CIRCLean: The agnostic USB sanitizer

A small, cute and opensource device to improve your security

CIRCL
Computer Incident
Response Center
Luxembourg

TLP:WHITE

info@circl.lu

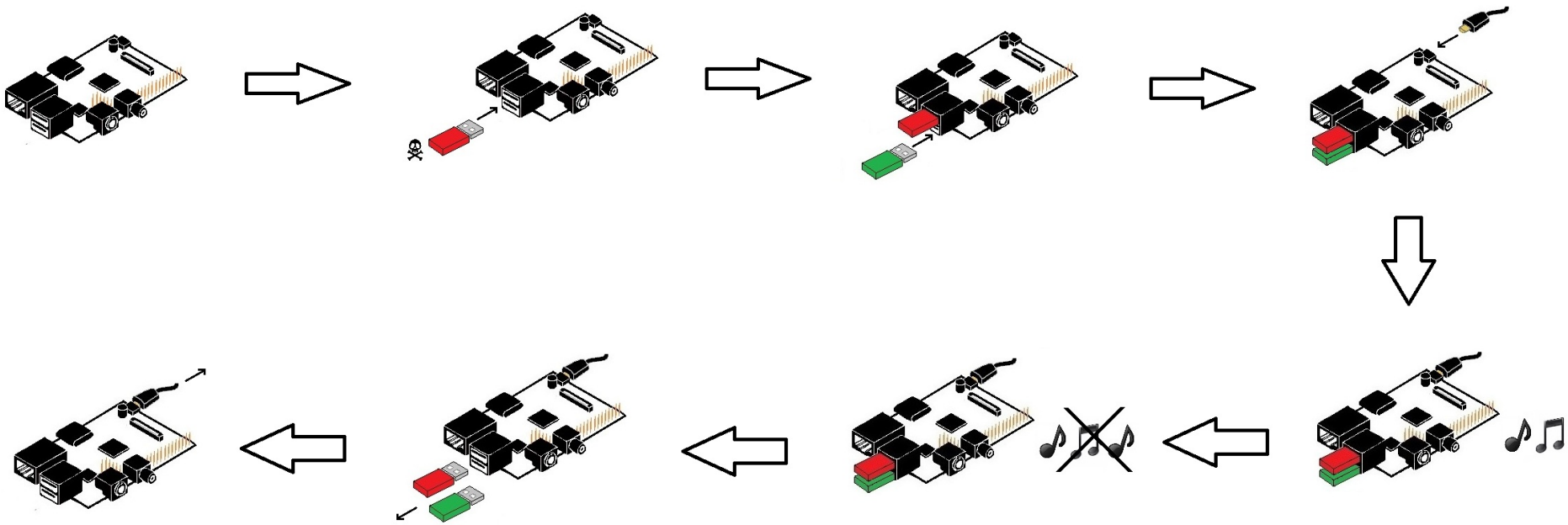
July 9, 2014

Overview

- USB keys are a major infection vector
- USB keys are blackboxes
- Antivirus catch at most 60% of the commons malwares
  - And almost 0% on a targeted attack
- The main targets are not-that-techie people

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**
  - Air gapped, no critical information and read only device
- **Portable**
- **Easy to use**



Usecases

- Politician in a foreign country
- Employee at a conference, visiting clients...
- Student copying his work from a shared computer
- USB Key found on the street
- Journalist
- Involved citizens
- You

CIRCLean is

- Easy and safe way to have a look at the content of a USB Key
- Air gapped system
- Portable
- Run on an off-the-shelf device
- ... and an off-the-shelf Operating system (Raspbian Jessie)
- Cheap
- Agnostic

CIRCLean is not

- Clever
- An antivirus
- The solution to all your security issues

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 documents are simply copied
- It plays a bunch of MIDI files during the copy

Technical part

Choices

- No modifications on the source key
  - Remove autorun.inf
- Source key and filesystem read only
- Conversion as user
- Bare operating system
- MIME types

Challenges of the testings

- CIRCLean is a bunch of scripts...
- ... but also a full operating system
- ... with many dependencies.
- ... and runs on ARM (arm1176)
- Covering all the cases (file-systems, files formats...)
- ... and all the failure modes.

Requirements

- As close as possible to reality
- ... but without needs to flash a SD card at each commit
- Without infecting myself
- No changes in the scripts
- Possibility to reproduct the results between runs
- Everything has to be virtual

What does "everything" means?

- Operating system
  - Did you know that arm1176 in qemu has no poweroff capability?
- USB keys (source and destination)
- Multiple partitions
- Multiple File systems
- ... also broken and unsupported ones
- ... and what about too small keys?
- ... or broken ones?

Creating a virtual USB key

- 1. Creating the file
  - dd if=/dev/zero of=fs.img bs=516096c count=200
- 2. Setting up the label
  - parted -s fs.img mklabel msdos
- 3. Creating a partition
  - parted -s fs.img mkpart primary 8192s 201599s
- 4. And finally creating the filesystem
  - losetup -o$((8192 * 512)) /dev/loop0 fs.img
  - mkfs.vfat /dev/loop0
- The repository has scripts to handle multiple partitions and other FS

Running the tests

- Running the virtual USB keys in the virtual operating system
- ... without poweroff
- Expect to the rescue.
- Qemu can redirect the serial output to stdout
- ... and has a monitoring interface
  - 1. wait until "System halted." shows up
  - 2. send quit to the monitoring interface
  - 3. win.

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
- **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.