WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

Powered by NTT Com Security

Teensy - Introduire une porte dérobé dans un périphérique USB

Antoine Cervoise (@acervoise)

17 juin 2016

NTT Communications | NTT Com Security

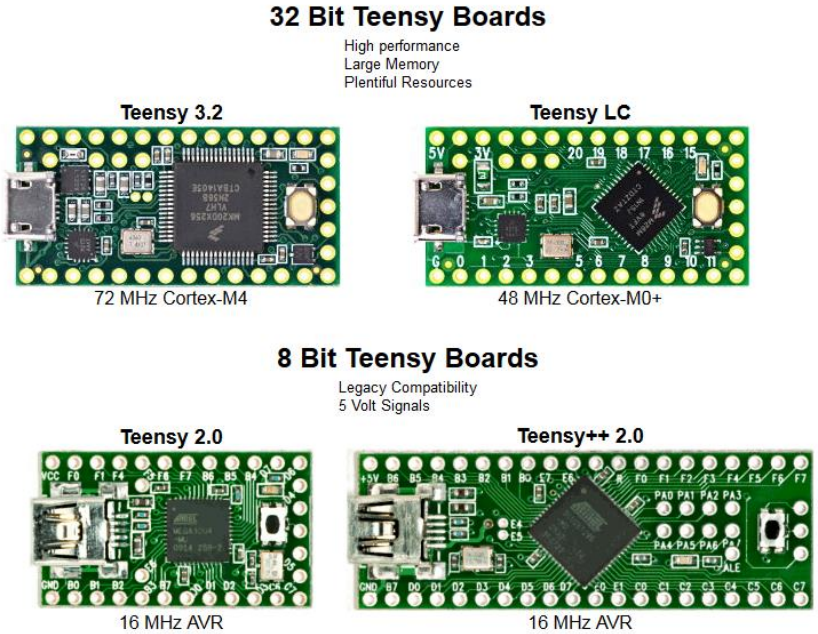
Contents

1. Teensy/Arduino/Rubber Ducky
2. Simuler un clavier mais encore ?
3. Simuler (un clavier) sans que ça se voit…
4. Simuler un clavier, et après ?

Teensy/Arduino/Rubber Duckey

Arduino

Teensy



Site officiel : https://www.pjrc.com/teensy/

Prix : 16 à 25 $

Payload :

- https://github.com/offensive-security/hid-backdoor-peensy
- https://github.com/samratashok/Kautilya

Rubber Duckey

Prix : 40 €

Payload :
http://ducktoolkit-411.rhcloud.com/Home.jsp

Convertir payload vers la Teensy :
https://github.com/Plazmaz/Duckuino

Decompilateur :

https://github.com/DavidSkrundz/ducky-decode

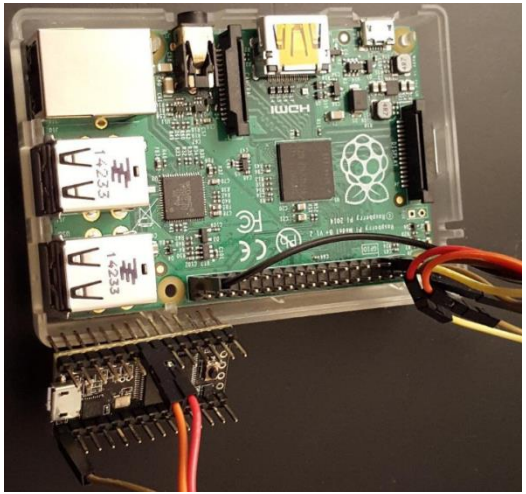
Quelques projets

Pa$$ware - a diy hardware password safe

http://fr.slideshare.net/sth4ck/sthack-2014-mano-0xsata-zwahlen-paware-a-diy-hardware-password-safe

Hardware Bruteforce Framework

https://github.com/cervoise/Hardware-Bruteforce-Framework-2



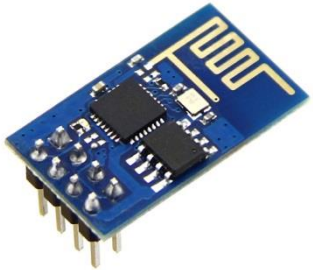
Simuler un clavier mais encore ?

