KittenGroomer

The agnostic USB sanitizer

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL - *TLP:WHITE*

info@circl.lu

December 19, 2013

A bit of context

- **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

Use cases

- 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

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**
- **Off the shelf, standard device**

How to use the KittenGroomer

Figure : Just plug the keys

What it actually does

- Windows executables are renamed
- All documents that libreoffice can open 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

Code and Links

- **Open source (BSD)**
  - Contains all the scripts to build your own image
  - https://github.com/Rafiot/KittenGroomer
    - for the issues, and the funny name
  - https://github.com/CIRCL/Circlean
- **Prebuild and ready-to-flash image**
  - http://circl.lu/files/2013-12-09_CIRCLean.img.bz2
- **Tutorial**
  - http://circl.lu/projects/CIRCLean/