BarbHack 2020

USB : Ami ou Ennemi

POGGI Jérôme
@EdGtslFcbngq6sk
EdGtslFcbngq6sk@itsnotmy.pw

Plan

- Qui suis je ?
- Quizz
- Pourquoi et comment pervertir l'USB ?
- Les « Armes » à disposition …
- Conclusion

Qui suis-je ?

- Tombé dans l'informatique à 12 ans
- +22 ans d'XP dans la SSI
- Dev, Admin, Pentesteur, Auditeur, Architecte …
- Actuellement RSSI dans une grande collectivité


QUIZZZZ

l'USB c'est quoi ?

- Réponse A : Un Bus Universel Série à 4 connecteurs
  - 2 pour l'alimentation 5V et +
  - 2 pour les données

- Réponse B : Un connecteur qui n'est jamais dans le bon sens ?
- Réponse C : De quoi recharger mon téléphone
- Réponse D : Un fabuleux accès aux équipements

Introduction

USB - HID

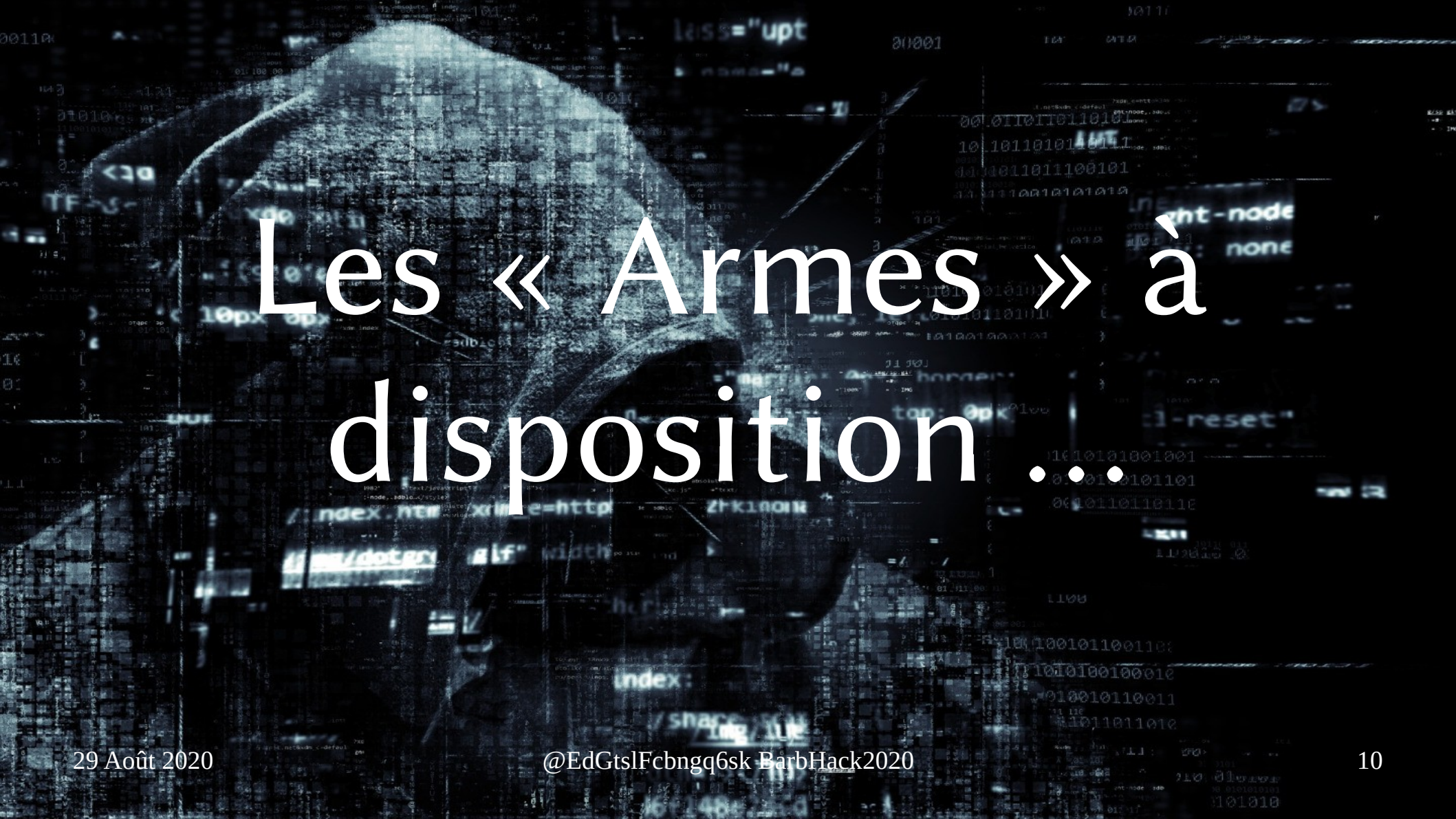
- *Human Interface Device*

- « Si ça parle comme un clavier et que cela s'identifie comme un clavier … alors c'est un clavier »

Pourquoi et comment pervertir l'USB ?

La perversion : pourquoi ?

- Parce que l'on est payé pour (Red-Team)
- Parce que l'on a besoin de sensibiliser (Equipe SSI / RSSI)
- Parce que le test d'intrusion depuis Internet a échoué (Red-Team qui en bave...)
  - Réseaux isolés, secteur sensible ...
  - Parce que personne ne clique ni sur les liens, ni n'ouvre le
