




# HOW TO R&D HACKING TOYS



## FOR FUN & NO-PROFIT



# Overview

-  @LucaBongiorni
- After this presentation, you will know:
  - How challenging & painful is to create hacking devices
  - What to do if you have an idea and wanna bring it to life
  - What to avoid in order to increase chances of success
  - About WHID Injector, WHID Elite and the upcoming POTAEbox



# Once Upon a Time... Many Engagements Ago...

I wanted to turn this weaponized Mouse into a remotely controlled one.

Sadly, I failed for many reasons:

- Lack of time (as usual)
- Lack of a small-enough RF RTX
- Not enough space in a mouse.

Eventually, the idea ended up in my never-ending TODO list. Until...



UNIVERSAL  
SERIAL ABUSE

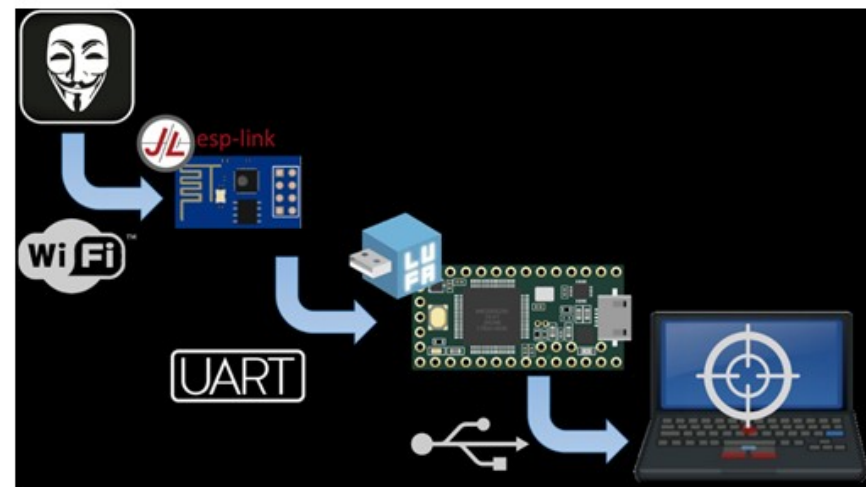
Defcon 24

Rogan "BFG" Dawes

Dominic "singe" White

# UNIVERSAL SERIAL aBUSE

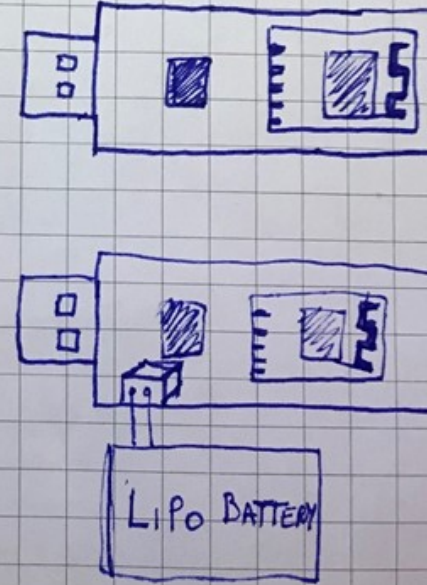
- Developed by [@RoganDawes](#) in 2016
- Bypass Air-Gapped restrictions
- Once connected to a PC:
  - Creates a WiFi AP
  - Stealthy Screensaver Killer
  - Injects PoSH scripts that creates a HID RAW as exfil channel to transfer data back.
  - Returns a CMD shell to the attacker
  - GAME OVER



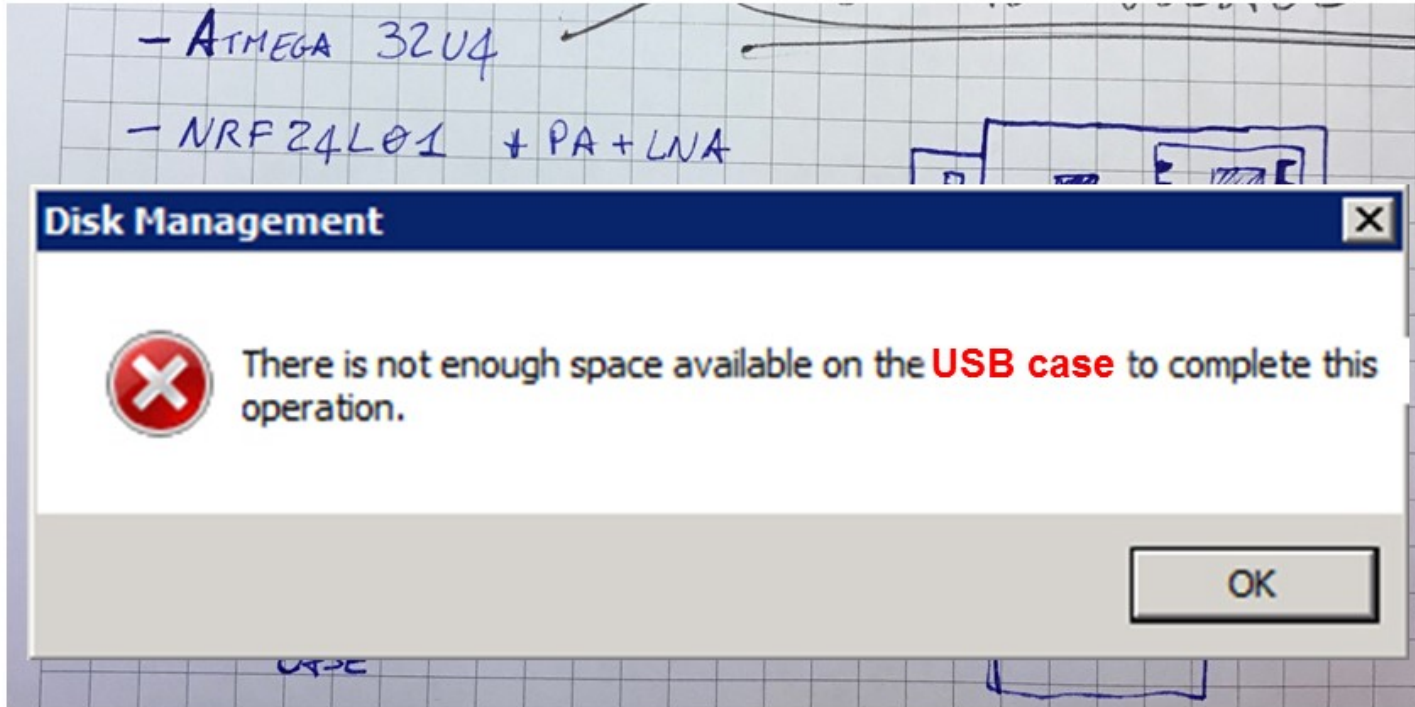


# Initial Concept

- ATMEGA 32U4
- NRF24L01 + PA + LNA
- USB-A MALE CONNECTOR
- LiPo CHARGER CIRCUIT
- EXTERNAL ANTENNA
- MULTISCAN/INJECTION
- FAKE/DUMMY PHONE CASE



# Initial Concept



# R&D Hardware

- **Idea:**

- HID Injector remotely controlled + Airgap bypass for Win & **Linux & OSX**
- Compatible also with USaBuse

- **Requirements:**

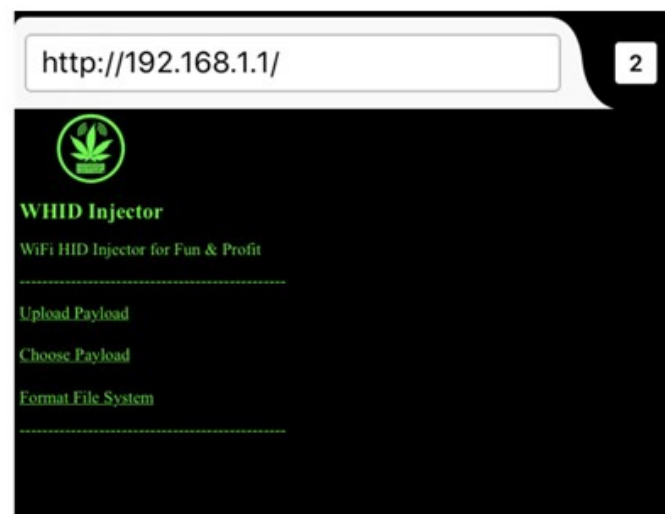
- ESP for remote control
- Atmega 32u4 for:
  - Emulating Keyboard and Mouse
  - Exfiltrating data of AirGapped machine through Serial
- USB Pinout to easily weaponize gadgets

- **PCB Design Tools:**

- CircuitMaker, KiCAD (Free)
- Altium Designer (Paid)

# R&D Software

- Requirements:
  - Able To Emulate Mouse & Keyboard
  - Able to be remotely controlled
  - Able to bypass Air-Gapped environments & Exfil Data
- Started working on SW
- Evaluating Github projects
  - ESPloit V1
  - WifiDucky
  - WiDucky
- Forked ESPloitV1 and Re-Adapted for the prototype HW >> WHID-gui
  - After WHID went to prod, [@exploit\\_agency](#) created ESPloitV2 >> Afterwards, it became Default software delivered with WHID Injector.



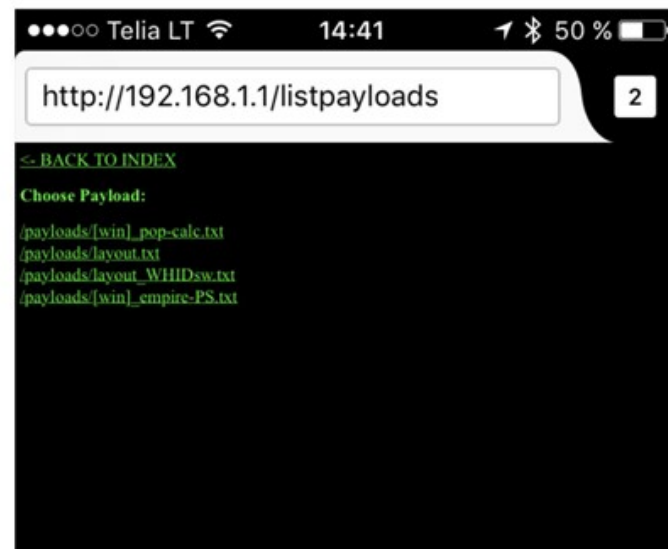
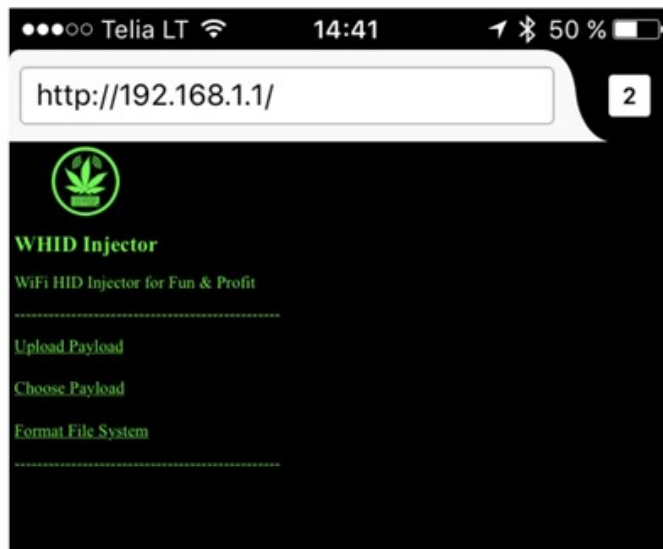


# The Business Un-deal

- The Odyssey Starts
  - Looking for Manufacturer
- The Un-Deal
  - I R&D it
  - I prototype it
  - I QA it
  - You make it
  - You sell it\* worldwide
    - \* At an acceptable price
  - You keep the profit
  - Everyone enjoys it!

