



# How To Bring HID Attacks To The Next Level

Luca Bongiorni  
14<sup>th</sup> October 2017

# Overview

-  @LucaBongiorni
- In Omnia Silendo Ut Audeam Nosco
- After this presentation, you will:
  - Be (even) more afraid of USB devices;
  - Learn about new tools for pranking your colleagues, pwn customers & scare CISOs;
  - Trash your Rubberducky and BashBunny
  - Not trust anymore your USB Dildo and Pump Breast!



# Human Interface Devices

“A **human interface device** or **HID** is a type of computer device usually used by humans and takes input and gives output to humans.” — Wikipedia

- Keyboard, Mouse, Game Controllers, Drawing tablets, etc.
- Most of the times don't need external drivers to operate
- Usually whitelisted by DLP tools
- Not under Antiviruses' scope



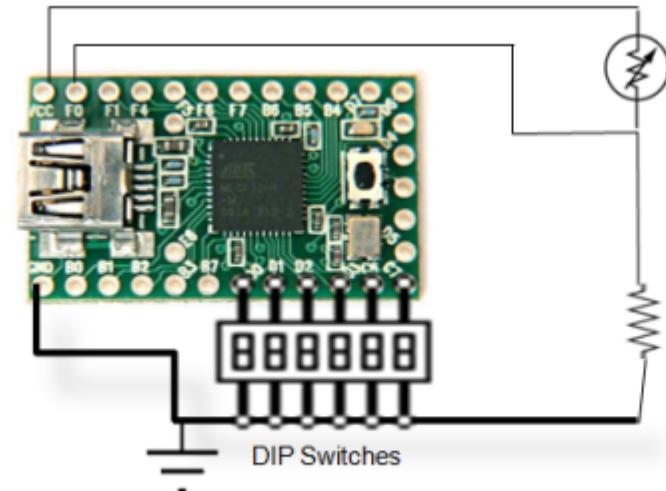
## What could go wrong?



# State of Art – 1<sup>st</sup> Generation

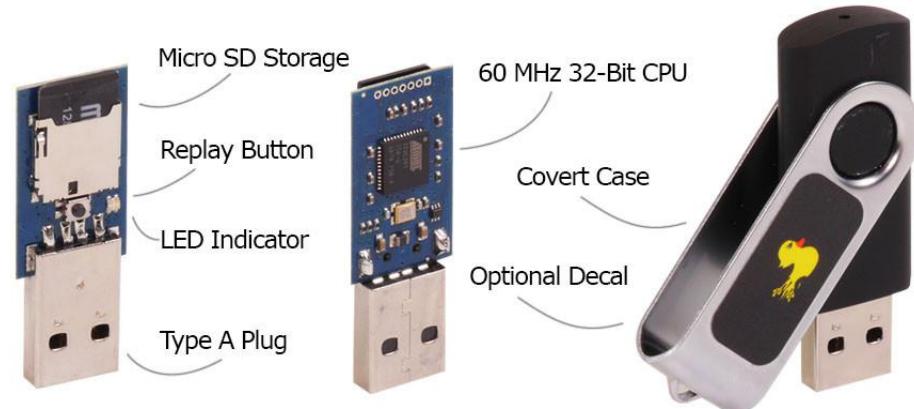
- **Teensy – (PHUKD 2009 & Kautilya 2011)**

- DIY Solution
- Multiplatform (Win, \*nix, OSX)
- Multipayload (through DIP-Switches)
- Cheaper (25 €)



- **Rubberducky (2010)**

- Dedicated Hardware
- Multiplatform (Win, \*nix, OSX)
- Can emulate Keyboard & USB Disk
- Multipayload (CAPS-INS-NUM)
- Changeable VID/PID
- Expensive (55 €)



# State of Art – 2<sup>nd</sup> Generation

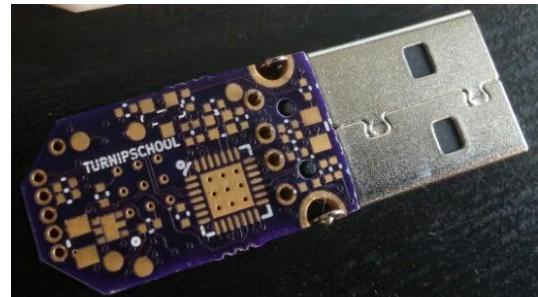
- **BadUSB (2014)**

- It exploits the controllers (i.e. Phison) within commercial USB devices and turns them into a covert keystrokes injecting device.



- **TURNIPSCHOOL (2015)**

- Is a hardware implant concealed in a USB cable. It provides short range RF communication capability to software running on the host computer. Alternatively it could serve as a custom USB device under radio control.



# State of Art – 3<sup>rd</sup> Generation

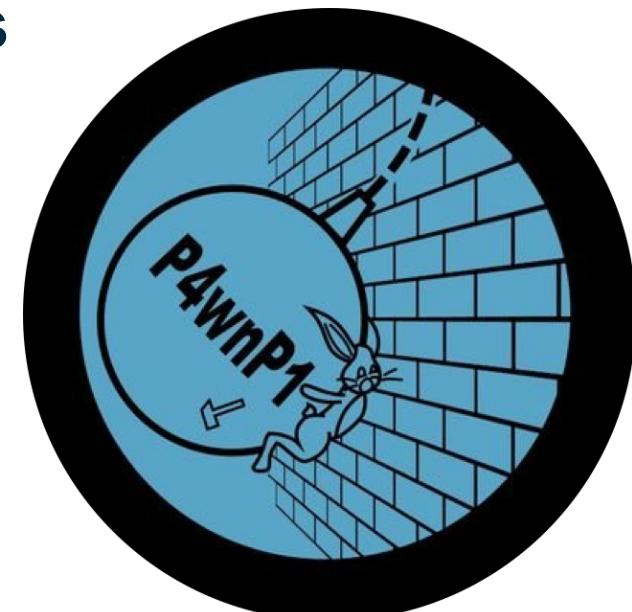
- **WHID Injector (2017) – A Rubberducky on Steroids**

