CIRCLean

The agnostic USB sanitizer

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL - *TLP:WHITE*

info@circl.lu

November 8, 2013

A bit of context

- **USB keys are very usefull**
  - And we will not stop using them
- **USB keys are exchanged between people all the time**
  - In the family, between friends, at events...
- **USB keys are a major infection vector**
  - Infected computer or malicious intent
- **USB keys are blackboxes**
  - No way to know before it is in your computer
- **Antivirus softwares catch at most 60% of the malwares**
  - And almost 0% on a targeted attack

How to fix those issues

- **Do not rely on an antivirus**
  - assume the files are potentially malicious
- **No guessing**
  - All the documents of the same type are handle the same way
- **Safe environment**
  - Airgraped, no critical information and read only device
- **Portable**
- **Easy to use**
- **Not (too) suspicious**

How to use the CIRCLean

- Unplug the device
- Plug the untrusted key in the top slot
- Plug your own (empty and big enough) key in the bottom slot
- Plug the SD card
- Plug the power cable
- Plug a headset
- Wait until the headset does not produce any sound (can take some time)
- Unplug the power
- Plug the bottom USB key into your computer

What it actually does

- Windows executables are renamed
- Office documents are converted to PDF and then HTML
- PDF are converted to HTML
- Archives are extracted (and the content processed)
- autorun.inf on the source key are renamed
- All the other documetns are simply copied
- It plays a bunch of MIDI files during the copy

Internals

- OS: Bare Raspian, up-to-date
- Office documents processed with Libreoffice
- PDFs processed with pdf2htmlEX (use libpoppler)
- 7z is used to unpack archives
- Script runs as user
- Matching based on MIME type
- Source key is read only after the check for autorun
- SD card read only all the time (hardware switch is recommended)
- Destination key mounted with noexec, nosuid and nodev

Known issues, and ideas for the workshop...

- Only work on keys formated in FAT32
- Could be easyer to install (NOOBS?)
- Lack of documentation
- No debian package
- Code review
- Just use it and tell me what is not working!

Code and Links

- **Open source (BSD)**
  - Contains all the scripts to build your own image
  - https://github.com/CIRCL/Circlean
  - https://github.com/Rafiot/KittenGroomer
    - for the issues, and the funny name
- **Prebuild and ready-to-flash image**
  - http://circl.lu/files/2013-11-05_CIRCLean.img.bz2
- **Tutorial**
  - http://circl.lu/projects/CIRCLean/