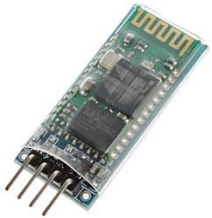
Comment interagir ?

CAPSLOCK / NUMLOCK

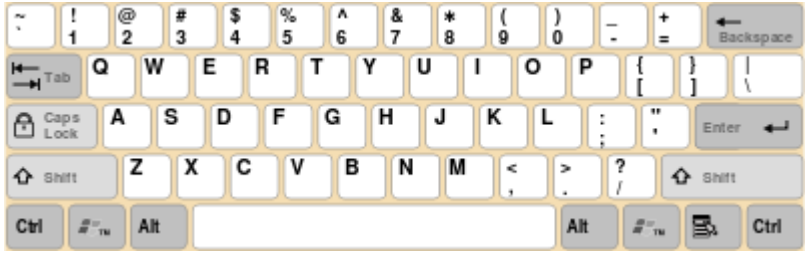
Carte SD (Teensy 2 et ++2)

Visuel (Bluetooth, Wi-Fi)

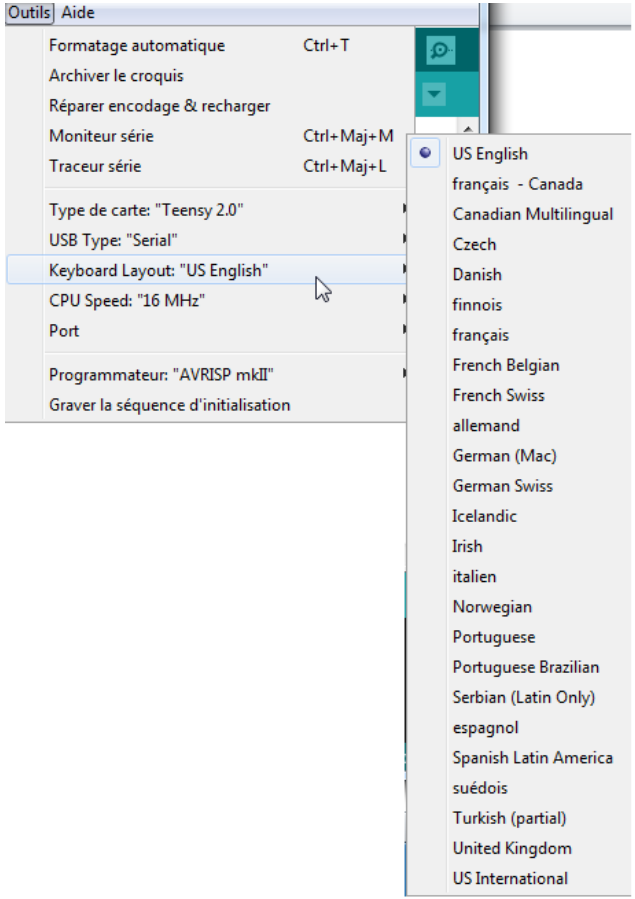




Problème majeur : langue et OS



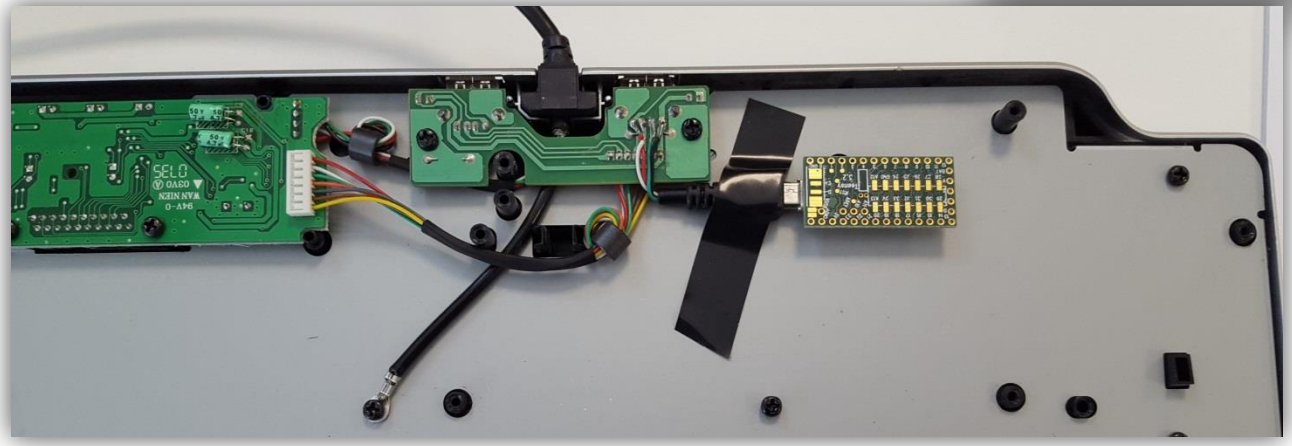