- Dedicated Hardware
- Multiplatform (Win, \*nix, OSX)
- Changeable VID/PID
- Has WiFi
- Cheap (11 €)



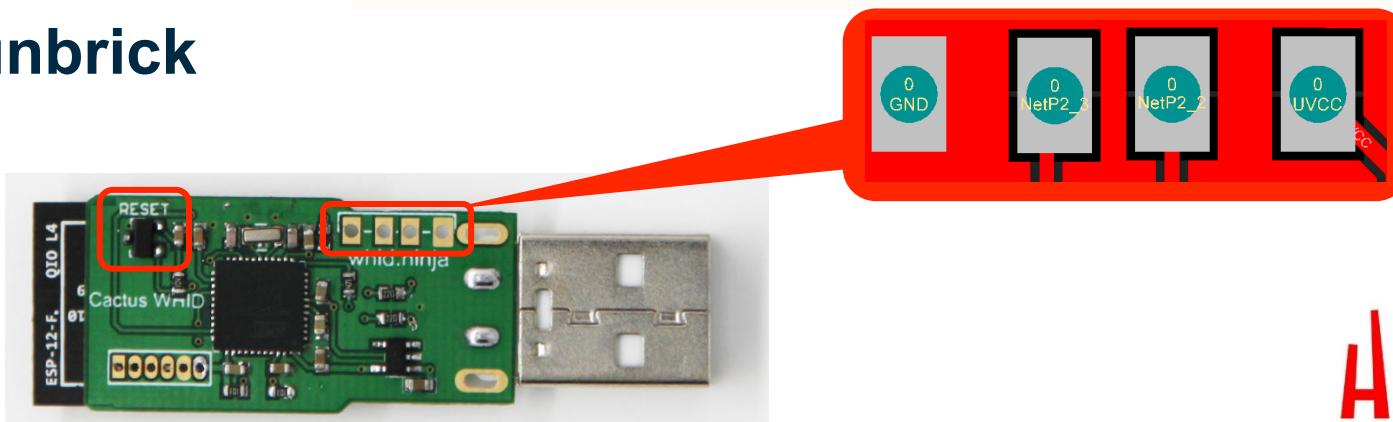
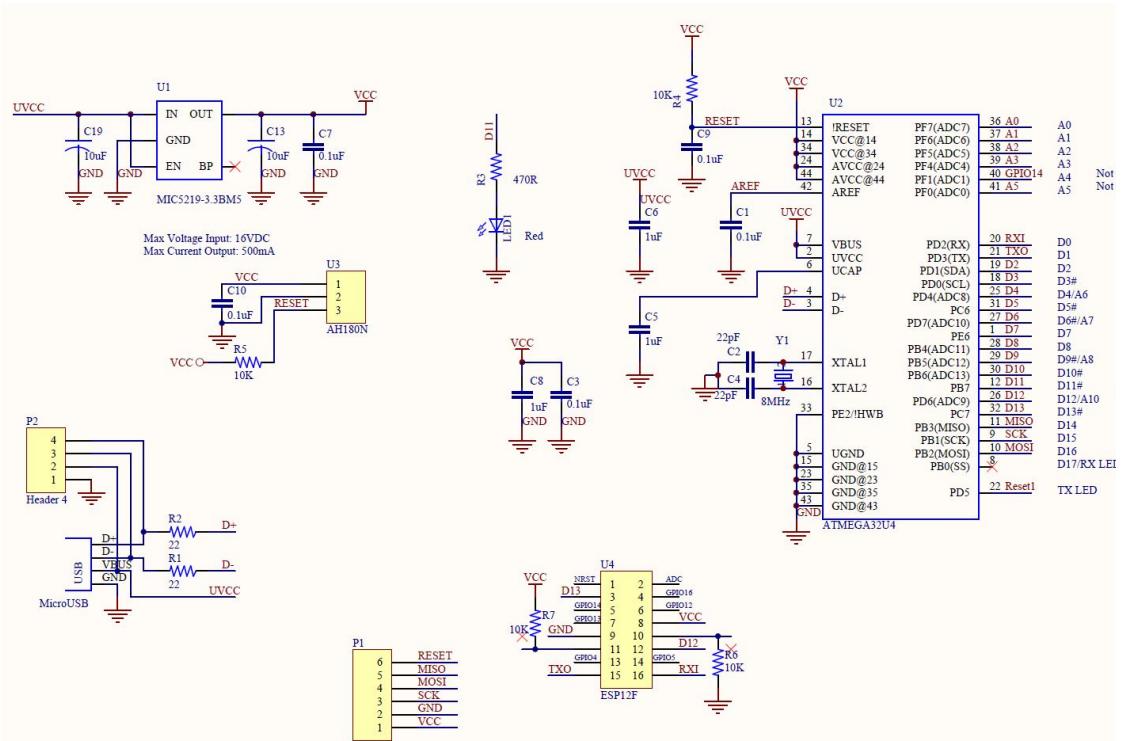
- **P4wnP1 (2017) – A BashBunny on Steroids**

- Based on RPi Zero W (~15 €)
- Has WiFi and USB to ETH
- It can emulate USB Key FileSystem
- Autocall Back to C2
- Changeable VID/PID
- And many other cool features!



