



Jouons avec des clés USB

Pierre-Yves Bonnetain
 py.bonnetain@ba-cst.com

1 Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403 ReSIST 27/11/2007



Les clés USB « U3 »

It's what's next. It's what's smart.



Powered by U3 Smart Technology

Meet the next generation of USB flash drives: the U3 smart drive. It's what's inside that makes them smart.

Store your data and carry software applications!

STORAGE+SOFTWARE+SMART


Imagine carrying your software on the same flash drive that carries your data. That's what you can do with a U3 smart drive. You can plug it into any PC and work, play a game, message friends, send email, take photos and more. A U3 smart drive makes any PC your own PC. And when you unplug it, it leaves no personal data behind.



The Launchpad makes the drive smart:

- Comes with **pre-installed software**
- Carry and access your files **easy!**
- Get more U3 smart software at www.u3.com
- Keep your data **safe and secure**
- Anti-virus comes bundled on most drives
- Build-in password protection
- Unplug the drive and leave no personal data behind


2 Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403 ReSIST 27/11/2007




Organisation de la clé

- ◆ Simuler un CD.
- ◆ Partition spéciale, lecture seulement, sur la clé (environ 6 Mo).
- ◆ Contient des programmes et un autorun.inf.
- ◆ Une fois branchée sur un ordinateur
 - un lecteur CD,
 - un disque amovible.


3 Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403 ReSIST 27/11/2007




Sur le poste de travail



Autre



4 Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403 ReSIST 27/11/2007



Sous Linux...

- ◆ La partition « CD-ROM » est invisible, sauf si le pilote SCSI est bien configuré :
- ◆ [*] Probe all LUNs on each SCSI device
- ◆ (CONFIG_SCSI_MULTI_LUN=y) }

```

* usb 1-1: Product: U3 Smart Drive
* usb 1-1: Manufacturer: EMTEC
* usb 1-1: SerialNumber: 0700077112B0C48
* usb 1-1: configuration #1 chosen from 1 choice
* Initializing USB Mass Storage driver...
* scsi0 : SCSI emulation for USB Mass Storage devices
* USB Mass Storage support registered.
* Vendor: EMTEC Model: U3 Smart Drive Rev: PMAP
* Type: Direct-Access ANSI SCSI revision: 00
* Vendor: EMTEC Model: U3 Smart Drive Rev: PMAP
* Type: CD-ROM ANSI SCSI revision: 00
  
```

5 Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403 ReSIST 27/11/2007



La partition CD



6 Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403 ReSIST 27/11/2007

Le LaunchPad

- ◆ Simule un menu « Démarrer »
- ◆ Fonctions de configuration
 - Paramètres
 - Ajout de programmes U3-isés
 - Mot de passe de la partition Flash (à creuser...)



7

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

Mise à jour du CD

- ◆ En théorie :
 - Ancienne version (LPInstaller.exe)
 - Image cruzeur-autorun.iso
 - cherche l'image en local (dans le répertoire où se trouve LPInstaller.exe) ou
 - la télécharge depuis updates.u3.com
 - NOTE : LPInstaller.exe est indisponible sur le site de sandisk.
 - Installation automatique sur la clé
- ◆ Possibilité de jouer avec le DNS pour diffuser une image « personnalisée »

8

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

Mise à jour

- ◆ Le LaunchPad dispose d'une fonction de mise à jour automatique.
- ◆ Exécutée au branchement de la clé (à l'initialisation du LaunchPad ?)
- ◆ Paramètre UpdatesAutoCheck (flash:/system/apps/lpgdb.xml)
- ◆ La clé se met à jour sur le site updates.u3.com
- ◆ En pratique :
 - A voir... lors de la prochaine mise à jour.