Problème majeur : langue et OS



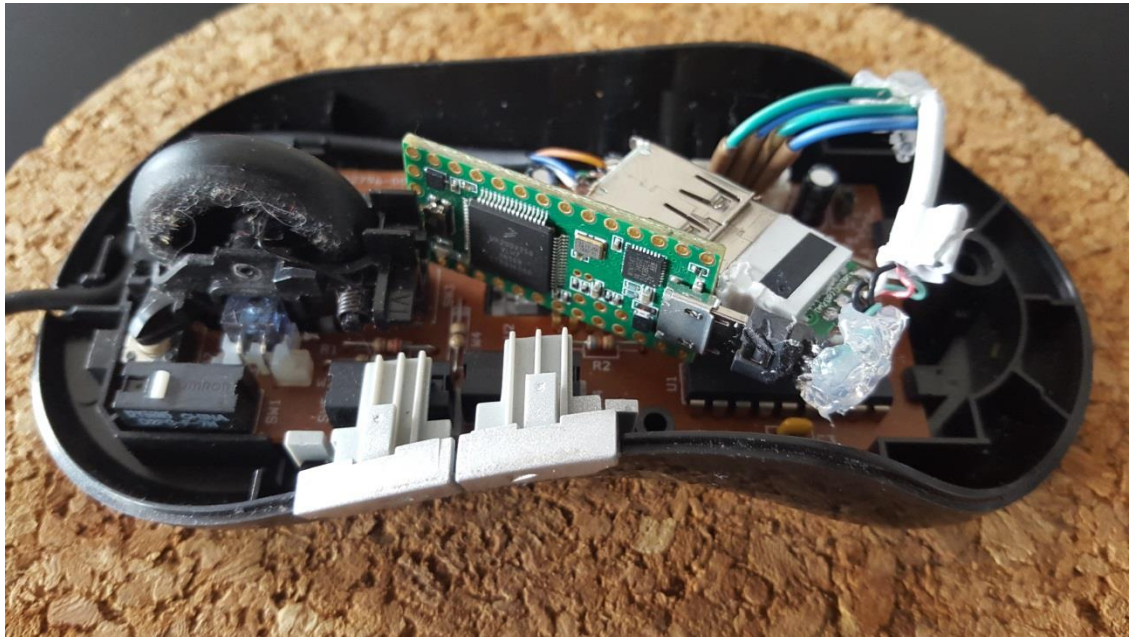
Simuler (un clavier) sans que ça se voit…

Lecteur MP3

Clavier



Souris



Méthodologie

Trouver la bonne cible

Trouver les bons composants

Les détruire

Recommencer

Des idées ?