# WHID Injector – Schematics & Specs

- Atmega 32u4
  - Arduino-friendly
- ESP-12
  - WiFi (both AP and Client modes)
  - TCP/IP Stack
  - DNS Support
  - 4MB Flash
- Pinout for weaponizing USB gadgets
- HALL Sensor for easy unbrick



# Weaponizing USB Gadgets



HACKINBO

# What's Next?

**Test for Social Engineering weaknesses within your target organization (e.g. DLP policy violations) and to bypass physical access restrictions to a Target's device!**

We've offered the companies budget-saving solutions for the past 10 years.

PLACE STAMP HERE

John Smith, CPO  
Piazza La Bomba e Scappa 1  
Rome, 10100 Italy

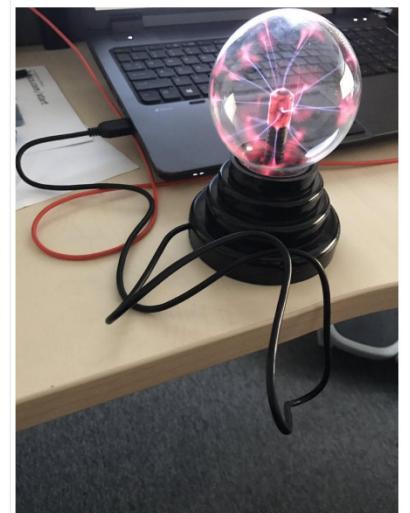
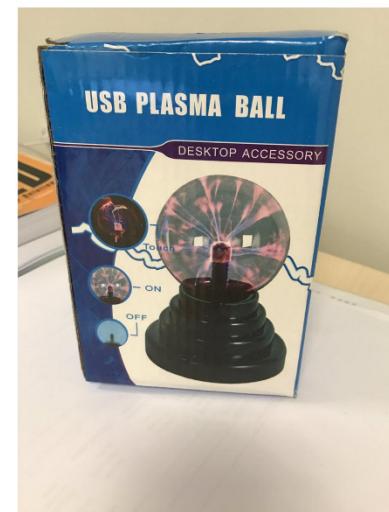
"We recommend Contoso to anyone who will listen to us because they're the best!"

- Mike Simms, CPO Microsoft

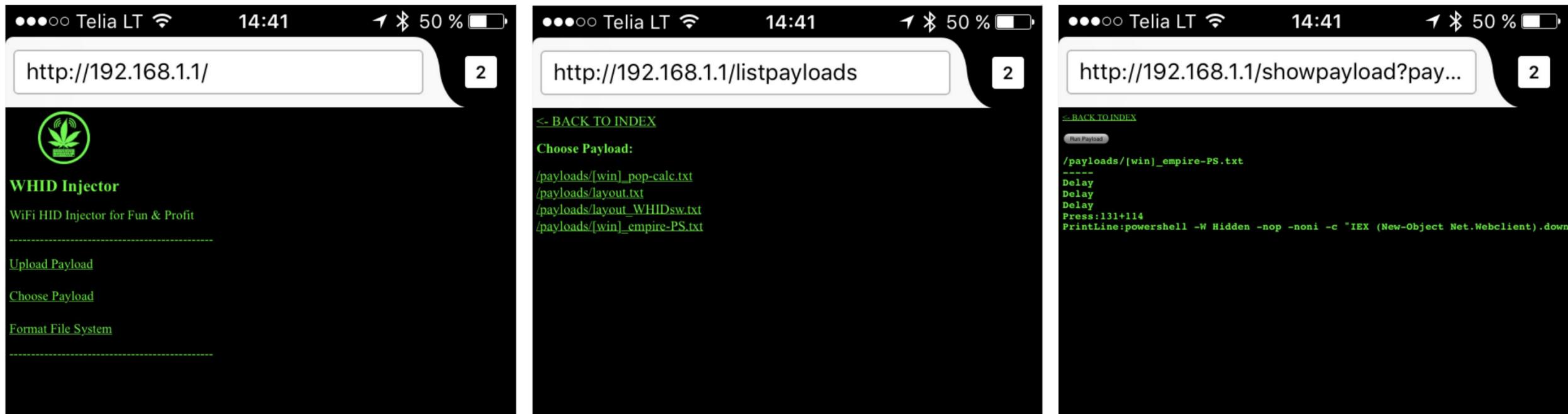
Contoso, Inc.  
1337 Main Street  
Raleigh, NC 27604-0000

