

Comment hacker une entreprise avec 11 euros ?

Introduction

« Salut, aujourd’hui je vais vous apprendre comment avec 11 euros d’investissements, vous allez pouvoir dégager des milliers d’euros de bénéfices en vous attaquant aux entreprises et en y plaçant des ransomwares ! »

Plus sérieusement, dans cet article nous allons aborder les attaques par **clé HID** (Human Interface Device). Ces fausses clés USB **se font passer pour des claviers**, et peuvent ainsi tapoter ce que l’attaquant voudra. Et dans notre cas, ce sera contrôlable à distance par Wifi.

Évidemment, comme ce ne sont que de simples « claviers tout gentils », aucun Antivirus ne s’excitera à leurs branchements, aucune permission ne sera demandée et désactiver l’Autorun U3 ne changera rien.

Ce style d’attaque permet de pouvoir directement **atteindre des machines importantes/cachées d’une organisation**, sans éveiller de soupçon, à l’inverse d’attaques complexes qui seraient menées depuis l’extérieur et devant désarmer les pare-feu et système de sécurité mis en place.

C’est excitant pas vrai ? Voici un scénario qui pourrait bien arriver à votre entreprise demain si des criminels ou des concurrents peu scrupuleux vous ciblent.



Scénario

Vous l’aurez bien compris, pour mettre en place cette attaque il va falloir avoir un **accès physique** pour brancher notre petite clé tout innocente.

La pensée de sécurité physique est souvent oubliée et exploiter les comportements humains pour gagner ces accès est plus facile qu'il n'y paraît.

Ici nous imaginons qu'un acteur malveillant va commencer par une **phase de reconnaissance** et d'**OSINT** sur l'entreprise nommée « Digital Bitcoin Supply Chain » pour savoir quelles personnes seraient vulnérables (en raison de pressions financières par exemple) et quelles personnes attaquer. Après avoir tiré profit de ces informations, il constate ceci :

- Bob, le directeur commercial de la boîte, ne verrouille pas souvent son PC, comme le montrent les posts Instagram corporatifs de l'entreprise plaisantant avec le fait qu'il doit souvent payer des croissants
- Une société de ménage externe à l'entreprise s'occupe pendant la pause du midi de nettoyer les bureaux de l'entreprise. Jeanne y est agente d'entretien et est apparemment mal payée et mécontente d'après ses posts Twitter

L'acteur malveillant va rentrer en contact avec Jeanne et lui propose 7000 euros en liquide en échange de brancher discrètement cette clé USB innocente sur l'ordinateur portable de Bob pendant qu'elle fera le ménage. Jeanne a accepté.



Autres scénarios

Voici une liste d'autres scénarios d'ingénierie sociale également applicable pour réussir à rentrer à l'intérieur d'un bâtiment :

- Avoir les bras chargés, simuler être un livreur
- Demander à la sécurité de vous ouvrir, en prétextant avoir oublié des affaires après un entretien d'embauche
- Avoir un gilet jaune et passer pour un technicien (ça marche super bien : cf)
- Se faire passer pour un stagiaire perdu et profiter pour aller là où souhaité

- Avoir une tête de geek et se faire passer pour le service informatique, en passant par une porte laissée ouverte par des fumeurs par exemple
- Méthode plus brutale, mais si il n'y a personne et c'est une serrure simple, on crochète !

À l'époque actuelle, rester anonyme même en venant physiquement dans les bureaux de votre victime est redevenu facile grâce à un petit accessoire obligatoire : le masque !

Combiné à une perruque, vous pouvez littéralement vous métamorphoser.

À l'attaque



Une fois la clé insérée, le réseau Wifi créé par la clé apparaît. Georges, le complice de l'attaquant se trouve à l'extérieur de l'entreprise et se connecte au Wifi depuis son portable et lance les [payloads](#) développés en amont.

Payload 1 : Désactivation du son

Afin de se faire le plus discret possible et pour ne pas attirer l'attention, la première charge va venir désactiver le son de l'ordinateur.

