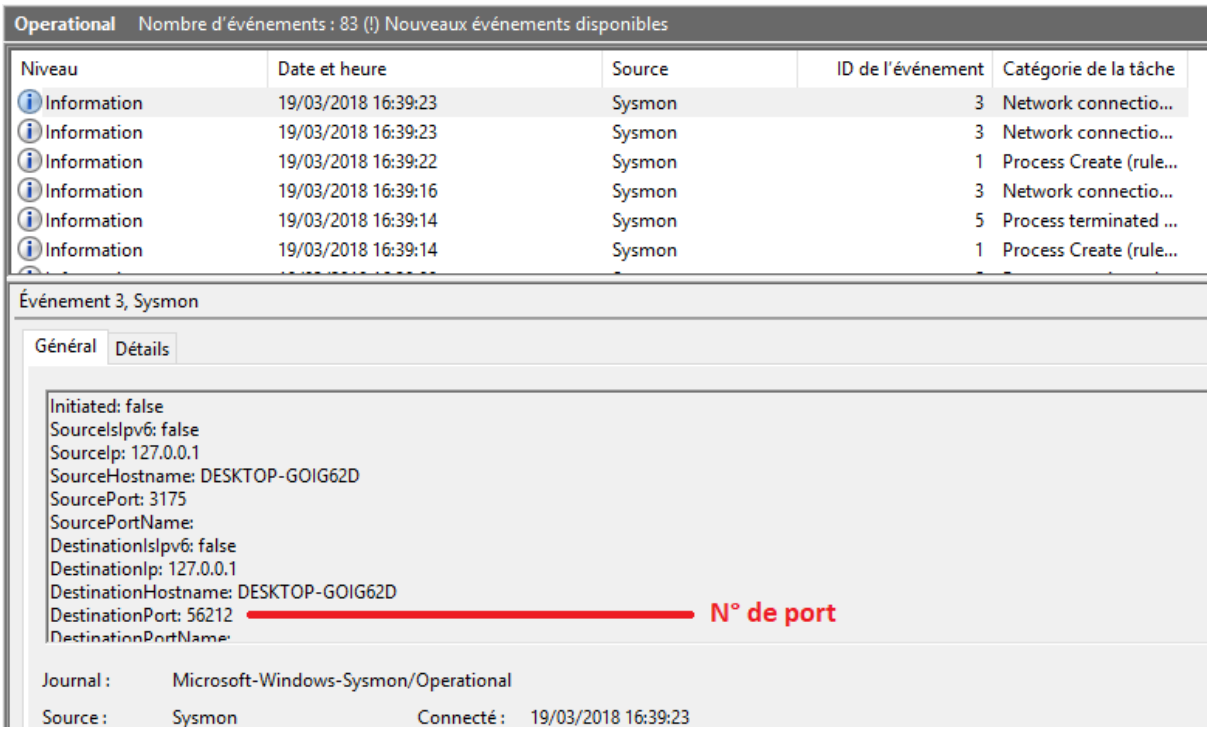
Les autres fonctionnalités de JSpy nous permettent respectivement de :

- parcourir les dossiers du PC infecté, et en modifier/copier/supprimer les fichiers
- ouvrir un chat sur le PC infecté
- lancer des commandes à la façon de l'invite de commandes Windows
- injecter un fichier .jar dans la mémoire
- obtenir des informations sur le PC infecté (OS, processeur, RAM…)
- et enfin, fermer l'accès à distance et le supprimer.

Pour la suite de cette étude pratique, nous allons donc nous connecter au PC infecté avec JSpy.



Retenons bien ce numéro de port, il est important pour l'observation avec Sysmon.
Nous actualisons l'observateur d'événements : le dernier événement remonté par Sysmon concerne une connexion, sur le port 56212.



Sysmon nous a donc rapporté qu'une connexion suspicieuse avait bien eu lieu.
L'ID de l'événement vaut 3, ce qui correspond à "Network connexion"

La liste des principaux événements remontés par Sysmon est la suivante :

- 1 : Process creation
- 2 : A process changed a file creation time
- 3 : Network connection
- 4 : Sysmon service state changed
- 5 : Process terminated
- 6 : Driver loaded
- etc.

Ainsi, Sysmon est capable de nous avertir lorsqu'un processus est créé ou encore lorsqu'on modifie un fichier.
Pour faire simple, les chevaux de Troie sont facilement détectables par les antivirus.
Et si jamais un antivirus ne détecte pas le cheval de Troie, grâce à Sysmon il est possible de retracer l'activité du RAT.

CONCLUSION

Les chevaux de Troie sont des logiciels malveillants, qui s'installent à l'insu de l'utilisateur. Ils permettent d'exécuter des fonctions ou d'obtenir le contrôle à distance de l'ordinateur infecté. On estime aujourd'hui qu'un ordinateur sur trois est infecté par un logiciel malveillant, et que la plupart provient d'un cheval de Troie.

Nous avons vu le fonctionnement d'un logiciel de ce type : JSpy. L'installateur du serveur JSpy est un simple fichier Jar, qui, une fois exécuté, nous donne un accès presque complet à l'ordinateur infecté.
Nous pouvons ainsi exécuter un certain nombre de fonctionnalités, à des fins malveillantes, ou à des fins bienveillantes pour aider un utilisateur à distance.

Un service tel que Sysmon permet de lever des alertes en cas de fonctionnement suspect du système. Nous avons vu au travers de la partie pratique que Sysmon est capable de détecter les connexions malveillantes, et les actions effectuées par le troyen.

Ainsi il est possible non seulement de détecter facilement les chevaux de Troie grâce à des logiciels de sécurité de type antivirus, et si ces derniers ne parviennent pas à les détecter, il est possible de retrouver les traces des actions malveillantes grâce à Sysmon.