Leader in Office Supplies

**contoso**



# WHID Injector – WHID GUI



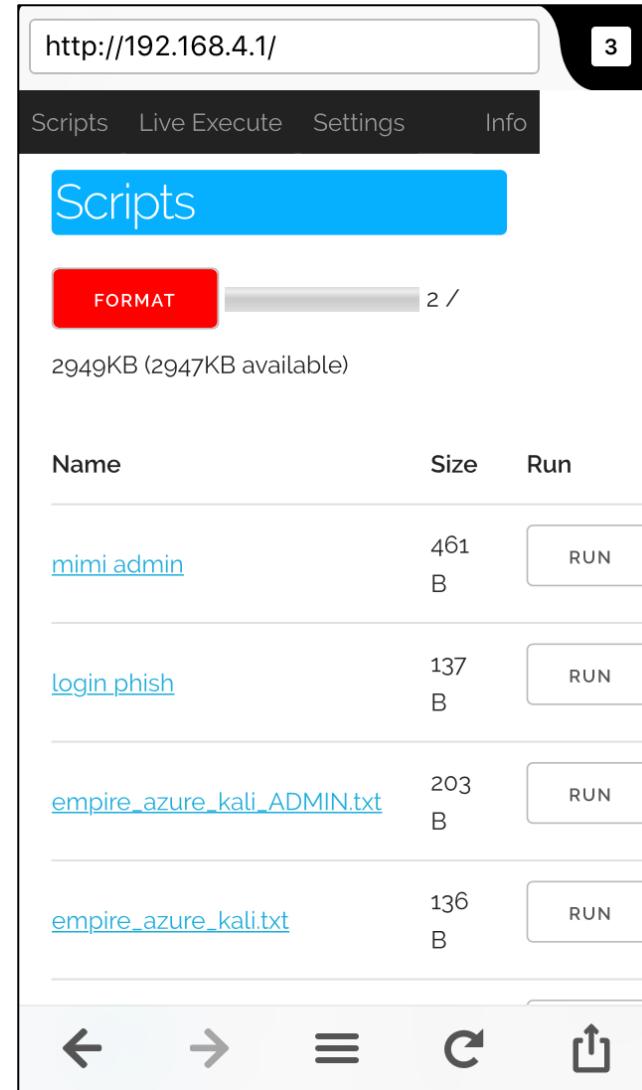
- Basic GUI
- Multi OS (Win, OSX, \*nix)
- Hardcoded WiFi Settings (Need to recompile Fw)
- Hidden SSID (if needed)
- No Live Payloads
- Changeable VID/PID

# Some Cool Payloads Against Windows 10 Enterprise



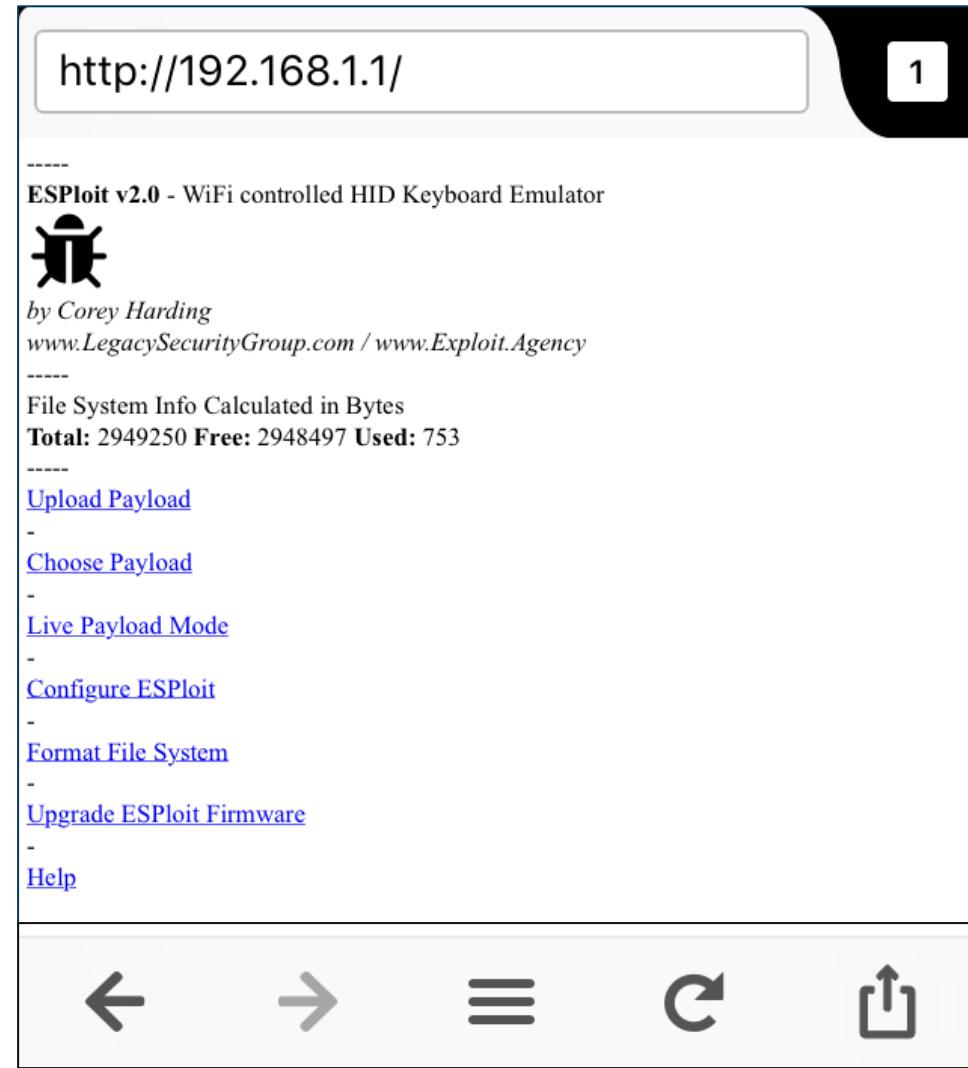
# WHID Injector – WifiDucky GUI

- Hidden SSID (if needed)
- Multi OS (Win, OSX, \*nix)
- AutoStart Function
- Fancy GUI
- Change settings on-the-fly
- Live Payloads
- Update FW on-the-fly
- Changeable VID/PID