Temps nécessaire : 10 secondes



Payload 2 : Désactivation de Windows Defender

Pour pouvoir lancer à foison toutes les charges malveillantes que l'attaquant voudra (et sans vouloir s'embêter à bypass Defender), la désactivation pure et dure de Defender est effectuée.

Temps nécessaire : 15 secondes



Payload 3: Reverse Shell

Pour prendre totalement contrôle de l'ordinateur à distance, l'attaquant va déployer un [reverse shell](#).

Temps nécessaire : 1 seconde

Sur la machine victime de Bob, on se connecte au serveur distant de l'attaquant avec le reverse shell [ConPty](#)



Côté attaquant, il n'y a plus qu'à attendre la connexion du pc de Bob à notre pc et pouvoir s'amuser dessus.

```
root@vmi467041:~# stty raw -echo; (stty size; cat) | nc -lvpn 3001
Listening on 0.0.0.0 3001
```

Dans cet exemple, l'attaquant va se balader sur l'ordinateur de Bob, le directeur commercial, puis exfiltrer vers son serveur les fichiers [Clients](#) de l'entreprise (un CRM et une proposition commerciale).

En moins de 30 secondes (26 pour être exact), l'attaquant a pu lancer 3 charges qui lui ont permis d'avoir la main mise sur l'ordinateur de Bob sans se faire détecter.

Quand il n'y en a plus, il y en a encore

Payload 4 : Persistence

Afin de ne pas perdre la main sur l'ordinateur de Bob et rester persistent dessus, l'attaquant va lancer ce payload et utiliser [SharPersist](#)

