Du Python, du Bash, un Raspberry Pi et des clefs USB

Kitten Groomer, le nettoyeur de clé USB.

CIRCL
Computer Incident
Response Center
Luxembourg

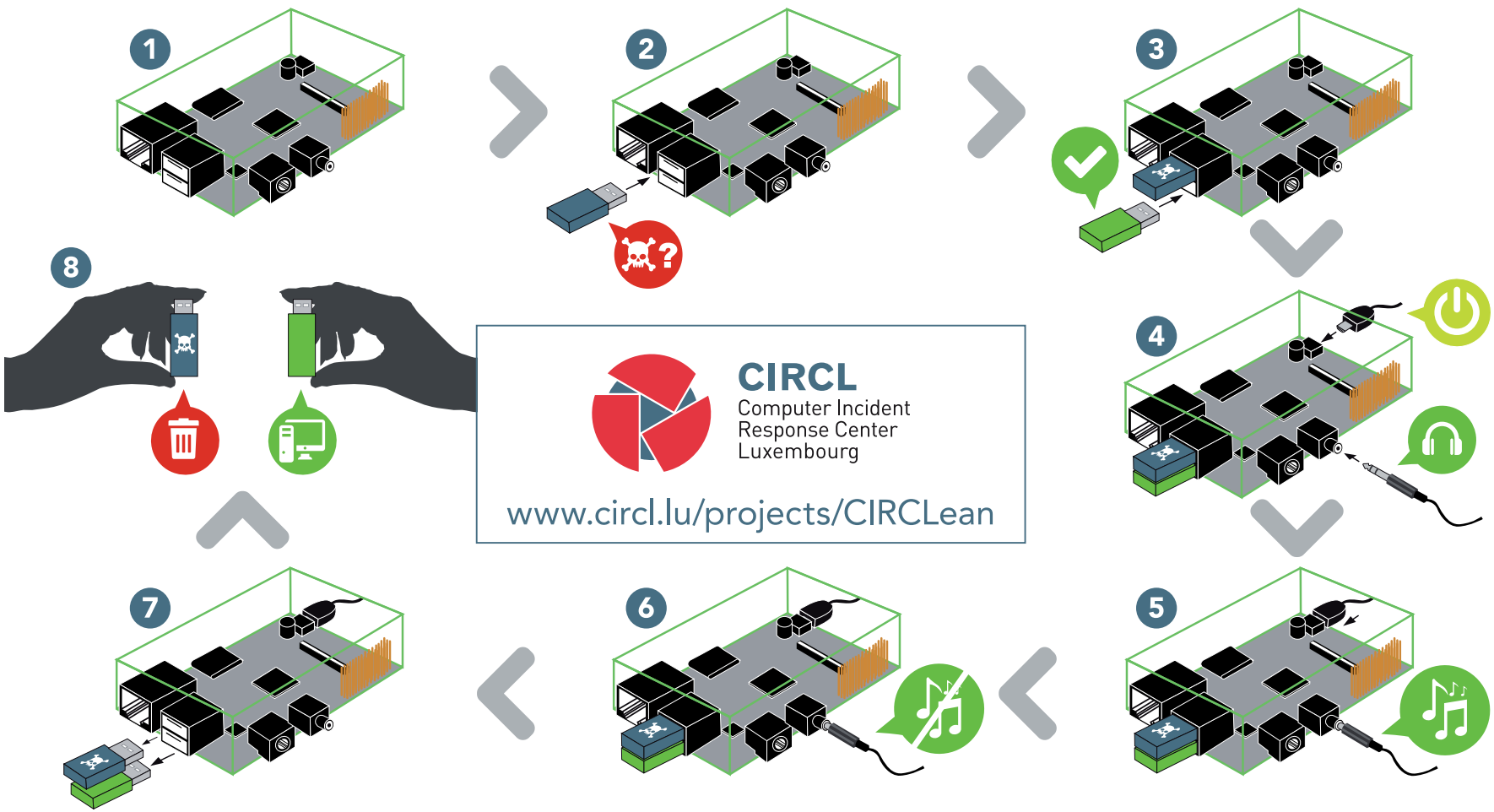
TLP:WHITE

info@circl.lu

June 17, 2015

Contexte

- Une clef USB est une boite noire
- Tout le monde utilise des clefs USB
- Les antivirus ne detectent pas plus de 60% des virus
  - Sans parler des attaques ciblées
- Il faut un outil simple


1
2
3
4
5
6
7
8
CIRCL
Computer Incident
Response Center
Luxembourg
www.circl.lu/projects/CIRCLean

Exemples d'utilisation

- Journaliste travaillant sur des documents tombés du camion
- Étudiant.e travaillant sur un ordinateur de l'école/université
- En famille, avec des ami.e.s pour échanger des photos
- En déplacement professionel/conférence pour échanger des documents

Avantages

- Ordinateur dédié et non connecté à un réseau
- Portable
- Fonctionne sur du matériel grand public
- ... avec un OS grand public (Raspbian)
- Pas cher

Qu'est ce que ca fait

- Renomme les executables Windows
- Croise les types MIME et les extensions
- Converis les docs office en PDF/A puis en HTML
- Converis les PDFs en PDF/A puis en HTML
- Extrait les archives
- Renomme le autorun.inf sur la clef source

Choix techniques

- Altération aussi limitée que possible de la clef source
- Clef source et OS en lecture seule
- Conversion sans droits root
- Modifications limitées à l'OS
- Conversion basée sur les types MIME

Challenges

- Le KittenGroomer est une série de scripts...
- ... avec un OS complet
- ... pas mal de dépendances.
- ... et qui doit fontionner sur Raspberry B, B+ et 2.
- Il doit couvrir un grand nombre de cas (systeme de fichier, formats...)
- ... et les erreurs pouvant arriver.

Implémentation

- Tout dernier Rasbpian (supporte toutes les version de rPi)
- 7z pour extraire les archives
- GhostScript pour la conversion PDF vers PDF/A
- Libreoffice / unoconv pour la conversion *office vers PDF/A
- pdf2htmlex pou la conversion des PDF/A en HTML

PyCIRCLean

- Passage de Bash à Python
- Module python installable indépendament
- Beaucoup plus flexible
- Implémentez votre propre outil! (2 sont disponibles)

PyCIRCLean - En detail

- 50 lignes de code pour copier une liste prédéfinie d'extensions
- Installable sur un ordinateur fixe
- Fonctionne en Python 2 et en Python 3
- Logging

Problèmes principaux

- Génération automatique d'images
- Tests sur environnements virtuels réalistes (uniquement rPi B pour l'instant)
- Test unitaires sur une batterie de fichiers
- Support des erreurs (clef pleine, crash en conversion....)
- Plus d'utilisateurs

Futur

- Kiosque pour entreprise
- Tests automatiques
- Support de plus de types fichiers
- Interface Web?
- Connection directe à un serveur de mail
- ...

Code source

- **Open source (BSD)**
  - Les scripts pour construire une image:
  - https://github.com/CIRCL/Circlean
  - Le module python (2 et 3) utilisable ou bon vous semble:
  - https://github.com/CIRCL/PyCirclean
- **Tutorial**
  - http://circl.lu/projects/CIRCLean/

Contact

- raphael.vinot@circl.lu
- https://www.circl.lu/
- OpenPGP fingerprint: 8647 F5A7 FFD3 50AE 38B6 E22F 32E4 E1C1 33B3 792F
- Document suspicieux? N'hésitez pas contacter CIRCL.