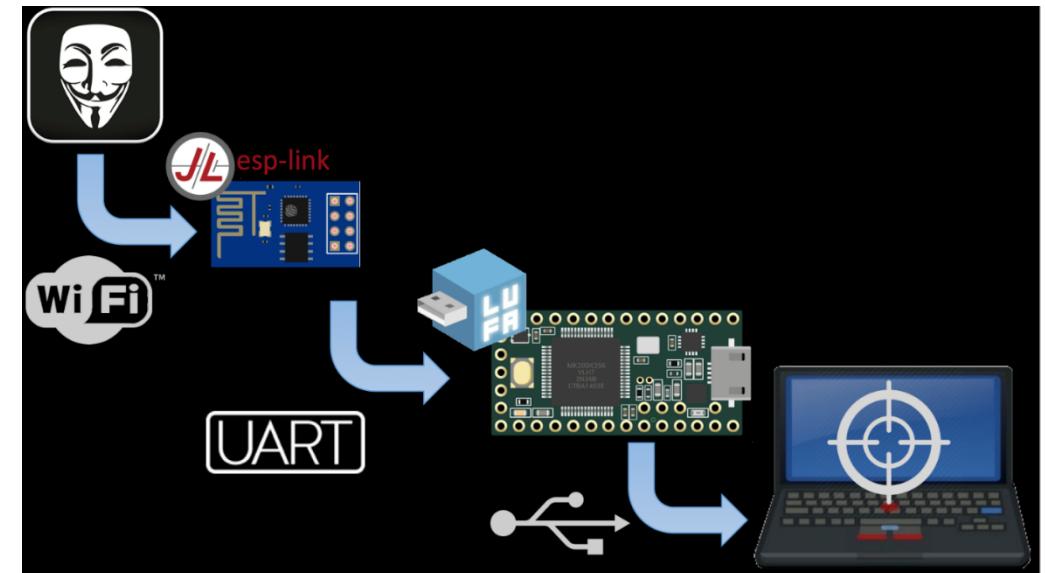
# WHID Injector – ESPloitV2 GUI

- Evolution of WHID GUI
- Shipped w/ Cactus WHID
- Hidden SSID (if needed)
- ESPortal Credentials Harvester
- Multi OS (Win, OSX, \*nix)
- Autostart Function
- Change settings on-the-fly
- Live Payloads
- Update FW on-the-fly
- Changeable VID/PID



# WHID Injector – USaBuse

- Bypass Air-Gapped restrictions
- Once connected to a PC:
  - Creates a WiFi AP
  - Injects PoSH scripts that creates a HID RAW as exfil channel to transfer data back.
  - Returns a CMD shell to the attacker
  - GAME OVER





Recycle Bin



McAfee  
AntiVirus Plus



Windows 8.1 Enterprise Evaluation  
Windows License valid for 90 days  
Build 9600



11:15 AM  
8/5/2016

```
(~/code/USaBuse)
```

The terminal window shows a file tree starting from the current directory (~). The path ~/code/USaBuse is highlighted in green. The cursor is located at the end of the path entry field.