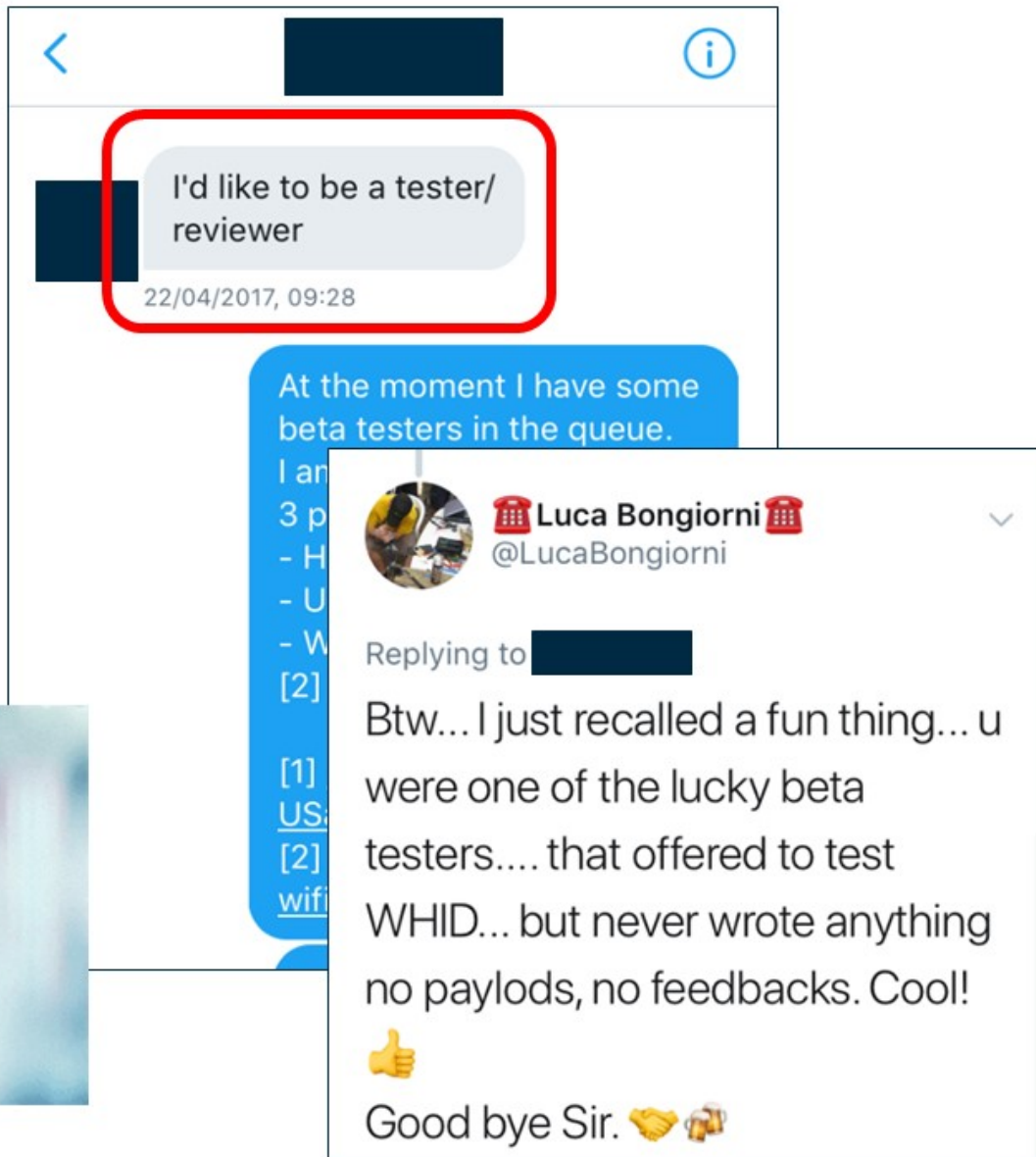


# First working HW & SW



# QA & Beta Test Phase

- **Select Wisely Beta Testers!**
- Most of them will say/promise everything just to get a free cool device!
- Then they'll disappear like "tears in the rain"...



< [Redacted] ⓘ

I'd like to be a tester/ reviewer

22/04/2017, 09:28

At the moment I have some beta testers in the queue.

I am...  
3 p...  
- H...  
- U...  
- W...  
[2]  
[1]  
US:  
[2]  
wif...

Luca Bongiorno  
@LucaBongiorni

Replying to [Redacted]

Btw... I just recalled a fun thing... u were one of the lucky beta testers.... that offered to test WHID... but never wrote anything no payloads, no feedbacks. Cool! 👍

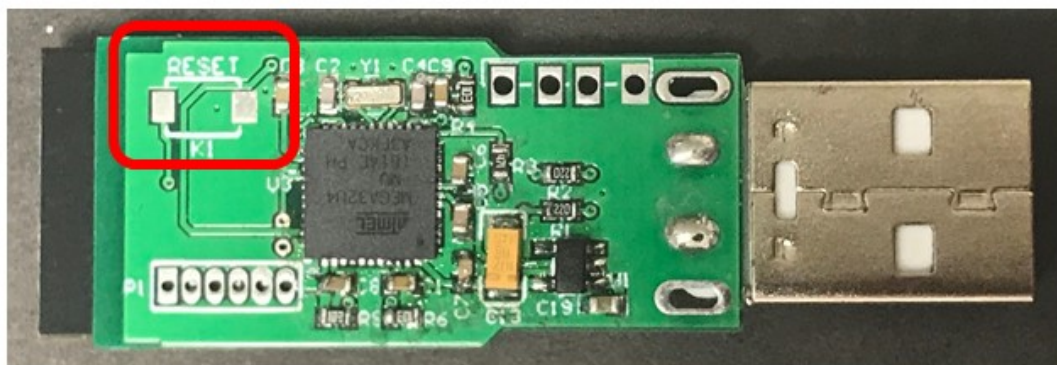
Good bye Sir. 🙌🍷



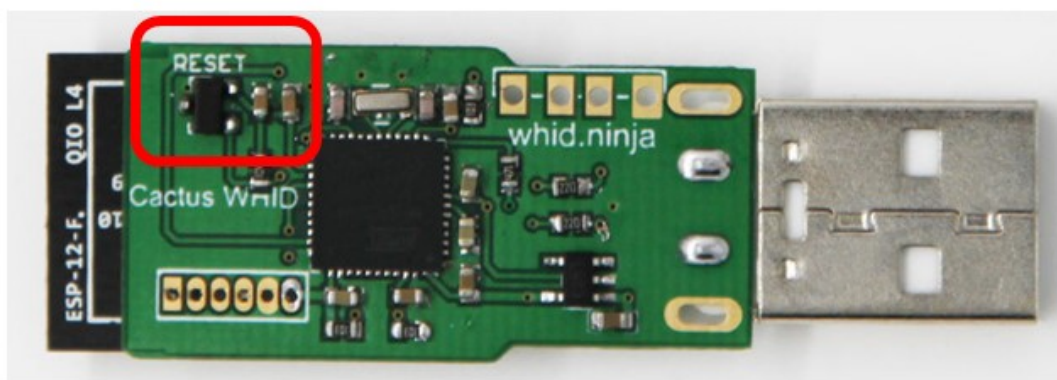
# We Are Getting There! (a.k.a. The 2<sup>nd</sup> Batch)

- HALL Sensor added! (thanks Rogan for the suggestion)

**BEFORE**

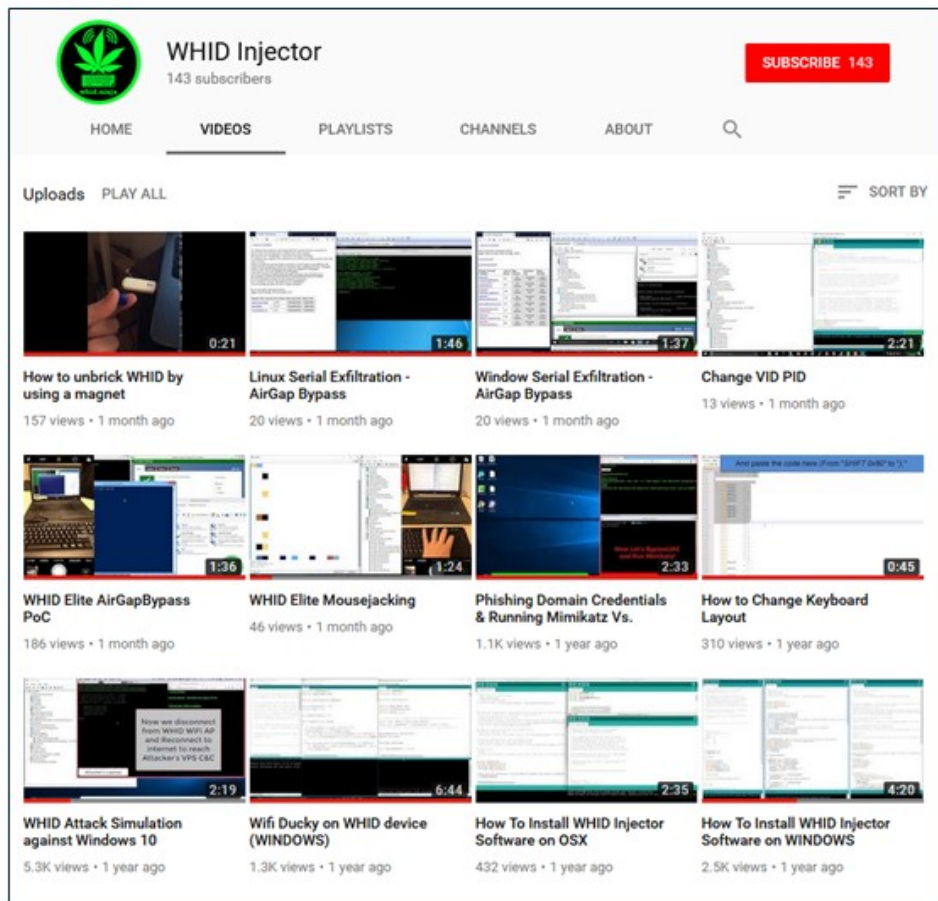


**AFTER**





# The Art of Writing Instructions for the most dumb person on Earth!



The image shows the YouTube channel page for 'WHID Injector'. The channel has 143 subscribers and a 'SUBSCRIBE' button with 143 subscribers. The page is divided into sections: HOME, VIDEOS, PLAYLISTS, CHANNELS, and ABOUT. The 'VIDEOS' section is active, showing a grid of 12 video uploads. The videos are arranged in three rows of four. The first row includes 'How to unbrick WHID by using a magnet' (157 views, 1 month ago), 'Linux Serial Exfiltration - AirGap Bypass' (20 views, 1 month ago), 'Window Serial Exfiltration - AirGap Bypass' (20 views, 1 month ago), and 'Change VID PID' (13 views, 1 month ago). The second row includes 'WHID Elite AirGapBypass PoC' (186 views, 1 month ago), 'WHID Elite Mousejacking' (46 views, 1 month ago), 'Phishing Domain Credentials & Running Mimikatz Vs.' (1.1K views, 1 year ago), and 'How to Change Keyboard Layout' (310 views, 1 year ago). The third row includes 'WHID Attack Simulation against Windows 10' (5.3K views, 1 year ago), 'Wifi Ducky on WHID device (WINDOWS)' (1.3K views, 1 year ago), 'How To Install WHID Injector Software on OSX' (432 views, 1 year ago), and 'How To Install WHID Injector Software on WINDOWS' (2.5K views, 1 year ago).