Temps nécessaire : 20 secondes

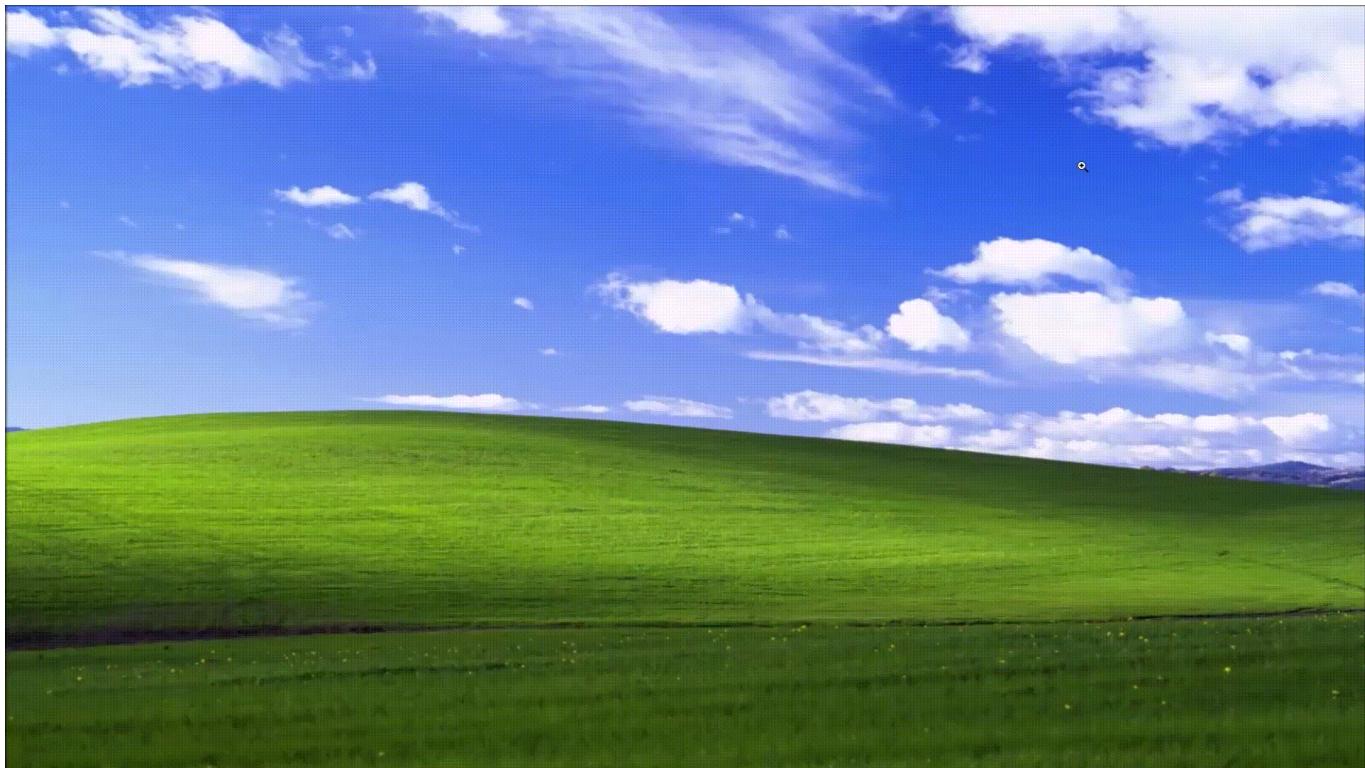


Payload 5 : Mimikatz

Si l'attaquant ne veut pas s'arrêter à l'ordinateur de Bob mais souhaite s'amuser sur l'[AD](#) de l'entreprise, un outil comme [mimikatz](#) peut s'avérer utile !

L'attaquant va ici sortir les hash, les mots de passe des sessions Windows et les tickets [Kerberos](#) pour les envoyer sur son serveur distant.

Temps nécessaire : 20 secondes



Bonus : le vice ultime

Afin d'obtenir définitivement le **mot de passe de déverrouillage** de l'ordinateur de Bob, l'attaquant peut lancer à distance l'outil [FakeLogonScreen](#) qui va simuler un faux écran de connexion Windows.

Quand Bob reviendra de sa pause du midi, il tapera innocemment son mot de passe pour déverrouiller son écran. Côté attaquant le mot de passe sera reçu sans problème.

The screenshot shows the Cobalt Strike interface. At the top, there's a navigation bar with links for Cobalt Strike, View, Attacks, Reporting, and Help. Below the bar is a toolbar with various icons. A main table displays network connections:

external	internal	listener	user	computer	note	process	pid	arch	last
10.120.0.16	169.254.39.234	http	User *	DESKTOP-FK33NC5		powershell.exe	2984	x64	52ms

Below the table is a large terminal window. The title bar of the terminal says "Event Log X | Listeners X | Beacon 169.254.39.234@2984 X". The terminal output shows:

```
Arrisis[DESKTOP-FK33NC5]\User * /2984 [2020Feb01 17:44:06] sleep 0
[*] Tasked beacon to become interactive
[+] host called home, sent: 16 bytes
```

At the bottom of the terminal, it says "[DESKTOP-FK33NC5] User * /2984 (x64) last: 52ms". The status bar at the very bottom of the screen shows system information: "No VPN", "02%", "1.6 GiB (41.4%)", "7.8 GiB (66.0 GiB free)", and the date/time "2020-02-01 17:56:18".

Pauvre Bob, et lui qui pensait avoir bien verrouillé sa session pour une fois ...

La clé HID montre ici clairement sa **supériorité** à un classique attaquant qui taperait manuellement les commandes après avoir réussi à avoir un accès physique à l'entreprise, avec 3 avantages :

- tape beaucoup plus vite (vous avez pu voir les délais nécessaires pour chaque charge, ce n'est pas humainement faisable)
- tape sans faire de fautes de syntaxe
- est beaucoup plus discrète ! Avec ses 2-3 centimètres, elle réussit à se faire beaucoup plus petite qu'un attaquant de 1 mètre 80 qui ne serait pas à sa place. Comme quoi **la taille compte** finalement.

