# IoT Malware Analysis Demo

Luxeria
29.04.2020

# What about


https://blog.malwarebytes.com/101/2017/12/internet-things-iot-security-never/

# What about

- **Tiny computers**
  - Usually Linux
  - Usually ARM / MIPS
- **Connected to Internet**
- **Usually no direct user interaction**
- **Usually no tight security *(«S» in IoT is for security)***

  **→ Interesting botnet target**

# https://github.com/Phype/telnet-iot-honeypot

- **Emulates linux shell**
- **Binds to telnet port**
- **Exposed directly to internet**
- **Accept *any username:password***
- **Collect stats and downloaded files**
- **Hot target:**
  - Collected 100+ distinct samples in a few days
  - ~ 2 – 3 new samples per hour

# How does it look like

- **Malware = *Malicious Software***
- **Binary format**
- **Machine and platform specific**

```
> xxd /tmp/hello_world.json
00000000: 7b0a 0922 7a6f 6f22 3a20 5b0a 0909 2266  {.."zoo": [..."f
00000010: 6f6f 223a 2022 6261 7222 0a09 5d0a 7d0a  oo": "bar"..].}.
```

```
> xxd malware/telnet-iot-honeypot/samples/b3428816758477771f013595b1ef
00000000: 7f45 4c46 0101 0103 0000 0000 0000 0000  .ELF............
00000010: 0200 2800 0100 0000 4005 0100 3400 0000  ..(.....@...4...
00000020: 0000 0000 0200 0004 3400 2000 0300 2800  ........4. ...(.
00000030: 0000 0000 0100 0000 0000 0000 0080 0000  ................
00000040: 0080 0000 2d97 0000 2d97 0000 0500 0000  ....-...-.......
00000050: 0080 0000 0100 0000 e018 0000 e098 0200  ................
```

# Analysing the sample: Tools

- **Dedicated reverse engineering tools**
  - Radare2
  - Ghidra
  - IDA
  - Binary Ninja
- **General hacker tools**
  - Emulators
  - Unpackers
  - Binutils

# Analysing the sample: Methods

- **General reverse engineering techniques**
  - Disassembly / Decompilation of machine code
  - Flow / Call Graphs
  - API calls (syscalls)
- **Malware often uses tricks**
  - Anti Debugging
  - Packers
  - Obfuscation
- **Needs pratice but can be learned (no black magic)**

# Lets do it!

# Questions?