**WHID Injector**  
143 subscribers

SUBSCRIBE 143

HOME VIDEOS PLAYLISTS CHANNELS ABOUT

Uploads PLAY ALL SORT BY

**How to unbrick WHID by using a magnet**  
157 views • 1 month ago

**Linux Serial Exfiltration - AirGap Bypass**  
20 views • 1 month ago

**Window Serial Exfiltration - AirGap Bypass**  
20 views • 1 month ago

**Change VID PID**  
13 views • 1 month ago

**WHID Elite AirGapBypass PoC**  
186 views • 1 month ago

**WHID Elite Mousejacking**  
46 views • 1 month ago

**Phishing Domain Credentials & Running Mimikatz Vs.**  
1.1K views • 1 year ago

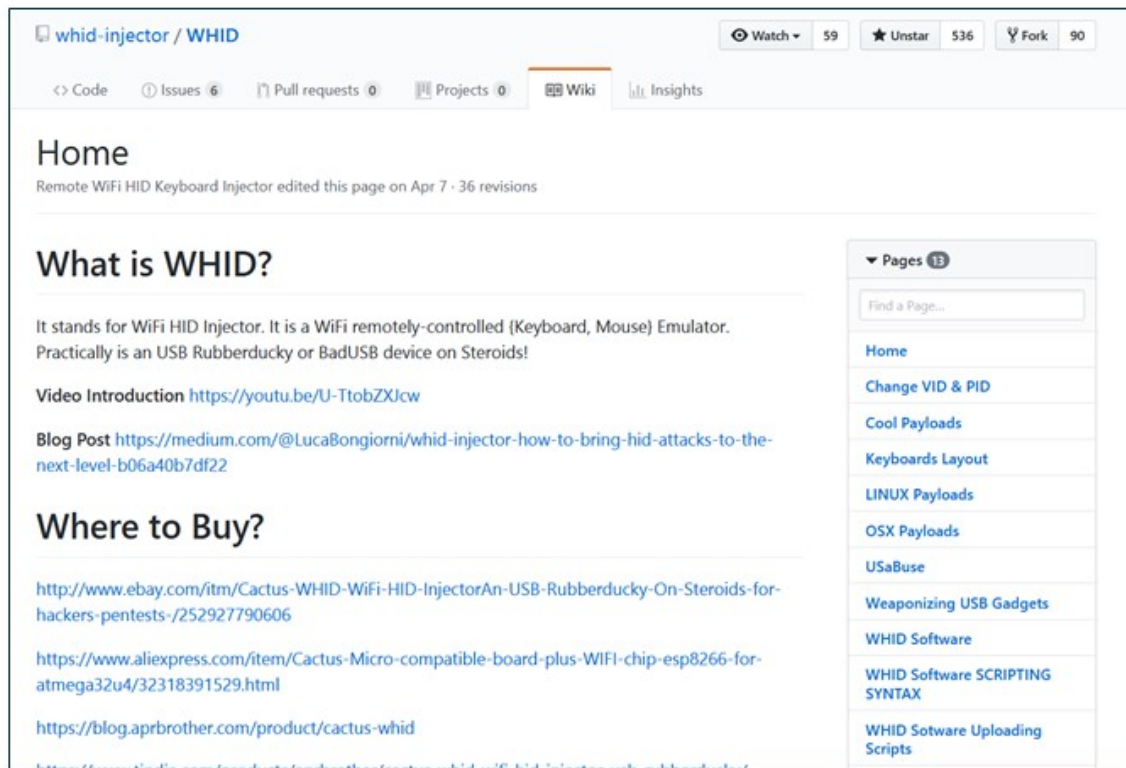
**How to Change Keyboard Layout**  
310 views • 1 year ago

**WHID Attack Simulation against Windows 10**  
5.3K views • 1 year ago

**Wifi Ducky on WHID device (WINDOWS)**  
1.3K views • 1 year ago

**How To Install WHID Injector Software on OSX**  
432 views • 1 year ago

**How To Install WHID Injector Software on WINDOWS**  
2.5K views • 1 year ago



The image shows the GitHub repository page for 'whid-injector / WHID'. The repository has 59 watches, 536 stars, and 90 forks. The 'Wiki' tab is selected, showing the 'Home' page. The 'Home' page has a description: 'Remote WiFi HID Keyboard Injector edited this page on Apr 7 · 36 revisions'. Below the description is a section titled 'What is WHID?' with the text: 'It stands for WiFi HID Injector. It is a WiFi remotely-controlled (Keyboard, Mouse) Emulator. Practically is an USB Rubberducky or BadUSB device on Steroids!'. There are links for 'Video Introduction' and 'Blog Post'. Below this is a section titled 'Where to Buy?' with three links: 'http://www.ebay.com/itm/Cactus-WHID-WiFi-HID-InjectorAn-USB-Rubberducky-On-Steroids-for-hackers-pentests-/252927790606', 'https://www.aliexpress.com/item/Cactus-Micro-compatible-board-plus-WIFI-chip-esp8266-for-atmega32u4/32318391529.html', and 'https://blog.aprbrother.com/product/cactus-whid'. On the right side, there is a 'Pages' sidebar with 13 pages listed: Home, Change VID & PID, Cool Payloads, Keyboards Layout, LINUX Payloads, OSX Payloads, USABuse, Weaponizing USB Gadgets, WHID Software, WHID Software SCRIPTING SYNTAX, WHID Software Uploading Scripts, and WHID Software Uploading Scripts.

whid-injector / WHID

Watch 59 Unstar 536 Fork 90

<> Code Issues 6 Pull requests 0 Projects 0 Wiki Insights

## Home

Remote WiFi HID Keyboard Injector edited this page on Apr 7 · 36 revisions

## What is WHID?

It stands for WiFi HID Injector. It is a WiFi remotely-controlled (Keyboard, Mouse) Emulator. Practically is an USB Rubberducky or BadUSB device on Steroids!

Video Introduction <https://youtu.be/U-TtobZXJcw>

Blog Post <https://medium.com/@LucaBongiorni/whid-injector-how-to-bring-hid-attacks-to-the-next-level-b06a40b7df22>

## Where to Buy?

<http://www.ebay.com/itm/Cactus-WHID-WiFi-HID-InjectorAn-USB-Rubberducky-On-Steroids-for-hackers-pentests-/252927790606>

<https://www.aliexpress.com/item/Cactus-Micro-compatible-board-plus-WIFI-chip-esp8266-for-atmega32u4/32318391529.html>

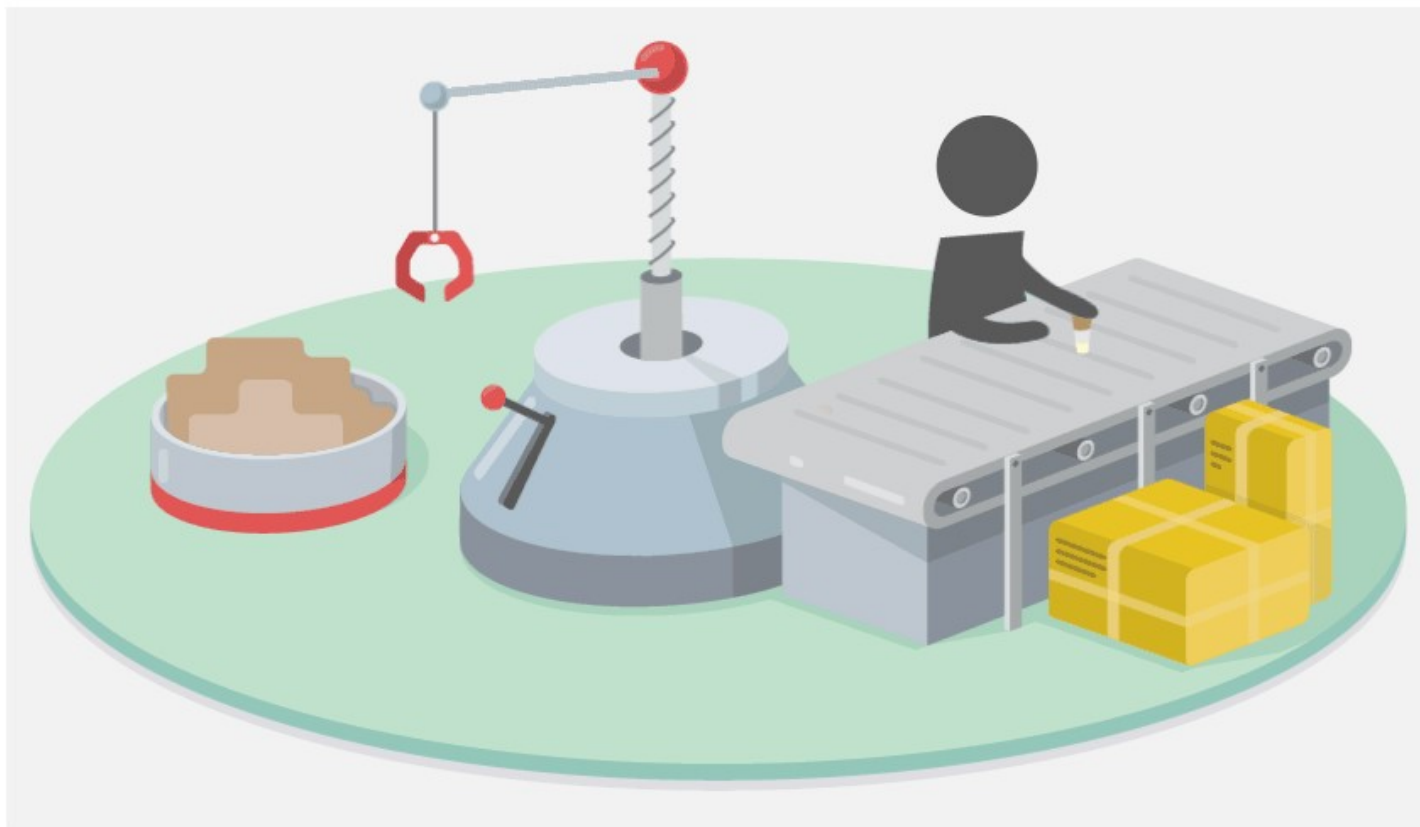
<https://blog.aprbrother.com/product/cactus-whid>

Pages 13

Find a Page...