Vecteurs d'attaque

Évidemment dans cet exemple notre attaquant a simplement exfiltré des fichiers confidentiels dans un cadre d'espionnage industriel, mais ayant un accès complet à l'ordinateur, plusieurs attaques peuvent être déployées :

- [Ransomware](#)
- Récupération des cookies de sessions des navigateurs et mots de passe pour se connecter
- Ajout sur le domaine de l'entreprise si le compte a les droits
- Changer le fichier [hosts](#) pour rediriger l'utilisateur et faire du phishing
- Saboter les fichiers présents sur le PC, modifier des parties déjà écrites
- Et plus encore

Mais au fait, quelle est cette clé ?



C'est une bonne WHID ! Cactus WHID a été créé par [Luca Bongiorni](#) en 2017 et est souvent résumé comme une "Rubberducky contrôlable à distance par Wifi ". Ce n'est d'ailleurs pas son seul avantage puisqu'elle ne coûte que [11 euros](#)

WHID contient deux modules :

- Une carte ATMega32u4 qui émule tout dispositif HID et dispose d'une mémoire flash autoprogrammable
- Un module Wifi ESP-12S

La portée du point d'accès Wifi va différer en fonction du bâtiment, mais à partir de 15 - 30 mètres la connexion va commencer à pârir. Dans certains cas un drone devra donc être utilisé pour approcher la zone et diriger la WHID.

Le stockage disponible pour les payloads est de 3Mb.

À l'achat, les Cactus WHID sont livrés avec le logiciel [ESPlloitV2](#).

Pour rendre la clé compatible avec les claviers français AZERTY, il vous faudra changer le clavier dans [Arduino](#) puis reflasher la clé en suivant ces [consignes](#).

Une fois votre clé configurée, le point d'accès Wifi sera visible avec comme nom par défaut [Exploit](#) et mot de passe : [DotAgency](#)

Rendez-vous à l'adresse par défaut <http://192.168.1.1> pour accéder au menu ESPlloit

C'est à partir d'ici que vous allez pouvoir upload vos payloads puis les lancer. Plusieurs options sont aussi possibles (dont la conversion des scripts Ducky en scripts ESPlloit)



i 192.168.1.1



ESPloit v2.7.41 - WiFi controlled HID Keyboard Emulator



by Corey Harding

www.LegacySecurityGroup.com/
www.Exploit.Agency

File System Info Calculated in Bytes

Total: 2949250 **Free:** 2940967 **Used:** 8283

[Live Payload Mode](#) - [Input Mode](#) - [Duckduino Mode](#)

-
[Choose Payload](#) - [Upload Payload](#)

-
[List Exfiltrated Data](#) - [Format File System](#)

-
[Configure ESPloit](#)

-
[Upgrade ESPloit Firmware](#)

-
[Help](#)

Vous pouvez également choisir de rendre visible ou non le SSID lors de la création du point d'accès.