  - Parce que l'équipe SSI a bien bossé
- Parce-que c'est « marrant » et que c'est mon ordinate



Les « Armes » à disposition …


Les élémentaires ...

Basique mais efficace

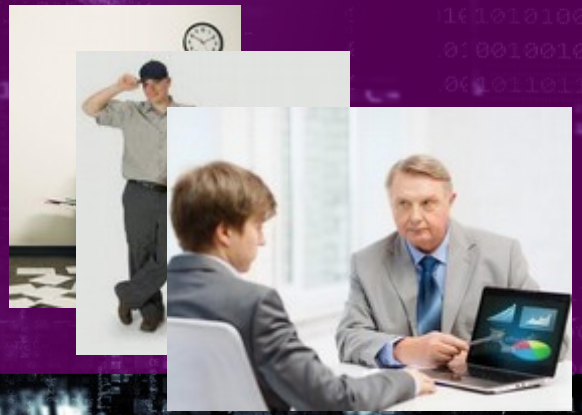
- Le micro clavier/souris sans fil …


L’accès à la cible …

L’accès direct

- Bureau sans personne
  - Pas fermé à clef
  - Fermé à clef, mais avec une serrure « simple »
  - Serrure plus complexe : on demande à la sécurité du bâtiment …

- Bureau occupé
  - Le stagiaire
  - Le livreur
  - L’entretien d’embauche



L’accès Indirect


CyberWar
USB
KEY
DROPPED
cyberwarzone.com

L’accès Indirect

- La clef USB qui « traîne » par terre dans le parking
  - Pas toute seule !!!
  - Il faut faire envie,
  - Inspirer confiance …


Le début de la fin ...

Le plus connu

- Le rubber ducky

USB Rubber Ducky

- Équipement matériel (clef USB) vu comme un clavier
- Programmable avec un langage simple
- Simule une frappe rapide au clavier
- Fonctionne avec tous les OS acceptant un clavier USB
- Rendu célèbre avec Mr ROBOT
- Rudimentaire, connu des EDR, (45$) mais efficace

Démo

- Reverse Shell avec MimiKatz en 30sec
- https://www.hak5.org/blog/15-second-password-hack-mr-robot-style