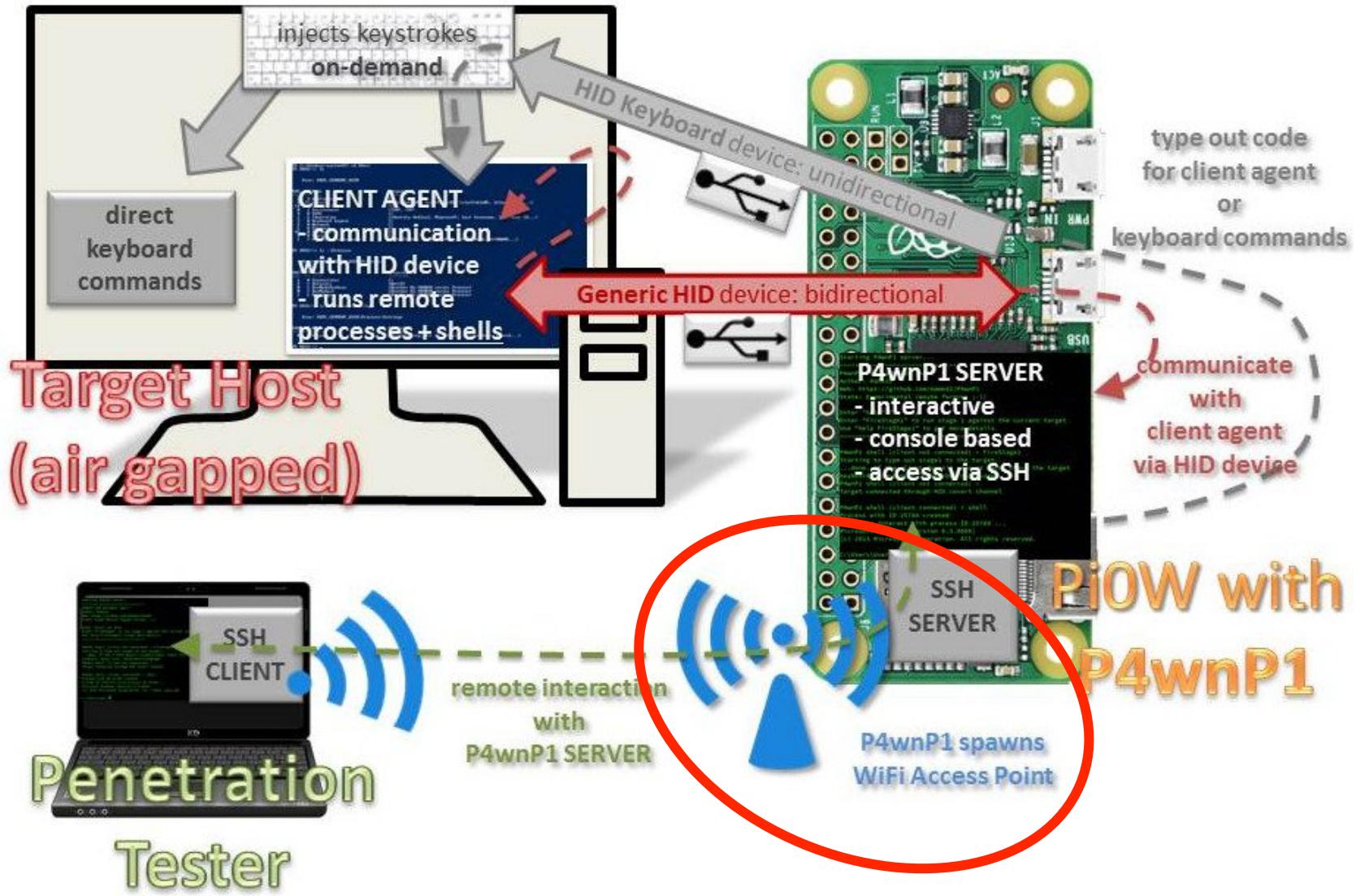
<https://youtu.be/5gMvtUq30fA>

# P4wnP1 – Operating Features

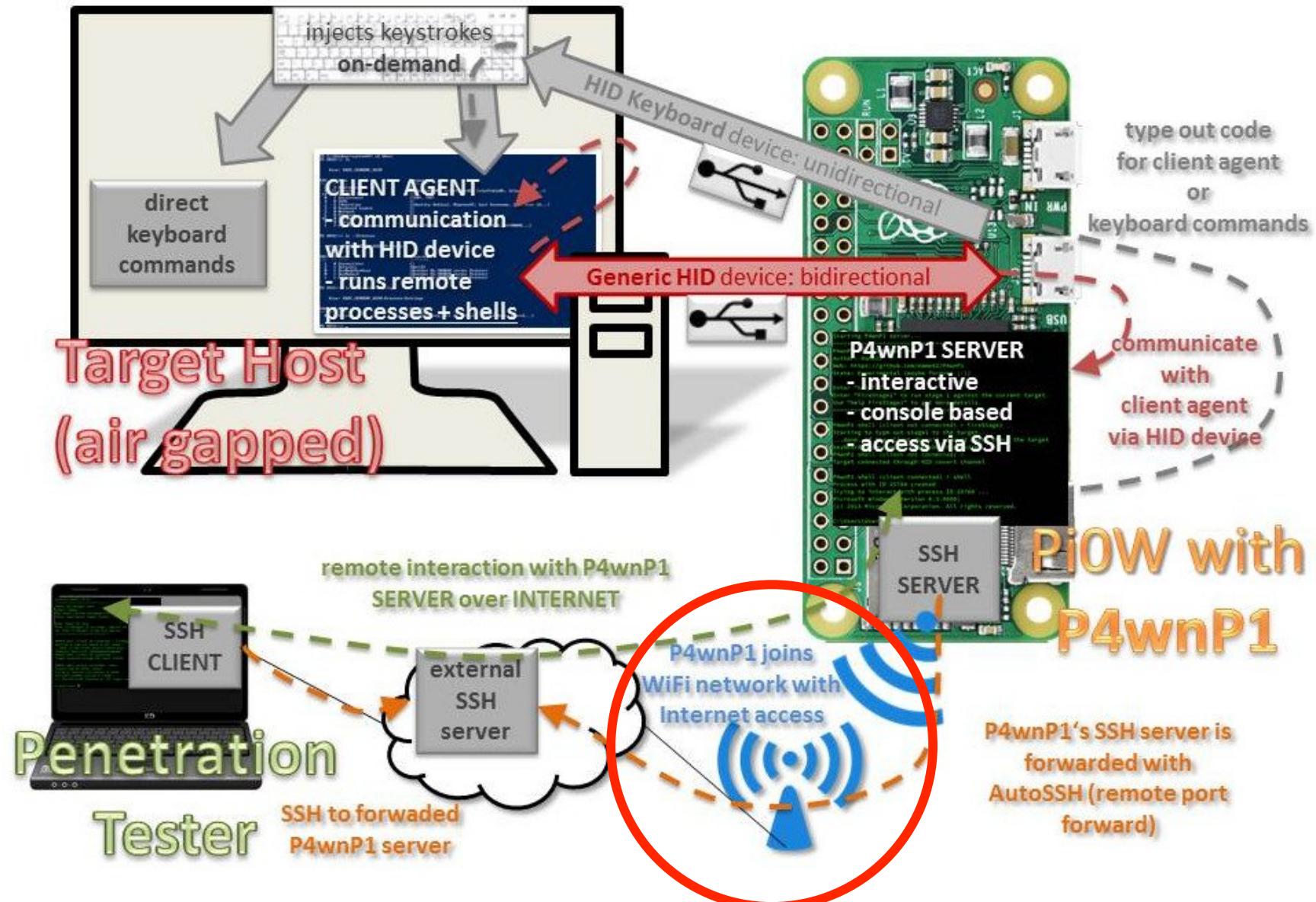
- **Bypass Air-Gapped restrictions**
  - Uses a HID RAW as exfil channel to transfer data back (~32Kb/s)
  - The HID backdoor can call back a remote C&C (in case of a weaponized gadget & a known WiFi network available)
- **Supports RubberDucky Scripts**
  - Can also be triggered by CAPS-, NUM- or SCROLL-LOCK interaction on target
- **Win10 Lockpicker**
  - Steals NetNTLMv2 hash from locked Windows machine, attempts to crack the hash and enters the plain password to unlock the machine on success