- Home
- Change VID & PID
- Cool Payloads
- Keyboards Layout
- LINUX Payloads
- OSX Payloads
- USABuse
- Weaponizing USB Gadgets
- WHID Software
- WHID Software SCRIPTING SYNTAX
- WHID Software Uploading Scripts

# Release the Kraken!



# ONE WHID TO PWN THEM ALL



# R&D Phase

- Requirements:
  - Able to Emulate Mouse & Keyboard
  - Able to be Remotely Controlled over MNOs
  - Able to bypass Air-Gapped environments
  - Able to conduct Mousejacking Attacks
  - Able to make Audio Surveillance
  - Able to get GPS Locations
  - Able to act as Standalone device (a.k.a. battery powered)
  - Able to do basic RF stuff (Jamming, Sniff ASK, Replay ASK, etc...)
- Started working on SW



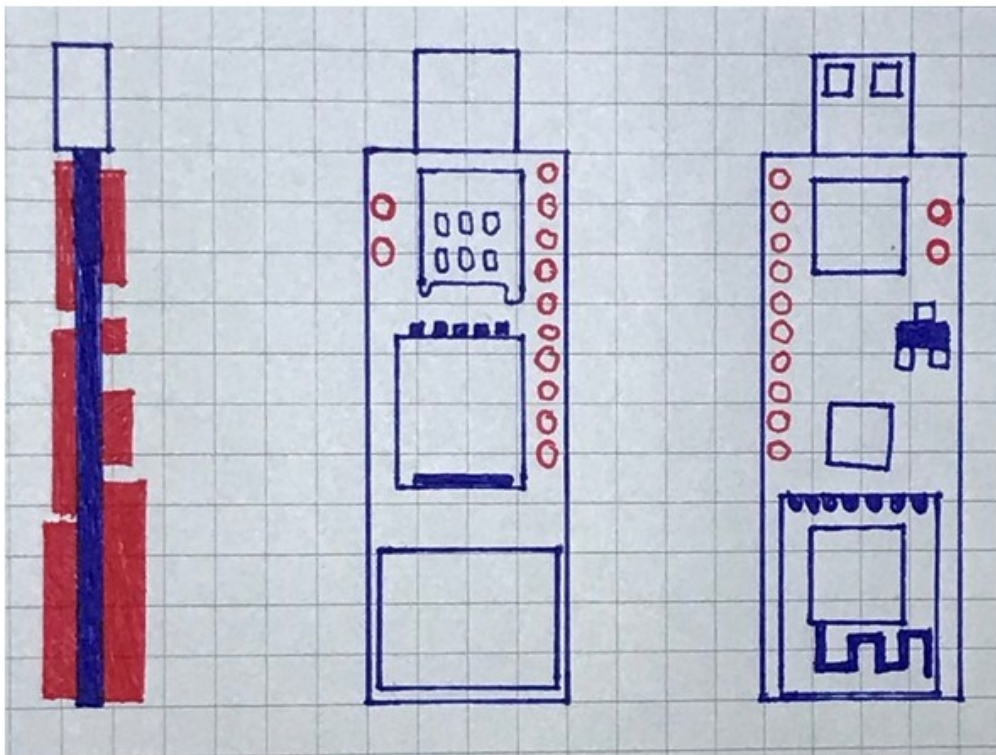
- Initial Requirements
- Logic Consequence
- Cool to Have



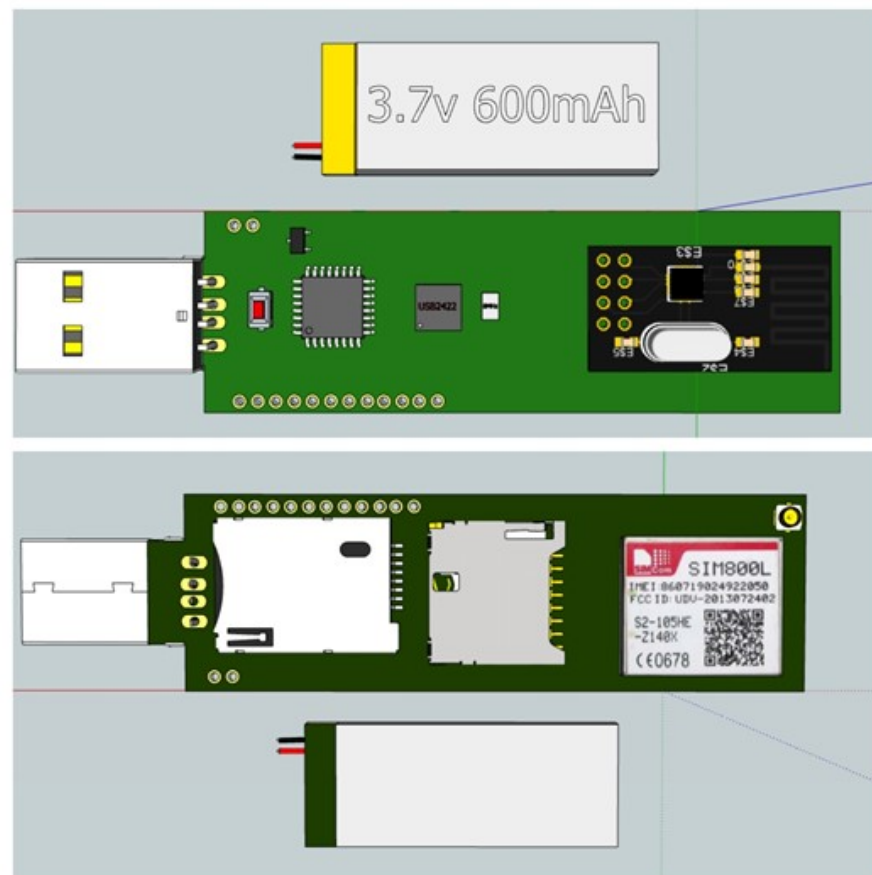
# Commands Available

```
#####  
### airgapwin:<COMMAND-TO-EXFIL>   ### Example:   ###   airgapwin:whoami   #  
### airgapnix:<COMMAND-TO-EXFIL>   ### Example:   ###   airgapnix:whoami   #  
### airgaposx:<COMMAND-TO-EXFIL>   ### Example:   ###   airgaposx:whoami   #  
### win:<COMMAND>                   ### Example:   ###   win:iexplore -k http://fakeupdate.net/wnc/ #  
### nix:<COMMAND>                   ### Example:   ###   nix:gnome-calculator #  
### osx:<COMMAND>                   ### Example:   ###   osx:open -n -a calculator #  
### spy:<PHONE-NUMBER>              ### Example:   ###   spy:0039123123123   #  
### mousejack:                      ### Example:   ###   mousejack:           #  
### mousescan:                     ### Example:   ###   mousescan:          #  
### asktxD11:<BINARY-PATTERN>       ### Example:   ###   asktxD11:101001011110101100000100 (Pin D11) #  
### asktxD7:<BINARY-PATTERN>        ### Example:   ###   asktxD7:101001011110101100000100 (Pin D7)  #  
### jamD11:<TIME-IN-MILLISECONDS>   ### Example:   ###   jamD11:60000 (hardcoded 10s for now) (Pin D11) #  
### jamD7:<TIME-IN-MILLISECONDS>    ### Example:   ###   jamD7:60000 (hardcoded 10s for now) (Pin D7)  #  
### askrx:                          ### Example:   ###   askrx: (Pin D3)         #  
### getlocation:                   ### Example:   ###   getlocation:        #  
#####
```

# WHID Elite: Concept



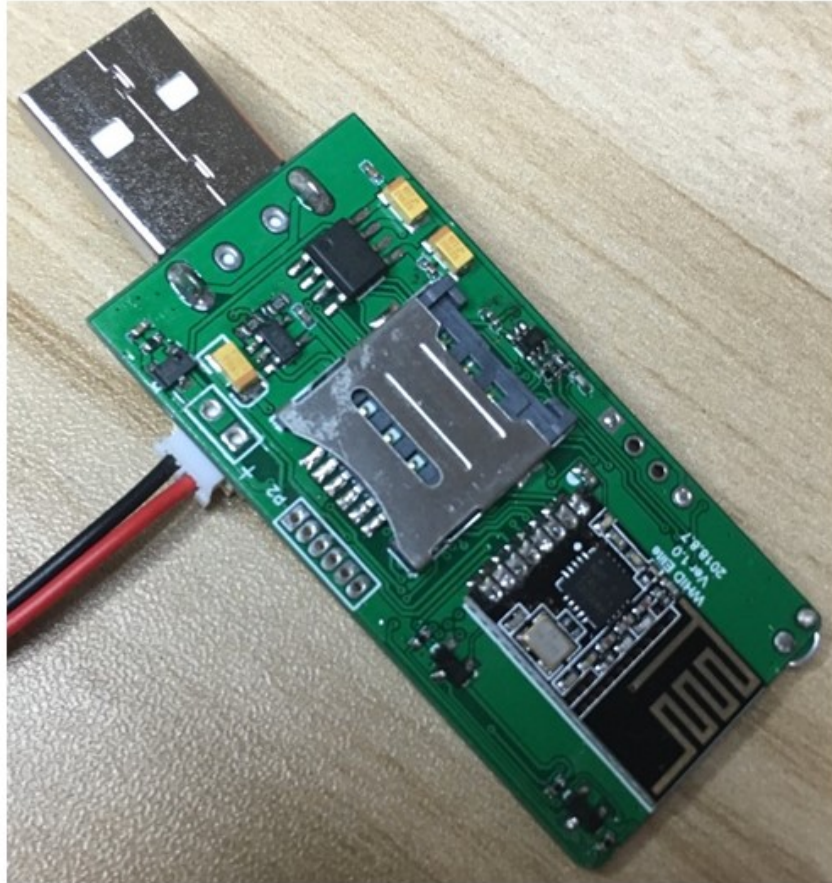
Pen & Paper Sketch



3D Sketch



# WHID Elite: Alfa PCB





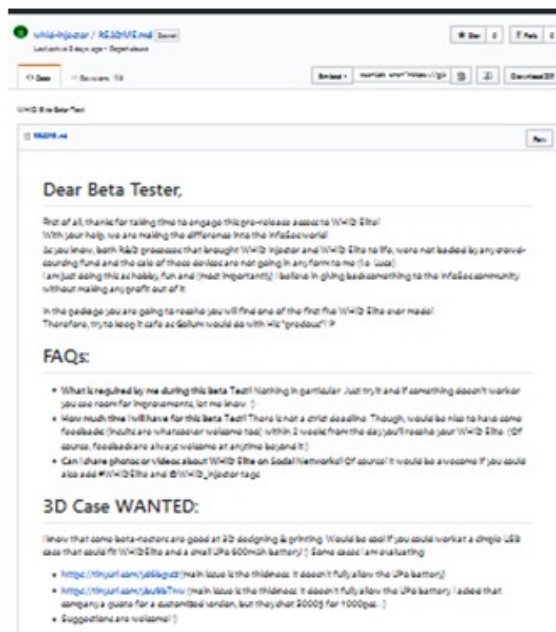
# WHID Elite: Beta PCB





# Time for Beta Test

- Select Wisely Beta Testers
- Do not Set High Expectations anyway (people are busy)
- Prepare easy-to-digest Documentation