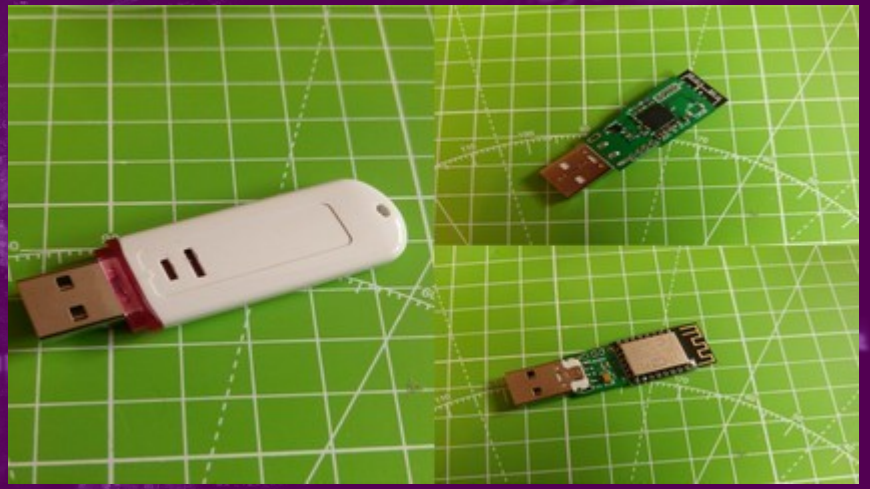
Utilité en Marketing

Marketing ???

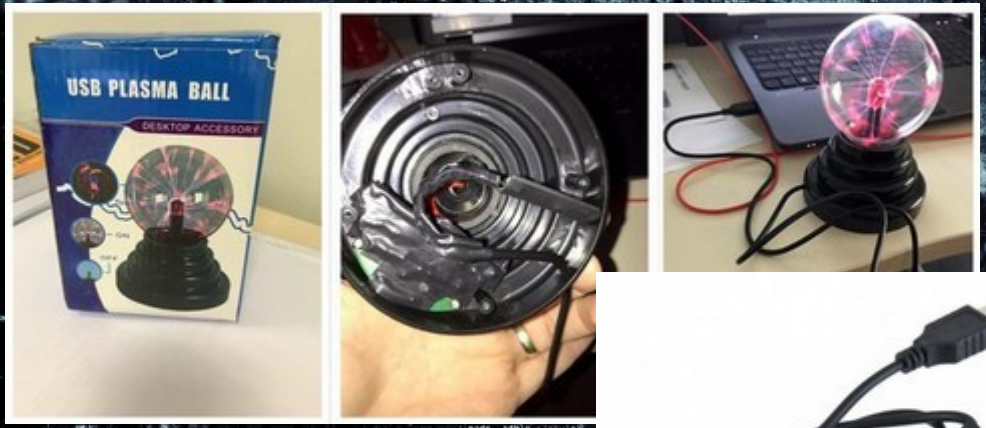
Evolution et petits frères …

WHID

- WHID : *Wireless Human Interface Device*
- Arduino + ESP8266 (15$!!!)
- http://whid.ninja/
  - Module Wi-Fi (ESP8266) + WPA
  - Serveur HTTP
  - Payload Rubber Ducky « like »
  - Multiples charges stockées dans la NAND
  - Déclenchement à souhait …
- @LucaBongiorni

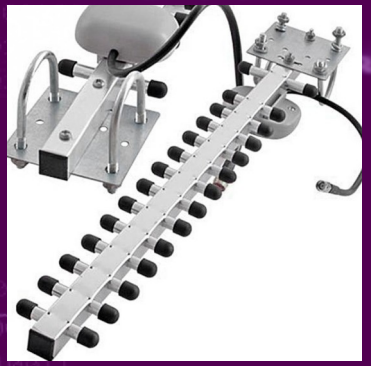


Piégeage de Gadget USB et ...



Scénario d'usage ...

- La clef est insérée par une personne ayant un accès physique
- Attente ...
- Drone, jumelle ou télescope pour la visu
- Antenne directionnelle pour la commande



Attirail de chez Hak5

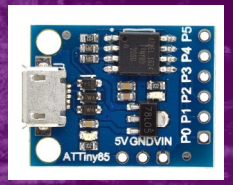
- Bunny BASH
  - Emulation ethernet, port série, stockage
  - Seulement 2 charges possibles
- LAN Turtle
  - Véritable « P0wn box »

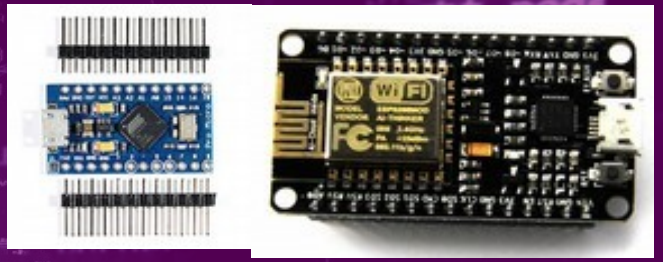
Peut-on faire pire ?