# AirGap Bypass – On Premises



# AirGap Bypass – Remote Call C&C



# P4wnP1 – Hide & Seek



```
Starting P4wnP1 server...
=====
P4wnP1 HID backdoor shell
Author: MaMe82
Web: https://github.com/mame82/P4wnP1
State: Experimental (maybe forever ;-))

Enter "help" for help
Enter "FireStage1" to run stage 1 against the current target.
Use "help FireStage1" to get more details.
=====

P4wnP1 shell (client not connected) > FireStage1
Starting to type out stage1 to the target...
...done. If the client doesn't connect back, check the target
keyboard layout with 'SetKeyboardLanguage'
P4wnP1 shell (client not connected) >
Target connected through HID covert channel

P4wnP1 shell (client connected) > shell
Process with ID 25784 created
Trying to interact with process ID 25784 ...
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Luca.Bongiorni>
```

A screenshot of a terminal window showing a HID backdoor shell session. The session starts with the server's startup message and then receives multiple 'client connected' messages. It then runs the 'FireStage1' command, which is described as starting to type out stage1 to the target. The session ends with a successful connection message and a Microsoft Windows command prompt.



- > Computer
- > Disk drives
- > Display adapters
- > DVD/CD-ROM drives
- > Human Interface Devices
- > IDE ATA/ATAPI controllers
- > IEEE 1394 host controllers
- > Imaging devices
- > Keyboards
- Memory technology devices
  - JMicron PCIe SD Host Controller
  - JMicron PCIe SD/MMC Host Controller
- Mice and other pointing devices
  - HID-compliant mouse
  - Synaptics SMBus TouchPad
- Modems
- Monitors
- Network adapters
- Ports (COM & LPT)
  - ECP Printer Port (LPT1)
  - Intel(R) Active Management Technology - SOL (COM4)
- Print queues
- Processors
- Security devices
- Software devices
- Sound, video and game controllers
- Storage controllers
- System devices
- Universal Serial Bus controllers
  - Generic USB Hub
  - Generic USB Hub
  - Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D
  - Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26
  - Intel(R) USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
  - Microsoft Mouse and Keyboard Detection Driver (USB)
  - USB Composite Device
  - USB Root Hub
  - USB Root Hub
  - USB Root Hub (xHCI)

Windows Defender

PC status: Protected

Home Update History Settings Help

Your PC is being monitored and protected.

Scan options:

Quick

Full

Custom

Scan now

Real-time protection: On

Virus and spyware definitions: Up to date

Scan details

Last scan: 9/5/2017 at 3:50 PM (Full scan)

The Windows Defender application window is open, showing the 'Home' tab. It displays a green checkmark icon indicating 'Your PC is being monitored and protected.' Below this, two status indicators are shown: 'Real-time protection: On' and 'Virus and spyware definitions: Up to date'. On the right side of the window, there are 'Scan options' buttons for 'Quick', 'Full', and 'Custom', with 'Quick' selected. A 'Scan now' button is also present. At the bottom left, a 'Scan details' section shows the last scan was performed on 9/5/2017 at 3:50 PM, and it was a 'Full scan'.



Target's Air-Gapped Computer



<https://youtu.be/7fCPsb6quKc>

# Prologue - The TETRA “deal”

**CPU:** 533 MHz MIPS 74K Atheros AR9344 SoC

**Memory:** 64 MB RAM

**Disk:** 2 GB NAND Flash

**Wireless:** Atheros AR9344 + Atheros AR9580

**Ports:** 4 SMA Antenna, **RJ45 Fast Ethernet**, Ethernet over USB, Serial over USB, USB 2.0 Host, 12V/2A DC



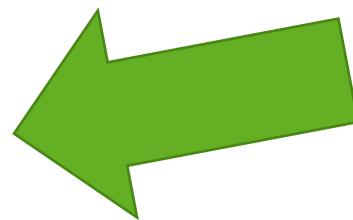
WIFI PINEAPPLE TETRA

€250.00

Add to Cart

## DETAILS

- Basic Edition includes the WiFi Pineapple TETRA, Antennas, and USB Y-Cables.
- WE DO NOT STOCK TACTICAL EDITION



# Prologue – The PowerPwn “deal”

**CPU:** 1.2 GHz ARM CPU

**Memory:** 512 MB RAM

**Disk:** 2GB NAND Flash + 16 GB SD card storage

**Wireless:** WiFi, Bluetooth, 3g Modem

**Ports:** 2x RJ45 Gigabit Ethernet, USB 2.0 Host, UART



## Power Pwn

\$1,995.00

THE POWER PWN HAS BEEN DISCONTINUED and has been replaced with the [Pwn Plug R2](#).

Building on the game-changing success of the Pwn Plug, the Power Pwn is a fully-integrated, patent-pending, enterprise-class penetration testing platform.

- Ingenious form-factor and highly-integrated/modular hardware design
- Covers the entire spectrum of a full-scale pentesting engagement, from the physical-layer to the application-layer



# The Reaction



My carpenter with 15 euro  
makes it better!