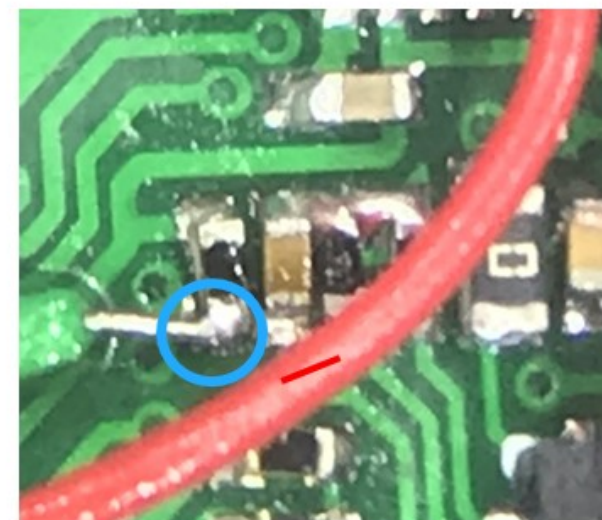
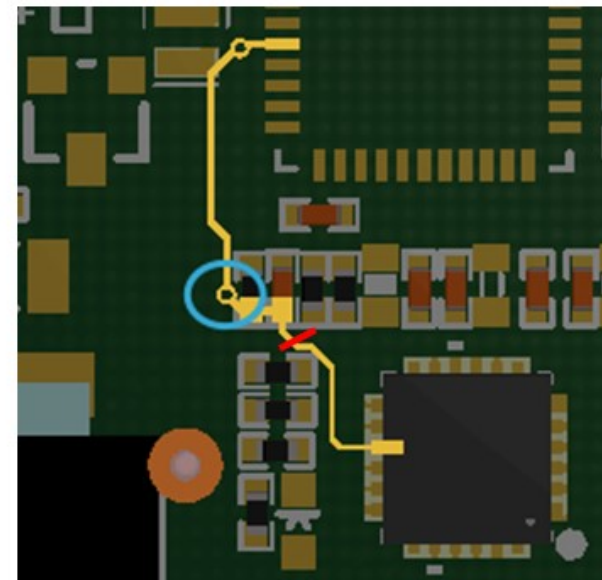
# More Features >> More Bugs

- I needed an INT Pin for RXing ASK-OOK signals
- Used D7 because was close and free!
- Got new PCB
- D7 is the most sucky INT of Atmega32u4...

Micro, Leonardo, other 32u4-based

0, 1, 2, 3, 7

INT6



## INT6 on Arduino Leonardo / ATmega32U4

The documentation for Arduino's [attachInterrupt function](#) lists the pins for the four interrupts available on an Arduino Leonardo. But the Leonardo uses the [ATmega32U4](#), which has a fifth external interrupt (called external interrupt 6, or INT6, just to be confusing). INT6 is not available from the `attachInterrupt()` function, but is available if you access it directly via the registers EICRB (External Interrupt Control Register B) and EIMSK (External Interrupt Mask Register):

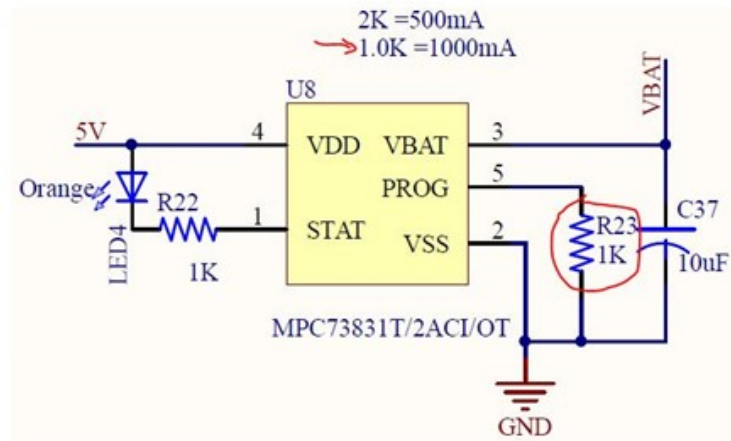
```
EICRB |= (1<<ISC60)|(1<<ISC61); // sets the interrupt type
EIMSK |= (1<<INT6); // activates the interrupt
```

- Re-Engineered the Board to use D3 instead



## Other Bugs Fixed

- Missing a diode which prevents the weaponized USB device to draw current from Lipo.
- D2 was bypassing the LiPO Charging Controller. It made the charging circuit not working properly.
- **Manufacturer forgot my suggestion...** Back in time I asked to change R23 from 1k $\Omega$  to 2k $\Omega$  in the LiPo controller circuit to not draw >500mA... He forgot... Spent hours debugging...



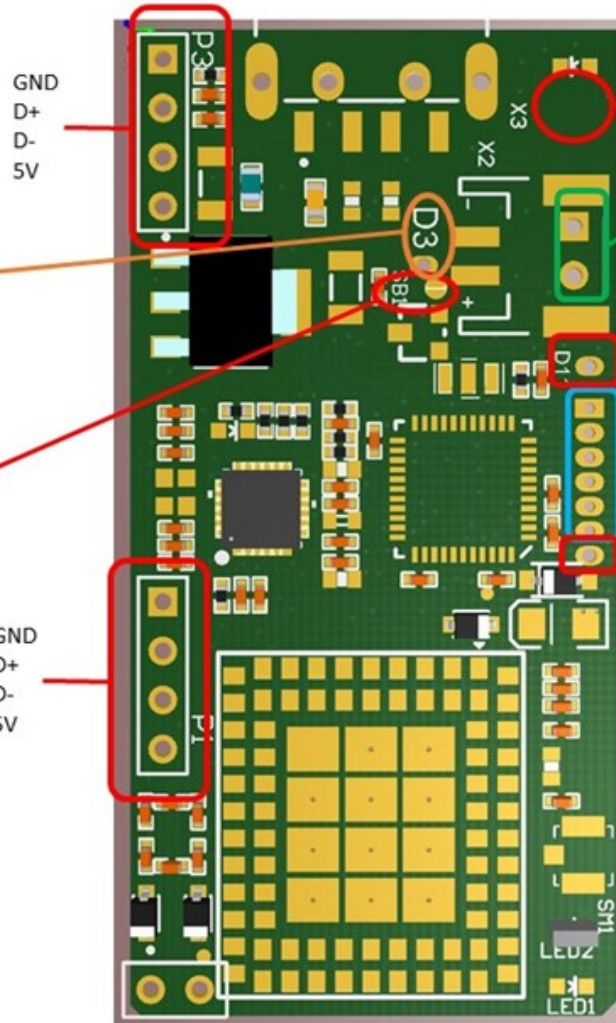
# Final PCB

**P3:** It shares the same Pins of the USB Male Connector. (It is supposed to be connected to target computer)

**D3:** Used, together with external 315/433MHz RX for RF attacks).\*

**SB:** If soldered, will allow 32u4 to run even w/o USB plugged, from LiPo current.

**P1:** Needs be connected to weaponized gadget. (e.g. Mouse, Keyboard, etc.)



**Hall Sensor:** to use with a magnet to soft unbrick the atmega32u4.

LiPo\_GND  
LiPo\_Vcc

**D11:** Used, together with external 315/433MHz TX for RF attacks).\*

RESET  
MISO  
MOSI  
SCK  
GND  
3.3V

**P2:** Used to hardware unbrick the atmega32u4.

**D7:** Used, together with external 315/433MHz TX for RF attacks).\*

**\*Wiring of external 433/315MHz TX/RX:**

GND >> GND

DATA >> D3/D7/D11

Vcc >> 5V



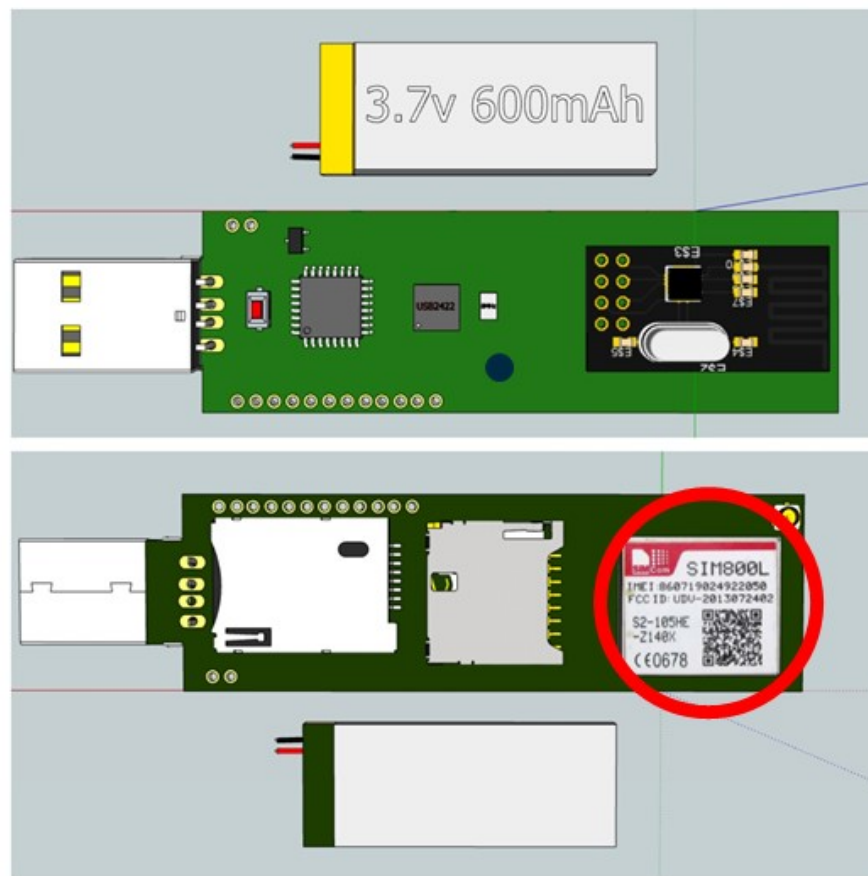
# WHID Elite

- Atmega 32u4
- USB2422 Controller
- **sed 's/ESP/SIMxxxx/'**
- Microphone
- NRF24L01+