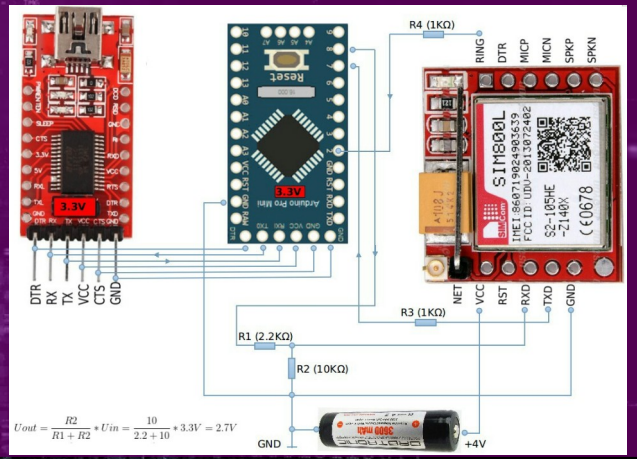
- C’est déjà stressant pour la Blue Team
- Mais c’est parfait pour la Red-team

Plus petit, moins cher et +

- Arduino à 3€
- ATTINY85 à 1€
- ESP8266 ou ESP32 à 15€ ...
  - Plus puissant et module radio intégré
- Ajout du module GSM SIM800L
- OrangePI GSM 30€
- RaspiZero
- Par contre ...
  - Il va falloir coder !







Le … mais non ! Pourquoi ?

- Le Zynqberry et ZynqberryZero
  - Un raspberry et un FPGA (Xilinx Zynq-7000)


Et si la cible disposait déjà de l'implant ?

MouseJack et CrazyRadio = JackIT

- Pourquoi implanter une backdoor alors qu'elle est déjà présente ?
- Compromission des dongles USB Souris/Clavier 2.4GHz
  - https://www.bitcraze.io/crazyradio-pa
    - nRF24LU1 « custom firmware »
  - https://github.com/RFStorm/mousejack
    - Sniffer, injecter et compromettre
- Jackit = « sulfateuse de payload »
  - Attaque injection à l'aveugle …
  - Il suffit d'attendre le retour du reverse shell
  - https://github.com/insecurityofthings/jackit.git

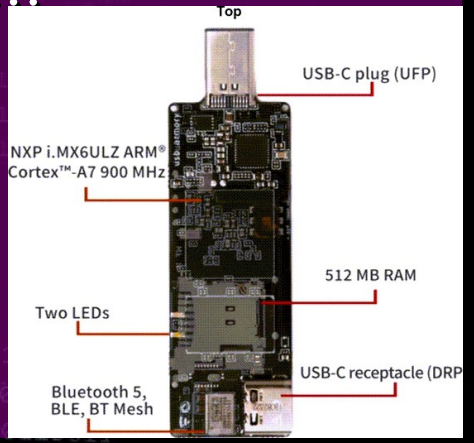
Encore plus de puissance, fonctionnalités ...

WHID 31337

- Compatible GSM (pilotable par SMS)
- Compatible MouseJack (ESP8266 en 2.4GHz)
- Disposant d'un micro
  - Possibilités infinies…
- Rejoue des signaux RF..
  - 433 MHz ou 315 MHz
- L'arme parfaite en Red-Team