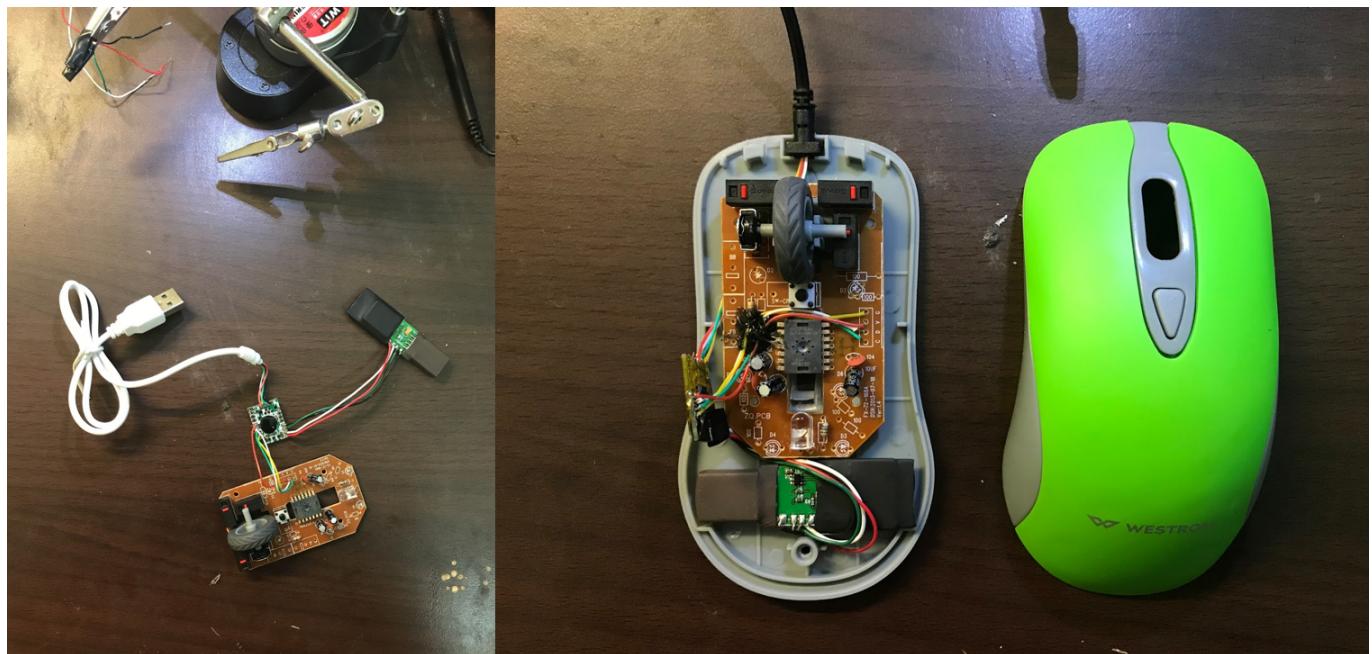
Le PID (Product ID) et VID (Vendor ID) sont également [modifiables](#) afin de par exemple contourner la protection mise en place par l'administrateur système n'autorisant le branchement que de certains produits USB.

Jouer à cache-cache

Pour les plus barbus équipés de fer à souder, il est possible de cacher directement la WHID dans d'autres objets câblés en USB et les offrir (faire croire à un cadeau d'une boîte collaborant avec la victime par exemple) ou les laisser traîner, puis attendre le branchement fatidique.

En voici quelques exemples :

- classique et discrète, la souris



- Une boule plasma, et pourquoi pas !



- et plus encore : des chargeurs de cigarettes électroniques, des ventilateurs, des hubs USB, tout est possible !

Comment s'en protéger ?

La solution miracle n'existe pas, mais un certain nombre de **mesures** peuvent être mises en place afin de se **défendre et prévenir** ce genre d'attaques :

- Former et **sensibiliser** les employés à connaître ce type de menace (à verrouiller leurs pc, vérifier que des clés n'ont pas été branchées entre temps) et ainsi pouvoir prévenir ces attaques
- Manière forte : bloquer tous les ports USB, malheureusement c'est presque impossible pour la majorité des entreprises
- Alors, ne limiter qu'à certains produits (avec le PID/VID) l'autorisation de se brancher et communiquer avec le système (pour Windows dans [Regedit>DeviceInstallRestrictions](#), pour Linux > [udev rules](#)).

Là encore, si l'attaquant fait bien son travail de reconnaissance en préattaque, il pourra voir quels types de claviers sont autorisés (par exemple que des Logitech) et [spoofe](#) le PID / VID.

- Sur Linux, il existe, depuis début 2020, l'outil [ukip](#) de Google, qui mesure la vitesse d'entrée des touches et déterminer si cela provient d'un humain ou d'une attaque.
- Ne branchez pas de clé USB inconnue ou trouvée. Et si vous devez brancher de nouvelles clés, faites-le sur un poste hors réseau ou sur une station blanche afin de vérifier que la clé ne soit pas menaçante pour l'entreprise.