V.1.0 – 2G



V.2.0 – NB-IoT

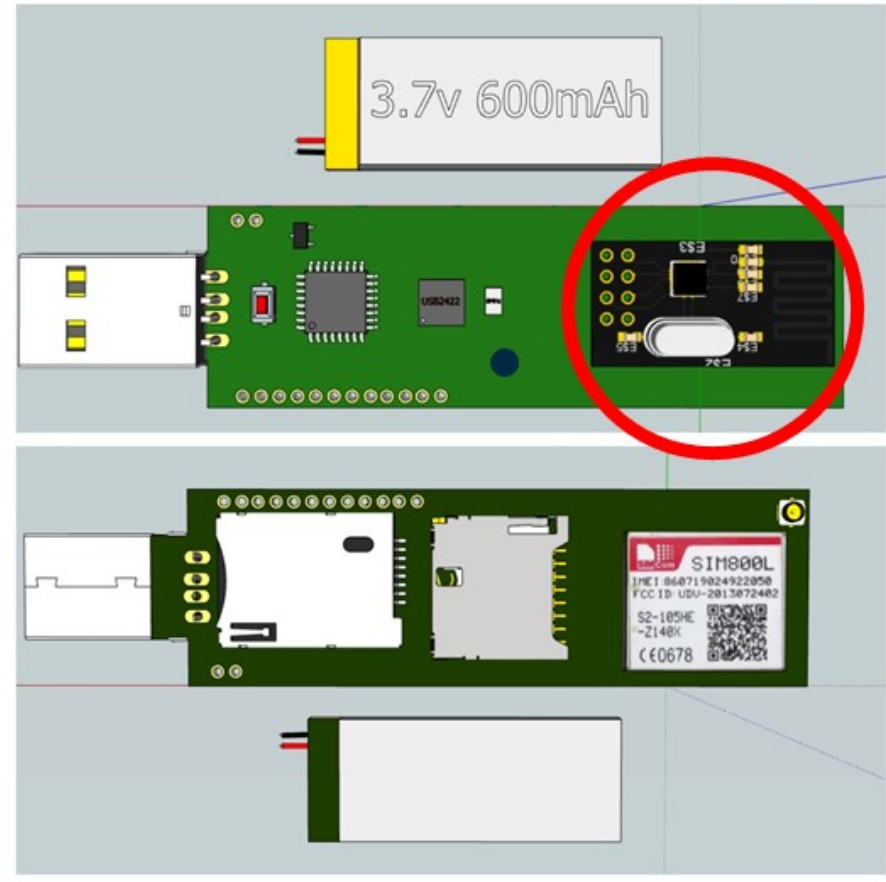


# Bypassing AirGapped Environments with WHID Elite



# WHID Elite

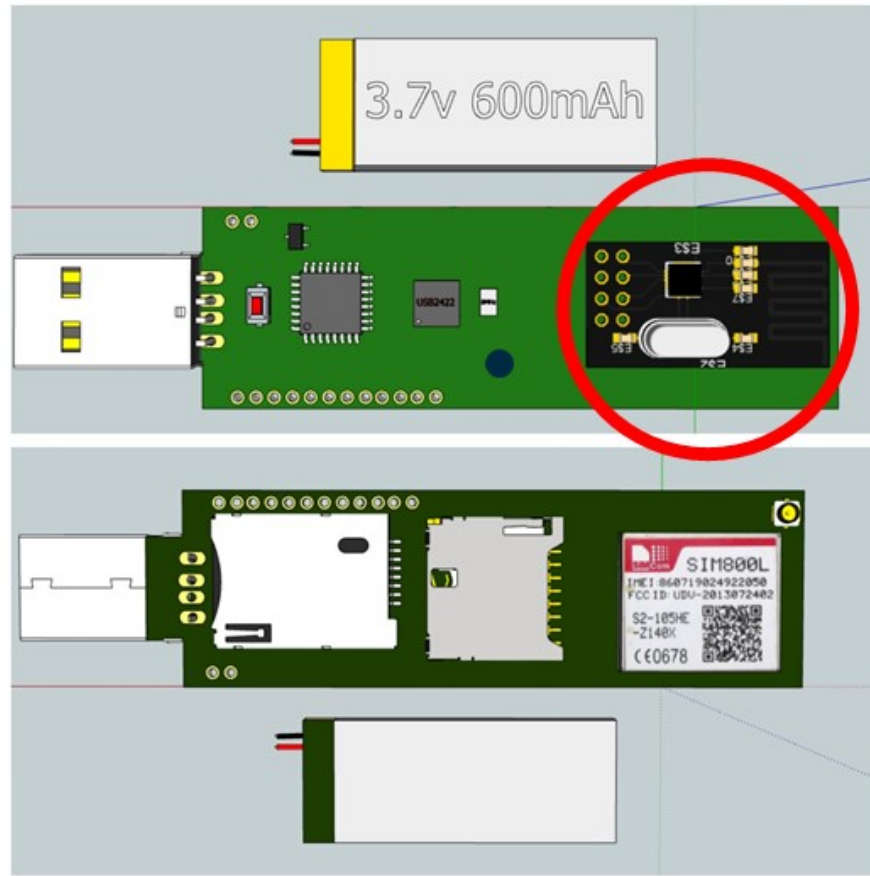
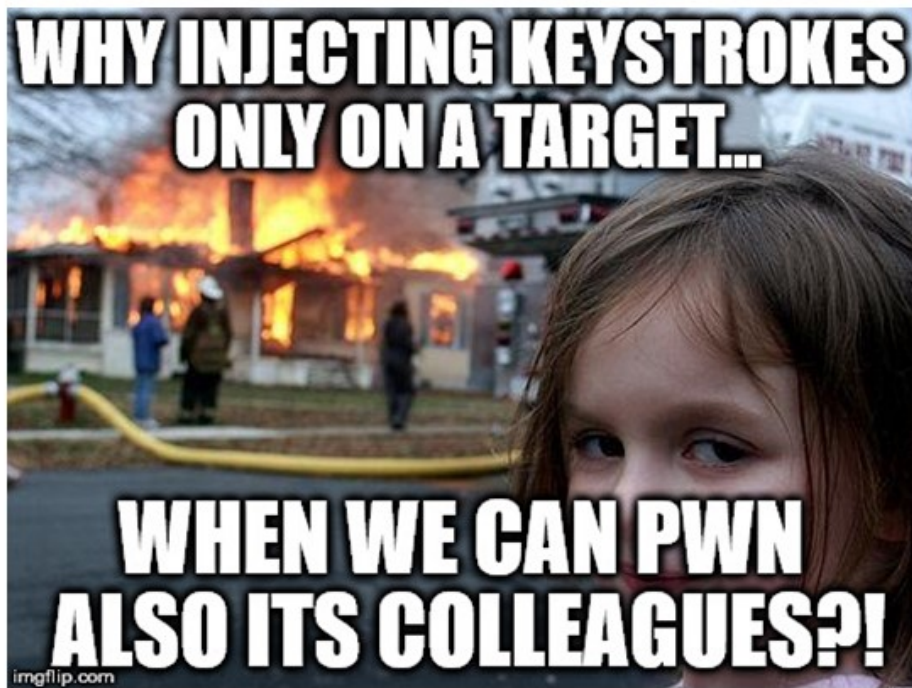
- Atmega 32u4
- USB2422 Controller
- `sed 's/ESP/SIMxxxx/'`
- Microphone
- **NRF24L01+**





# WHID Elite

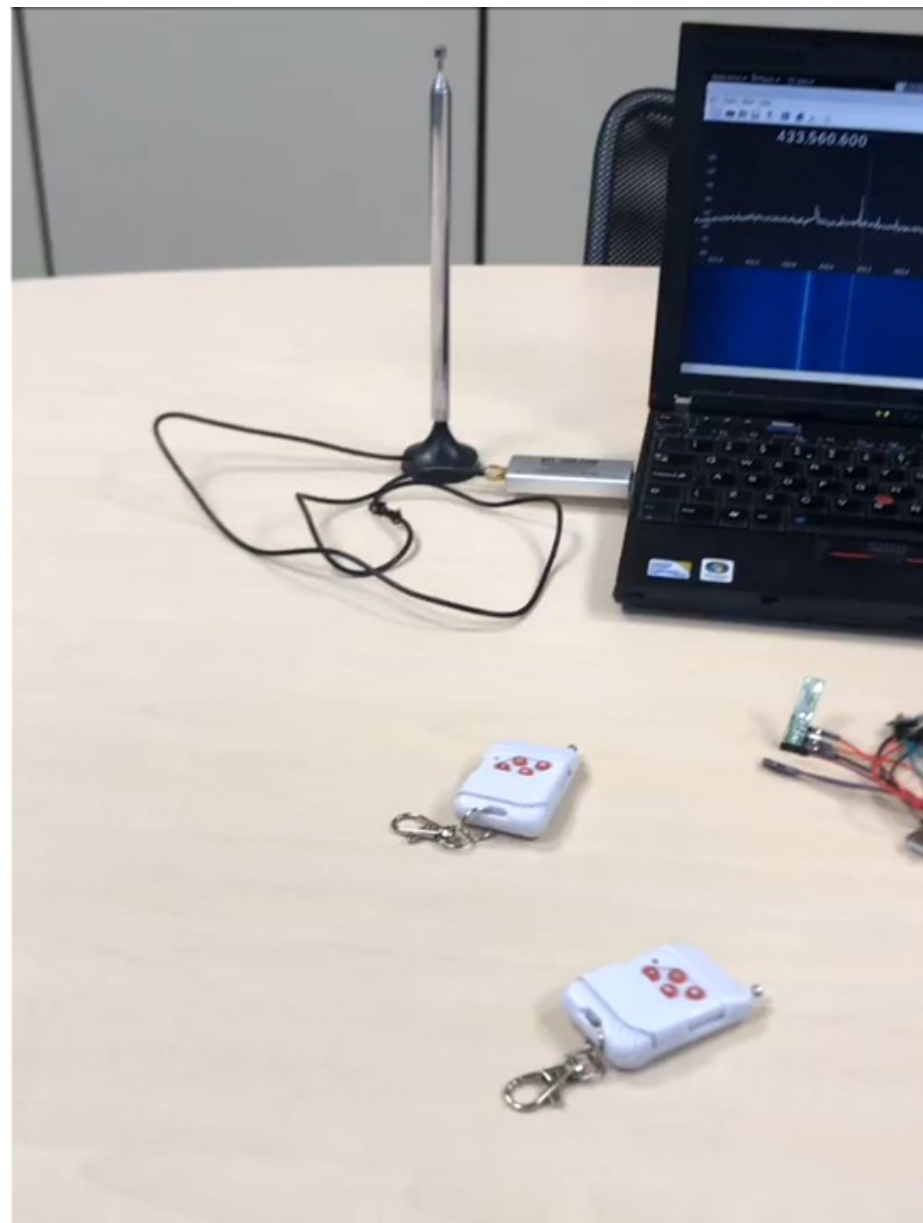
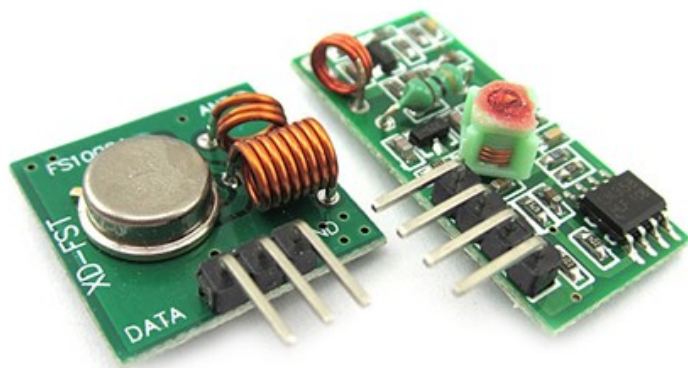
# Mousejacking Wireless Keyboards & Mice