9

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

Protocole de mise à jour

- ◆ GET /lpupdate (+ paramètres)
- ◆ Les paramètres amusants :
 - unique et instance : identifiants de la clé ?
 - capacity et used : volume total de la clé, volume utilisé effectivement sur la partition flash.
 - apps : nombre d'applications « u3-isées » installées.
- ◆ Récupère un fichier XML définissant la mise à jour (ou son absence)

10

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

Fichier de mise à jour

```
<u3updatemanifest>
<LPUpdateAvailable>0</LPUpdateAvailable>
<LPUpdateVersion></LPUpdateVersion>
<LPUpdateProtocolVersion>1.0
</LPUpdateProtocolVersion>
<AddressURL></AddressURL>
<description></description>
<ReleaseWebPageURL />
</u3updatemanifest>
```

11

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

Universal Customizer

- ◆ www.hak5.org/packages
- ◆ Version modifiée de LPInstaller, qui permet
 - De créer une image ISO9660 avec « ce que l'on souhaite dedans »
 - D'écrire une image sur la partition CD d'une clé U3
- ◆ ATTENTION :
 - parfois ça marche, parfois moins (clés SanDisk // clés EMTEC ?)
 - risque de perte des données de la partition flash

12

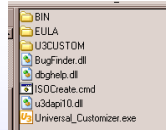
Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

Organisation et utilisation

◆ Procédure complète :

- Placer les fichiers dans le répertoire u3custom.
- Exécuter ISOCreate.
- Puis Universal_Customizer



◆ Procédure abrégée :

- Placer une image ISO9660 nommée U3CUSTOM.ISO dans le répertoire BIN
- Exécuter Universal_Customizer.

13

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

Déroulement

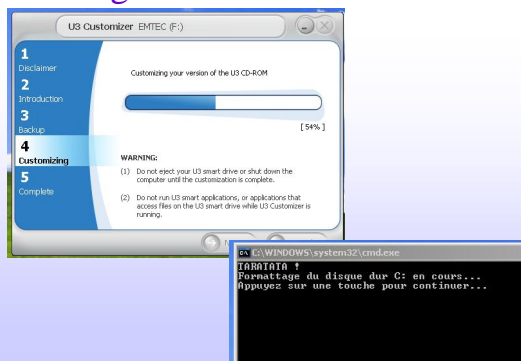
- ◆ Recherche d'une clé USB U3.
- ◆ Sauvegarde des données de la partition flash (fichier ZIP avec mot de passe demandé à l'utilisateur).
- ◆ Formattage de la partition CD.
- ◆ Ecriture de l'image U3CUSTOM.ISO.
- ◆ Restauration des données de la partition flash.
- ◆ NOTE : le programme en AUTORUN peut être exécuté durant la procédure !

14

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

En images



15

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

Hacksaw

- ◆ wiki.hak5.org/wiki/USB_Hacksaw
- ◆ Extraction automatique du contenu de toutes les clés USB connectées au système « infecté ».
- ◆ Envoi des documents vers un compte Gmail.
- ◆ Propagation possible vers une autre clé U3.
- ◆ Utilise USBDumper, Blat, Stunnel (et Gmail).

16

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

SwitchBlade

◆ wiki.hak5.org/wiki/Switchblade_Packages :

- ensemble de programmes que l'on peut ajouter sur la partition CDFS
- Avec des fonctionnalités très diverses

- 6 ArmingID saming the drive
- 6 Switchblade Kill Switch
- 7 Systems Info
- 8 Dump SAM
- 9 Product Key
- 10 Internet Explorer Password Grabber
- 11 Windows Update Lister
- 12 Network Password Dumper
- 13 CacheDump
- 14 Installer
- 15 Port Scan
- 16 Messenger password Dumper
- 17 IE History Viewer
- 18 Prefetch Password Stealer
- 19 Wireless Passwords
- 20 Dhalup Password Dump
- 21 Usname Insider
- 22 Editing Send.bat (and stunnel.conf)
- 23 Silent VNC Installer (with external IP send)
- 24 Reverse VNC Connection
- 25 USB H2K Saw
- 26 Internal IP Mapper
- 27 Folding@Home Installer
- 28 Folder Popper (to show trash)
- 29 Netcat Bindshell
- 30 Netcat Reverse Shell
- 31 Truesynt
- 32 Automated Backup and Restore
- 33 Connect the Switchblade towards a special computer

17

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007

Des questions ?

- ◆ Le PDF de la présentation est disponible (sur une clé USB...)

18

Pierre-Yves BONNETAIN - pyb@ba-cst.com - (0) 567 040 403

ReSIST 27/11/2007