CIRCLean - USB key sanitizer

Some bash, some python, a RaspberryPi, and a lot of glue.

CIRCL
Computer Incident
Response Center
Luxembourg

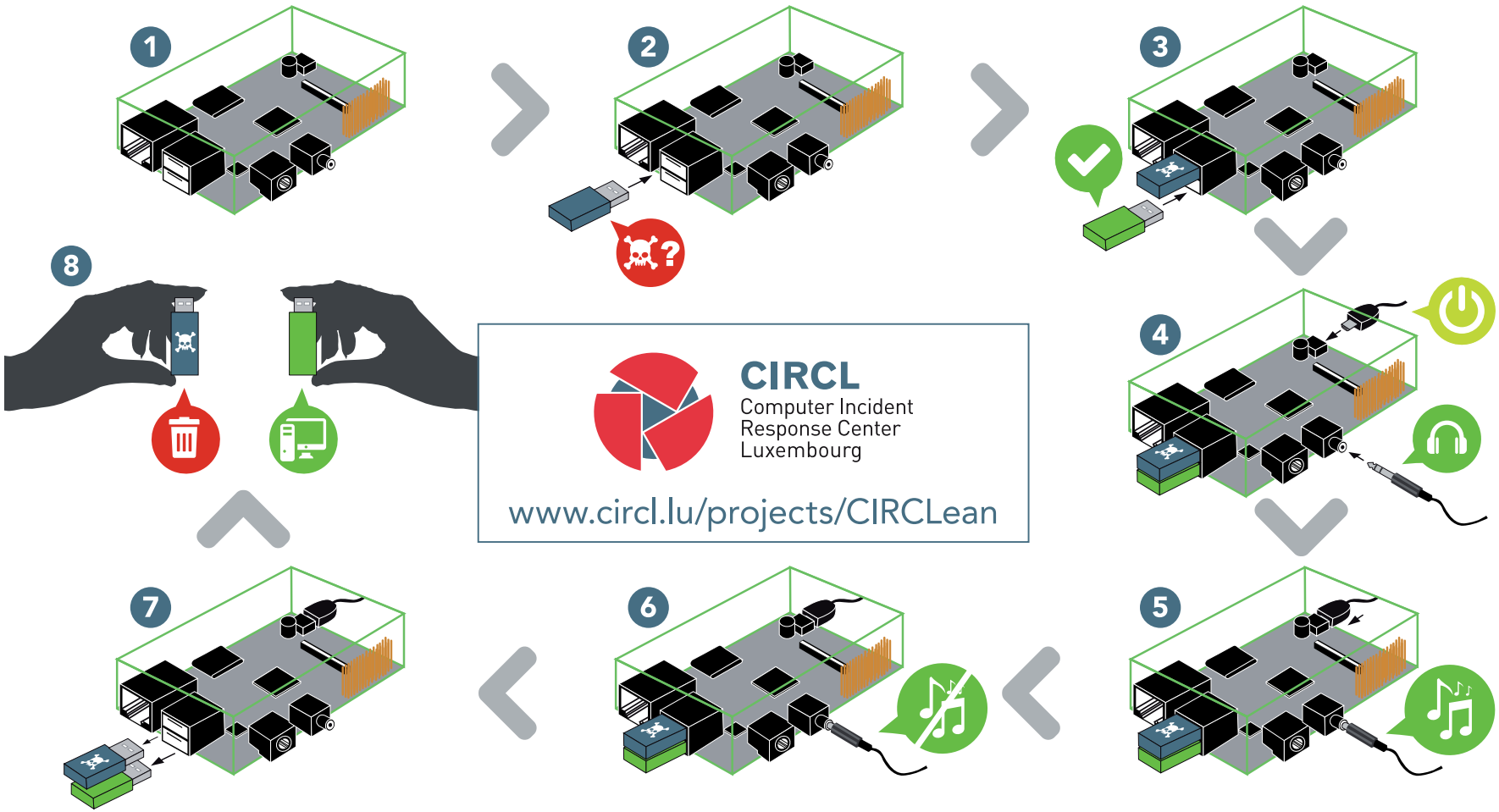
TLP:WHITE

info@circl.lu

July 7, 2015

Context

- An USB key is a blackbox
- We all use USB keys
- Antiviruses won't detect more than 60% of common malwares
  - Without talking of targeted attacks
- We need a simple tool


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

Usage

- A journalist receiving documents on a USB key
- A Student working on a computer at school/university
- Within the family, to exchange pictures
- In a business trip, at a conference, to exchange documents

Advantages

- Dedicated and air-gaped computer
- Portable
- Run on an off-the-shelf device
- ... and an off-the-shelf Operating system (Raspbian Jessie)
- Cheap

What does it do?

- Rename Windows executables
- Cross-check MIME types with current extension of the file
- Convert office documents to PDF/A and then to HTML
- Convert PDFs to PDF/A and then to HTML
- Extract the archives and process the content
- Rename the autorun.inf on the source key

Technical decisions

- (Almost) no changes on the source key
- Source key and OS mounted as RO during processing
- Processing as user
- Bare operating system
- Processing based on the MIME types

Challenges

- CIRCLean is a bunch of scripts...
- ... with a will OS
- ... many dependencies
- ... and that has to work on Raspberry B, B+ and 2.
- Has to cover a lot of different cases (files systemes, file formats...)
- ... and all the faillures modes.

Implementation

- Most recent version of Rasbpian (support all versions of rPi)
- 7z to extract archives
- GhostScript for converting PDF to PDF/A
- Libreoffice / unoconv to convert *office to PDF/A
- pdf2htmlex to convert PDF/A to HTML

PyCIRCLean

- Reimplementation of the project as a Python module (2.7 and 3*)
- Usable on a desktop
- Two existing processing scripts (generic and simple copy)
- Helpers to make it simple (log, copy, rename...)
- Implement your own tool
- 50 lignes of code to copy a predefined list of extensions

Main issues

- Automatically generate images, with your own scripts?
- Automated testing on realistic virtual environments (and not just rPi B)
- Unit tests on known files
- Error handling (key full, crash during a conversion...)
- We need more users

Future

- Desktop for offices
- LEDs to give a visual feedback to the user
- Automated tests
- Support of more files formats
- Web Interface
- Postfix plugin

Source code

- **Open source (BSD)**
  - Scripts to build an image:
  - https://github.com/CIRCL/Circlean
  - Python module (2.7 and 3*) installable where ever you want:
  - 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
- Found suspicious documents? Don't hesitate to contact CIRCL.