# Pentest Dropboxes Everywhere

1<sup>st</sup> Generation (2006) – Price ~ 30 €



3<sup>rd</sup> Generation (2016) - Price < 15 €



2<sup>nd</sup> Generations (>2011) – Price 40~200 €



# What's Next?



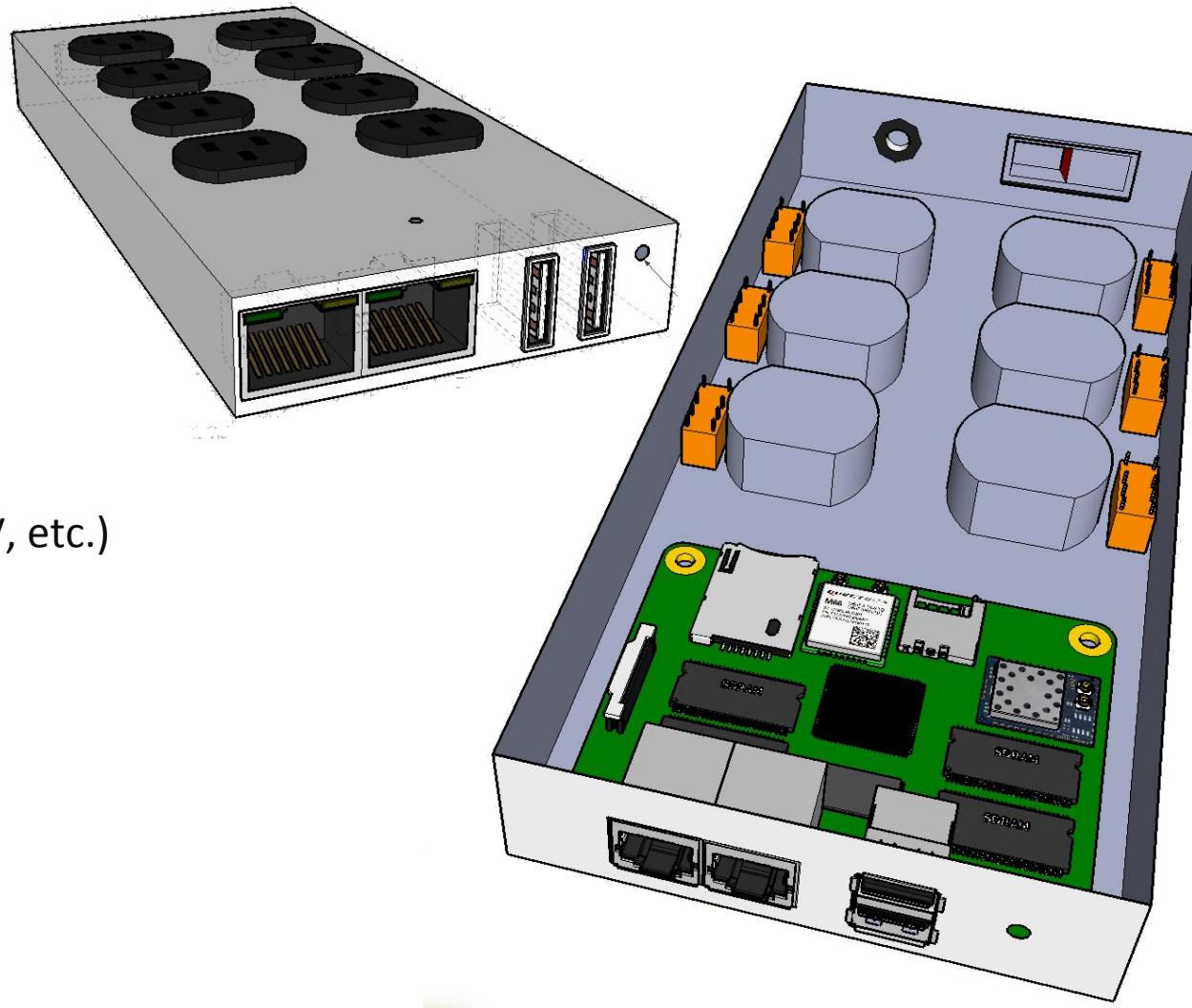
**Penetration Over The {Air, Ethernet} box**

# POTÆbox – Penetration Over The {Air, Ethernet} box

- Quad-core CPU ARM
- 2gb RAM
- 8gb NAND
- 2x Gigabit Ethernet Ports (for MiTM, NAC Bypass, etc.)
- 2x USB 2.0 Ports
- Embedded Microphone
- Embedded Camera (at least, connector for it)
- 2G/3G Module (w/ SIM card slot)
- uSD card slot
- Atheros Wifi Chipset ( 2x space permitting)
- Relays controlled by GPIOs (to remotely control lights, TV, etc.)
- HDMI in & out (for HDMI MiTM) – WIP

## POTAEbox Purposes:

- Security Operations (i.e. Penetration Tests)
- Surveillance (i.e. Mic & Camera)
- Network Appliance (i.e. Firewall, IDS, Honeypot)
- Home Automation (i.e. Lights)
- Generic Electronic Projects



Please Share!



<http://share.potaibox.com>

HACKINBO

# Resources

- <http://whid.ninja>
- <https://medium.com/@LucaBongiorni/>
- <https://github.com/exploitagency/ESPloitV2>
- <https://github.com/sensepost/USaBUSe>
- <https://github.com/mame82/P4wnP1>
- <https://github.com/mossmann/cc11xx/tree/master/turnipschool>
- <https://srlabs.de/bites/usb-peripherals-turn/>
- <https://hakshop.com/products/usb-rubber-ducky-deluxe>
- <https://nsa.gov1.info/dni/nsa-ant-catalog/usb/index.html>



Special thanks to [@RoganDawes](#) and [@exploit agency](#) for their help!

**Fin.**