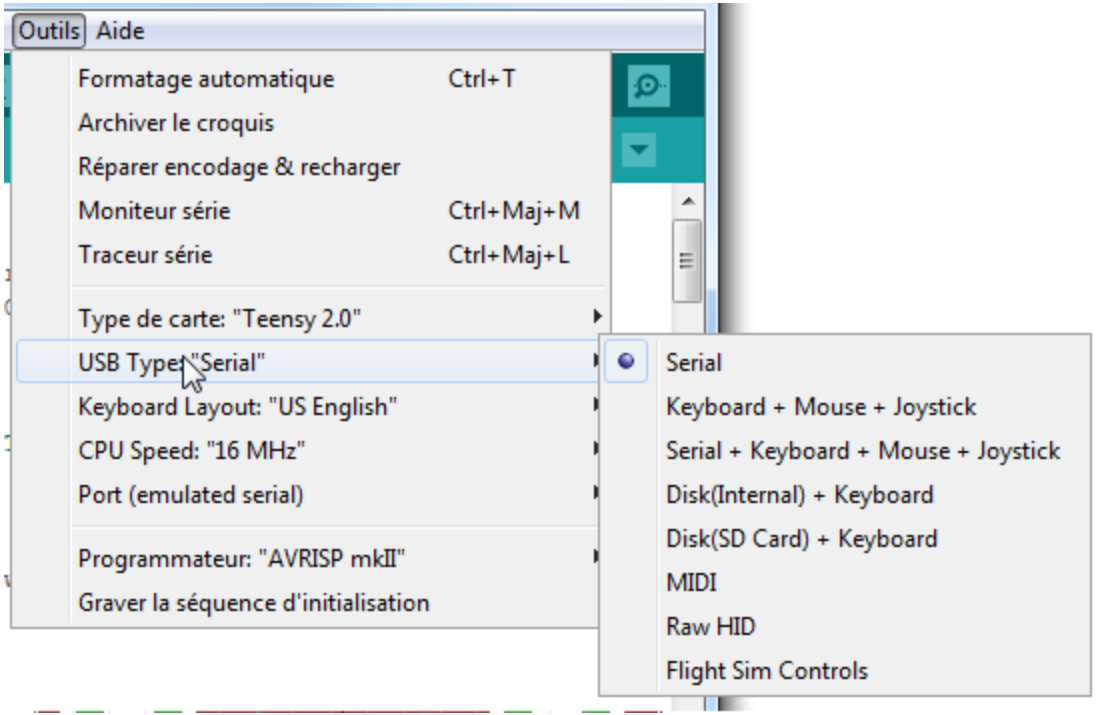
Autre option

USB Keyboard

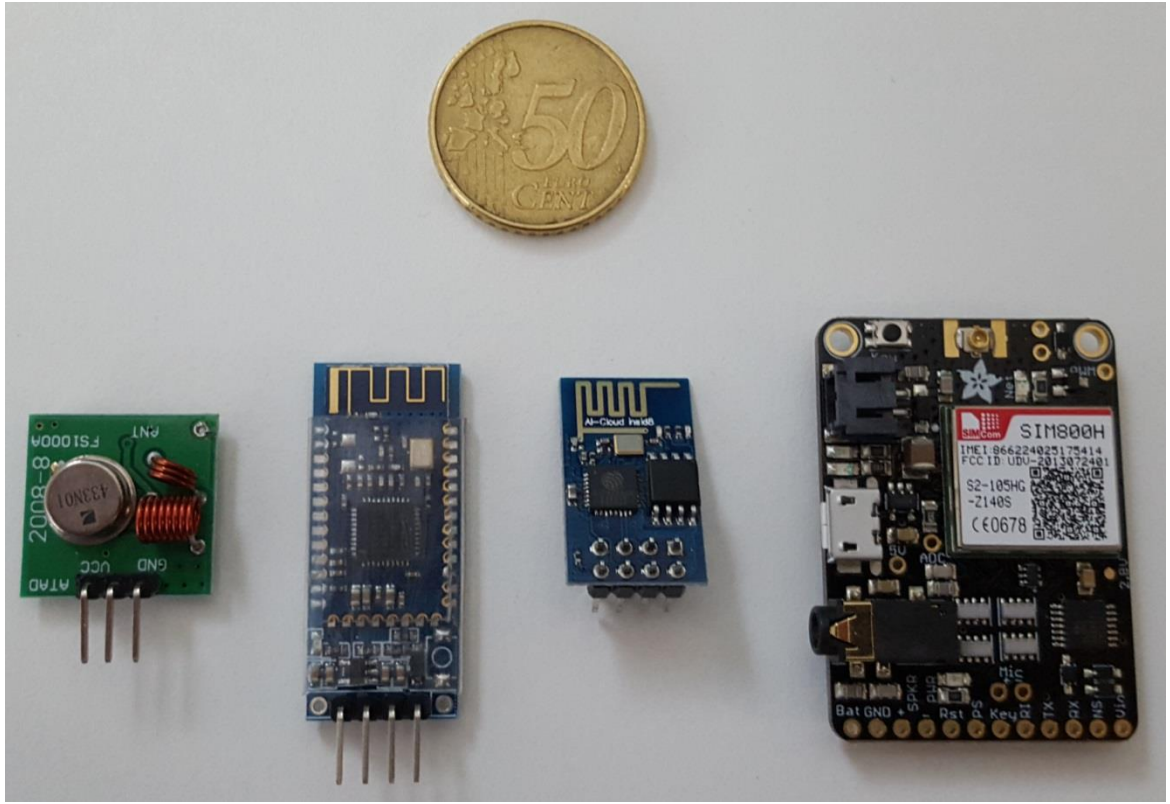
https://play.google.com/store/apps/details?id=remote.hid.keyboard.client&hl=fr

Simuler un clavier, et après ?

LeakyStorage



LeakyStorage



LeakyStorage

Composant :