# Remote Radio Hacking

- External Cheap 315/433MHz RTXs to:
  - **Replay Attacks** >> RollJam (WIP)
  - **Fuzzing** (e.g. crashing target)
  - **Bruteforce** (e.g. from Arm to Disarm packet)
  - **Jamming**
  - **What Else?**



# Controlling RC Cranes (maybe)?

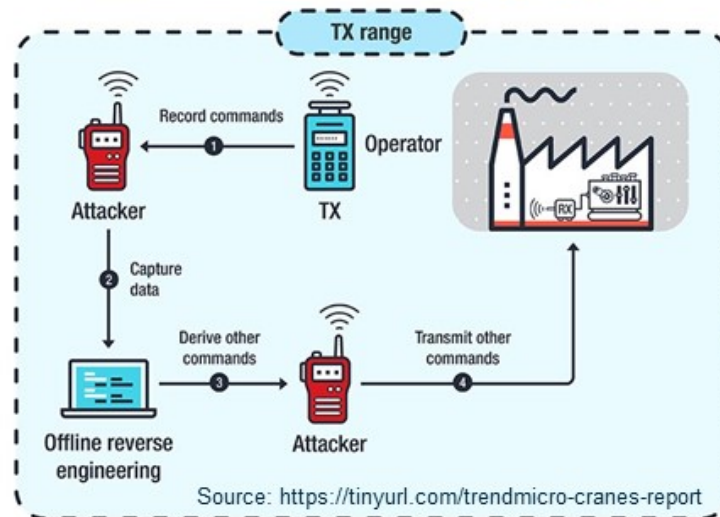
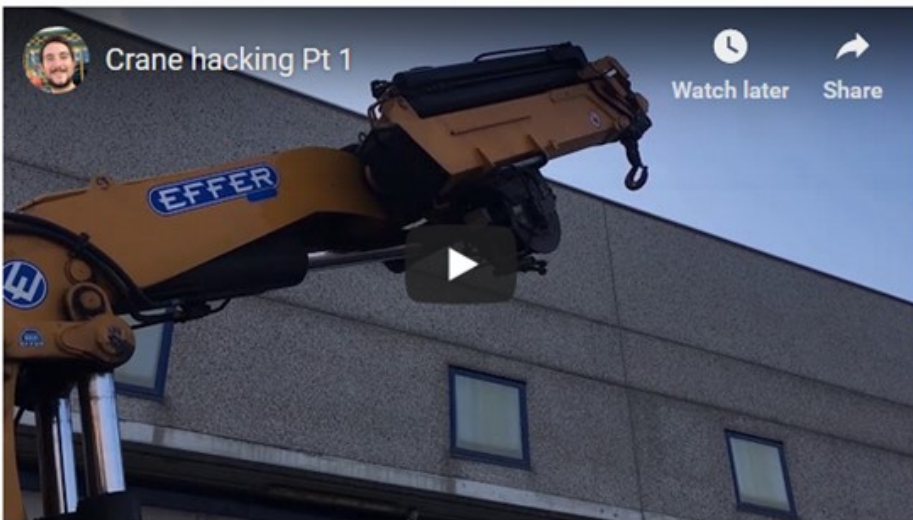
## Exclusive: Hackers Take Control Of Giant Construction Cranes



**Thomas Brewster** Forbes Staff

Cybersecurity

*I cover crime, privacy and security in digital and physical forms.*



# Lessons Learned

- Pick Wisely Beta Testers
- Listen to customers
  - Improvements derived from it:
    - Mobile App (thanks [@PaulWebSeC](#))
    - Firmware Pre-Flashed before delivery
    - Easier Way to Weaponize USB Gadgets
    - WHID Elite
- Prioritize action items
  - Since I do it as no-profit and during free time... is very important to pick what to work on next!
- What else? Beware of some human beings...



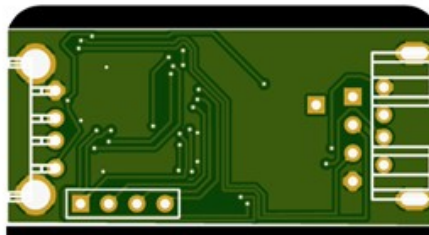




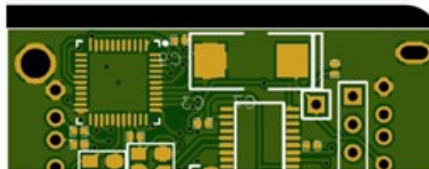
So I got curious...

- No opensource repo
- Sold for 80€ when is worth max 25€
- Wanted a free consultation from me, for his own profit.

Guess what? I BLOCKED him.



What do you think of this pcb design? It is a hardware keylogger using a atmega32u4 and a usb host controller + whatever uart based you like to connect from esp or hc-12 or sim800l (thats why the place for that big capacitor).



Start a message



not bad

11:49 ✓

Let me know if you have any recommendations this was my first ever pcb.

11:50

well, I would need to see  
gerbers and sources. Any  
github repo?

11:51 ✓

Nahh I wouldnt rather share either, but I got no errors so I will see. I also breadboard checked if



Start a message



## Avoid these kind of people

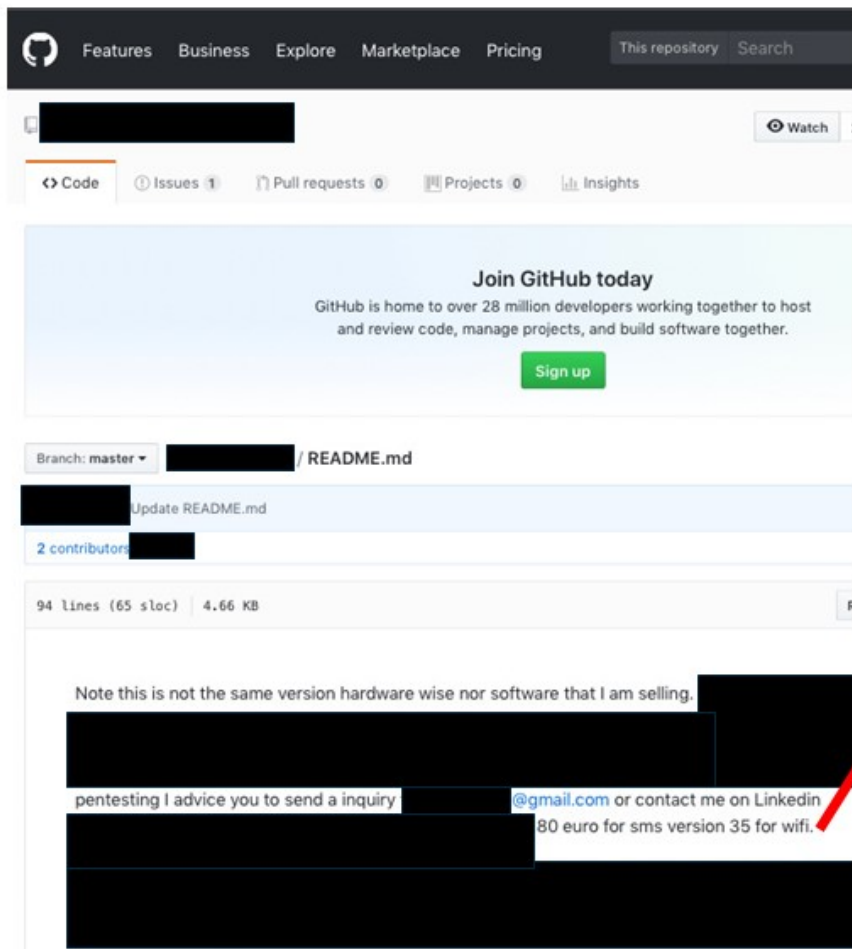


Nahh I wouldnt rather  
share either, but I got no  
errors so I will see. I also  
breadboard checked if  
everything worked fine.

11:53



# So I Got Curious...



- OpenSource the WiFi version
- No trace of the GSM version
- Plus... this note...

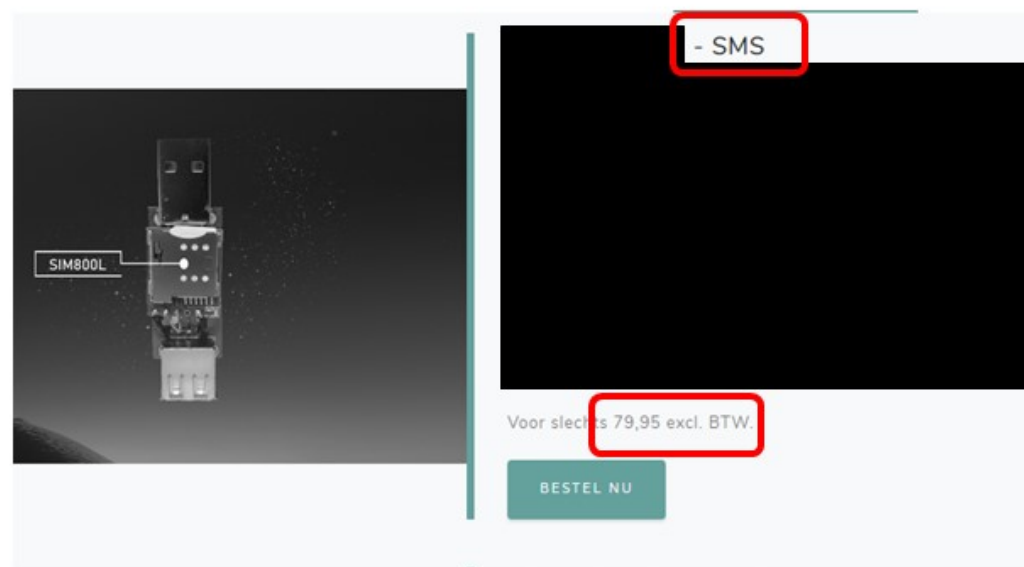
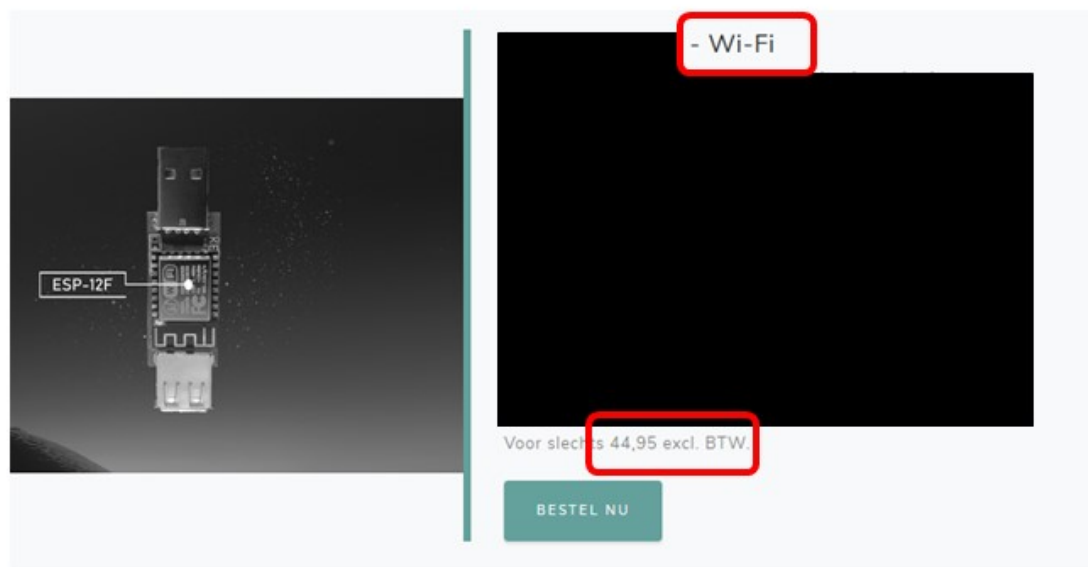
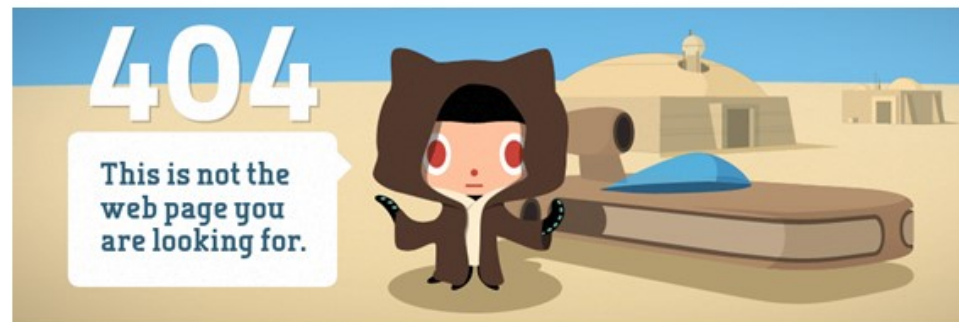
80 euro for sms version 35 for wifi.