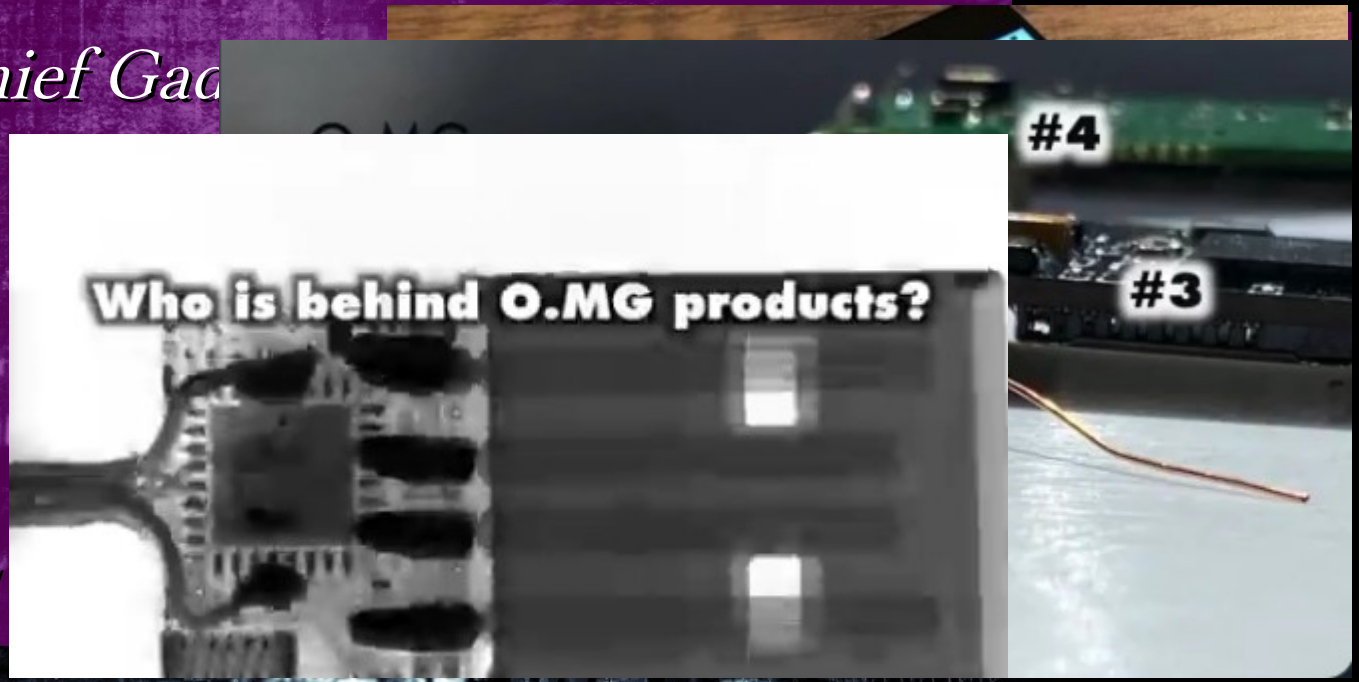
USB-Harmory MK II

- Linux 100 % autonome
  - Cortex A7, 512Mbps de RAM, 16G eMMC + µSD
  - Secure BOOT, True RNG, Crypto processeur …
    - Stockage sécurisé
  - Emule un adaptateur Ethernet après boot
    - Attaque Windows avec RNDIS_ETHERNET



OMG cable

- Cable Lightning 100 % fonctionnel
  - *Offensive Mischief Gad*
  - Mais …
    - Keylogger
    - Ruber
    - …
  - https://o.mg.lol/




La destruction ...

Jusqu'à la destruction

USB KILLER …
De 3€ à 30€

Conclusion

Conclusion

- Un accès physique direct ou indirect
  - Et c'est la compromission quasi assurée
- Connaître ses faiblesses, ses risques et les armes d'en face
  - Et la compromission sera moindre …

Merci

« La vérité vous à été révélée, Faites en ce que vous voulez ... »

Références

- https://github.com/certsocietegenerale/Publications/blob/master/DFRWS%20EU19%20-%20The%20Rise%20Of%20HID%20Devices.pdf
- @whid_ninja et @LucaBongiorni
- https://www.hackster.io/news/zynqberry-s-new-little-cousin-zynqberryzero-927dff2a39ad
- https://twitter.com/_MG_
- https://github.com/insecurityofthings/jackit