> Teensy 2

> SD Adaptor

> 3.3 Volt Regulator

> ESP8266

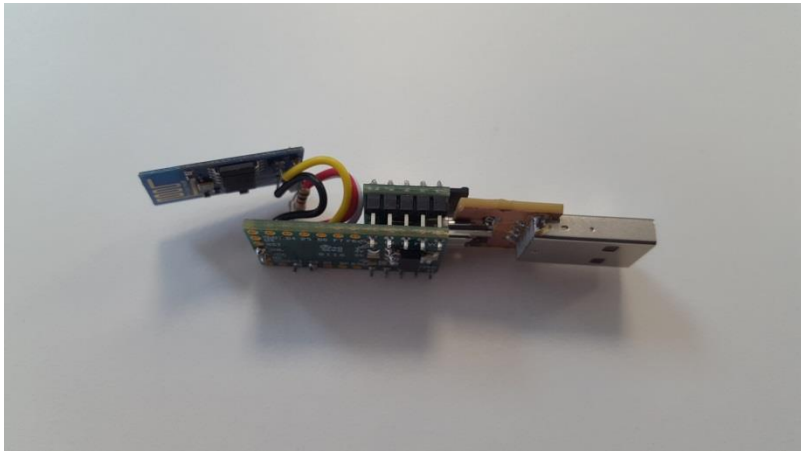
Prix : 16 $ + 8 $ + 1$ + 4$ = 29 $

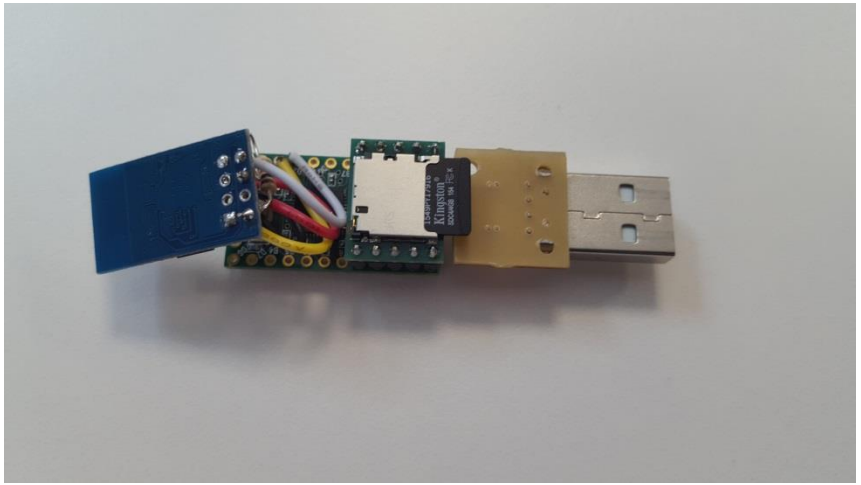
DIY :

> Adaptateur Micro USB / USB

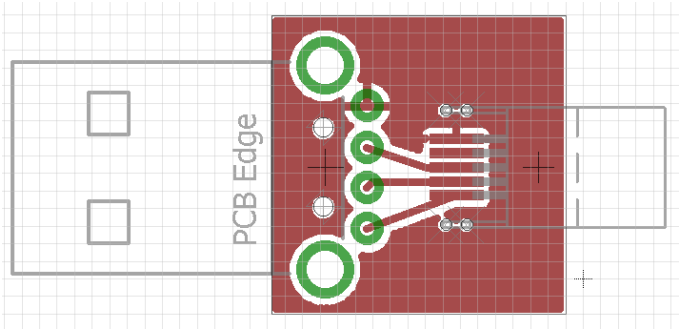
> Boitier

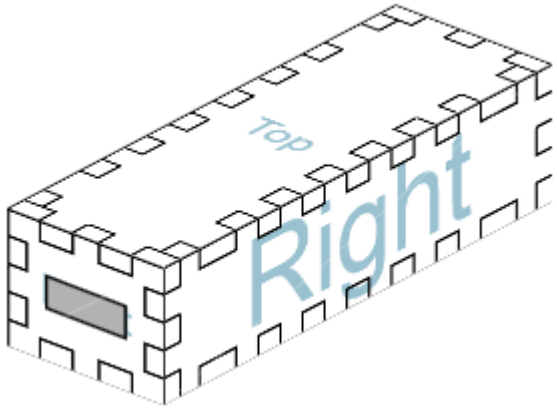
LeakyStorage





LeakyStorage

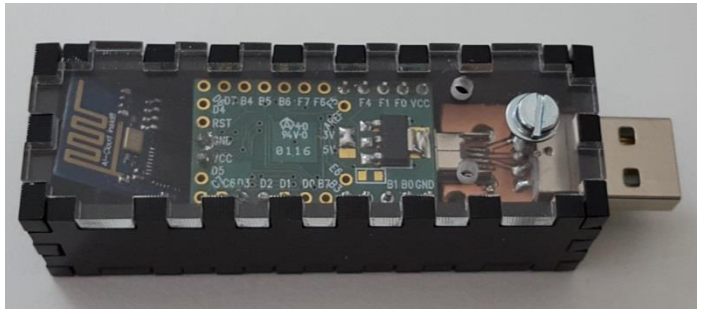




LeakyStorage

https://github.com/nttcomsecurity/LeakyStorage

- Arduino
- Case
- Server
- USB_adapter
- LICENSE
- README.md



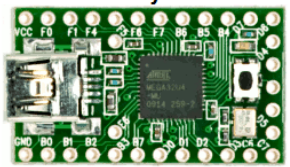
LeakyStorage : problèmes connus

```
Compilation terminée.

Le croquis utilise 23 194 octets (71%) de l'espace de stockage de programmes. Le maximum est de 32 256 octets.
Les variables globales utilisent 784 octets (30%) de mémoire dynamique, ce qui laisse 1 776 octets pour les variables locales.
```

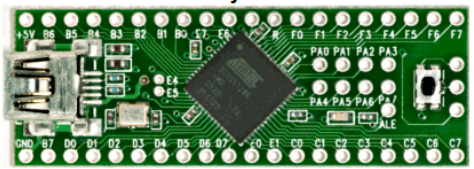
Specification	Teensy 2.0	Teensy++ 2.0
Processor	ATMEGA32U4 8 bit AVR 16 MHz	AT90USB1286 8 bit AVR 16 MHz
Flash Memory	32256	130048
RAM Memory	2560	8192
EEPROM	1024	4096
I/O	25, 5 Volt	46, 5 Volt
Analog In	12	8
PWM	7	9
UART,I2C,SPI	1,1,1	1,1,1
Price	$16.00	$24.00

Teensy 2.0



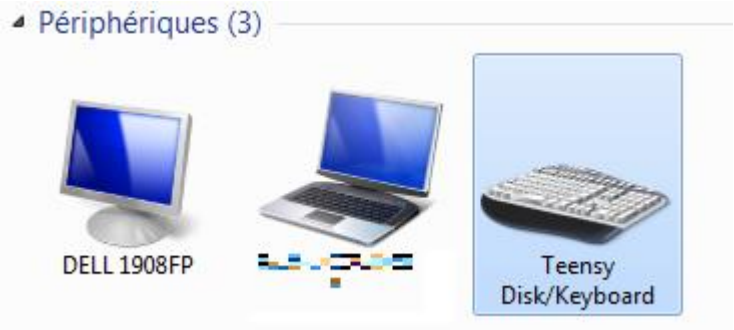
16 MHz AVR

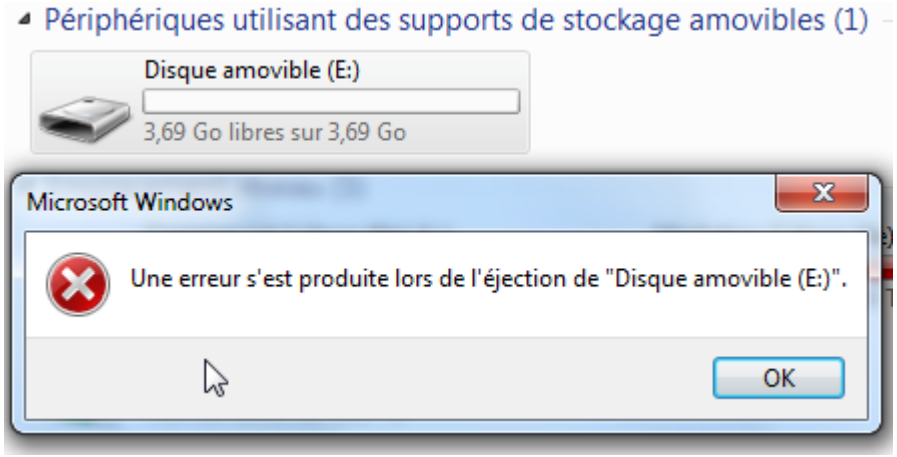
Teensy++ 2.0



16 MHz AVR

LeakyStorage : problèmes connus





LeakyStorage : problèmes connus

```
[  383.506904] usb 1-4.3.4: new full-speed USB device number 9 using xhci_hcd
[  383.597024] usb 1-4.3.4: New USB device found, idVendor=16c0, idProduct=0484
[  383.597027] usb 1-4.3.4: New USB device strings: Mfr=0, Product=1, SerialNumber=2
[  383.597029] usb 1-4.3.4: Product: Teensy Disk/Keyboard
[  383.597030] usb 1-4.3.4: SerialNumber: 123456789ABCDEF0
[  383.598553] input: Teensy Disk/Keyboard as /devices/pci0000:00/0000:00:14.0/usb1/1-4/1-4.3/1-4.3.4/1-4.3.4:1.1/0003:16C0:0484.0004/input/in
put22
[  383.651251] hid-generic 0003:16C0:0484.0004: input,hidraw3: USB HID v1.11 Keyboard [Teensy Disk/Keyboard] on usb-0000:00:14.0-4.3.4/input1
[  383.652454] hid-generic 0003:16C0:0484.0005: hidraw4: USB HID v1.11 Device [Teensy Disk/Keyboard] on usb-0000:00:14.0-4.3.4/input2
[  383.668729] usb-storage 1-4.3.4:1.0: USB Mass Storage device detected
[  383.668934] scsi host2: usb-storage 1-4.3.4:1.0
[  383.669004] usbcore: registered new interface driver usb-storage
[  383.670131] usbcore: registered new interface driver uas
[  384.668126] scsi 2:0:0:0: Direct-Access     Generic  USB Flash Disc   1.00 PQ: 0 ANSI: 4
[  384.668401] sd 2:0:0:0: Attached scsi generic sg1 type 0
[  384.669163] sd 2:0:0:0: [sdb] Attached SCSI removable disk
[  386.686296] sd 2:0:0:0: [sdb] 7774208 512-byte logical blocks: (3.98 GB/3.70 GiB)
[  386.698093]  sdb: sdb1
```

Questions ?

Univershell

Workshop sécurité sur Paris

Dernier jeudi du mois

Exemples de workshop réalisés

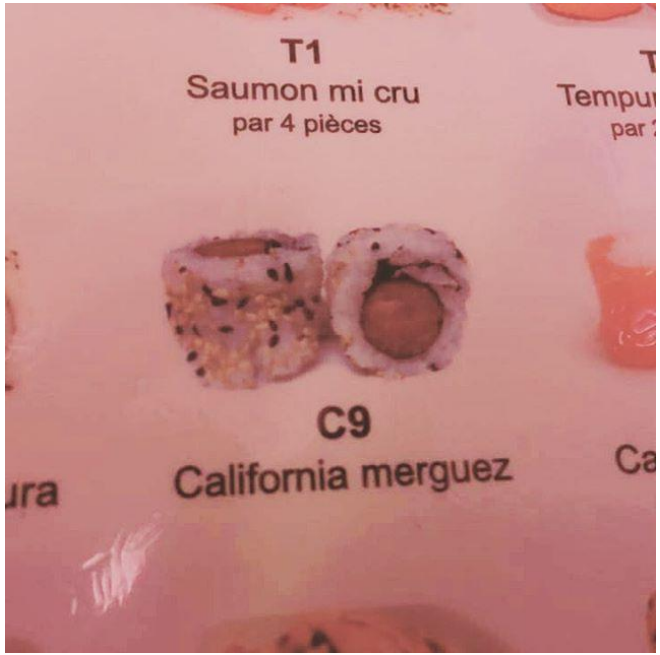
> *BTA, MIASM, SCADA, DFF*

Merci à NoLimitSecu, SSTIC et BeeRumP pour la pub

https://www.univershell.net/

https://twitter.com/_Univershell_

@_Univershell_



Fabelier

Hackerspace parisien

Tous les mardi et mercredi soir à partir de 19h

Pour une première visite, venez un mercredi !

Equipements de prototypage rapide : fers à souder, imprimante 3D, découpeuse laser

Ouvert à tous/toutes

Une seule « exigence » : libérer/documenter son projet

Fabelier.org

@fabelier

Thank you

ANTOINE CERVOISE
PENTESTER - SECURITY AUDITOR
NTT COM SECURITY

antoine.cervoise@nttcomesecurity.com
www.nttcomsecurity.com