## After my Tweet...

He removed also the WiFi version from his GitHub and went fully closed-source & commercial!



# What's Next?



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

# 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!**

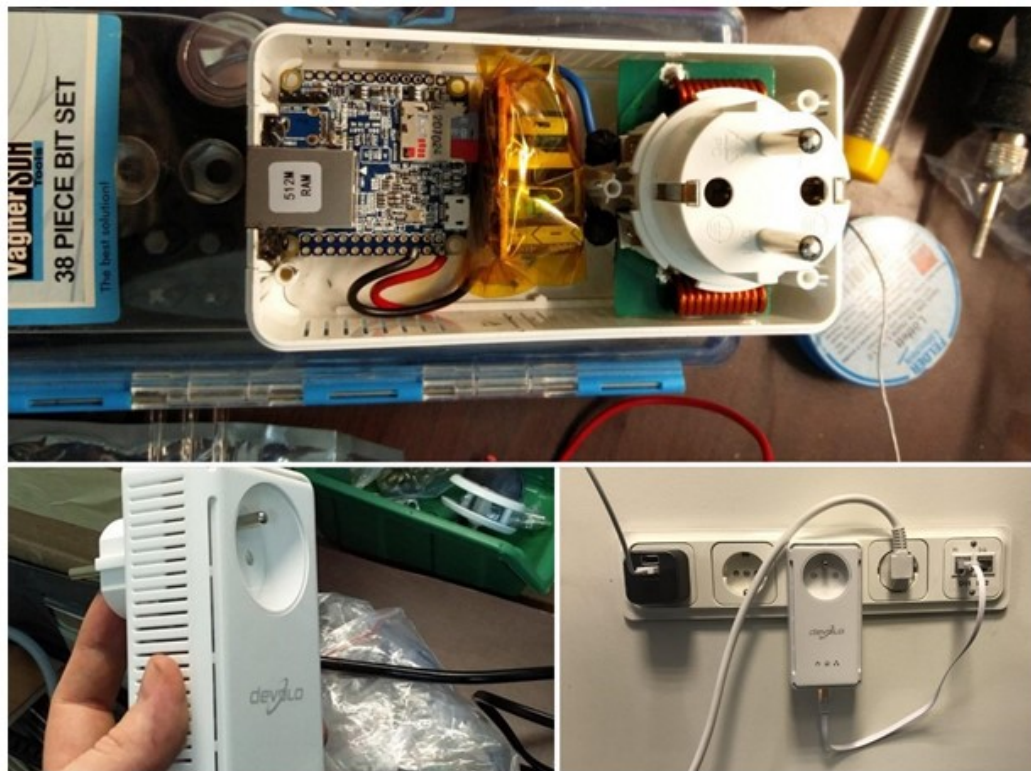


# Pentest Dropboxes Everywhere

**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 €**







Luca Bongiorni

@LucaBongiorni

Replying to @vysecurity

NanoPi NEO hidden in a Powerline adaptor  
FTW 😎



2:20 PM - 4 Jun 2017

12 Retweets 30 Likes



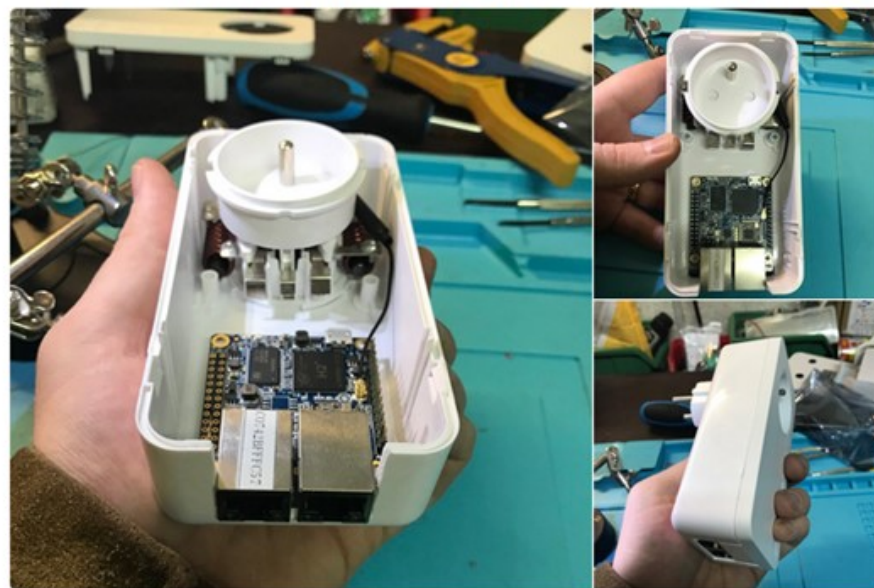
2 12 30



Luca Bongiorni

@LucaBongiorni

OrangePi R1 fits magnificently!  
Perfect as Pentest Dropbox with 802.1x NAC  
bypass capabilities ❤️  
P.S. POTAEbox will be way cooler though! 😎



9:42 PM - 2 Oct 2017

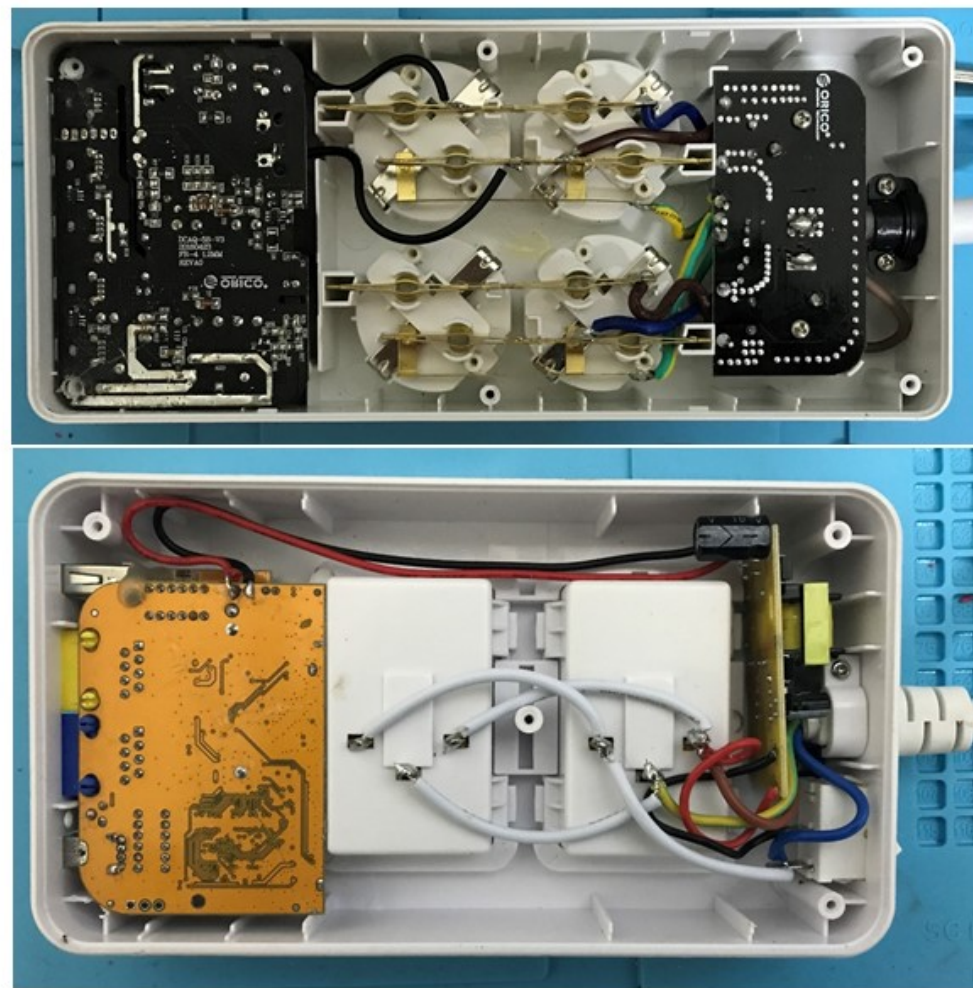
18 Retweets 40 Likes



3 18 40



# R&D: SBCs and Covert Cases Evaluation



# Chinese SBCs – The State of Art

- **Many Chinese xxxxxPis on the market... and no one with a dominant position!**
  - OrangePi, BananaPi, NanoPi, PotatoPi, TrumpPi,...
- **PROs:**
  - Cheap
  - New HW versions every 2Qs
- **CONS:**
  - Very limited technical support or resources
    - One or Two Linux images public and that's it. (Zero LTS [LongTerm Support])
  - New HW versions every 2Qs >> very short life cycle for older models



# My Vision

- A **well designed & well maintained** (from SW point of view) **SBC** that has acceptable features that can last couple of years from technical specs point of view and be still competitive.
- **Dedicated LTS OS Security Oriented** (e.g. CallHome over 2/3G, IceBreaker, DeathStar, 802.1x Bypass Module, Bettercap, MANA, etc.)

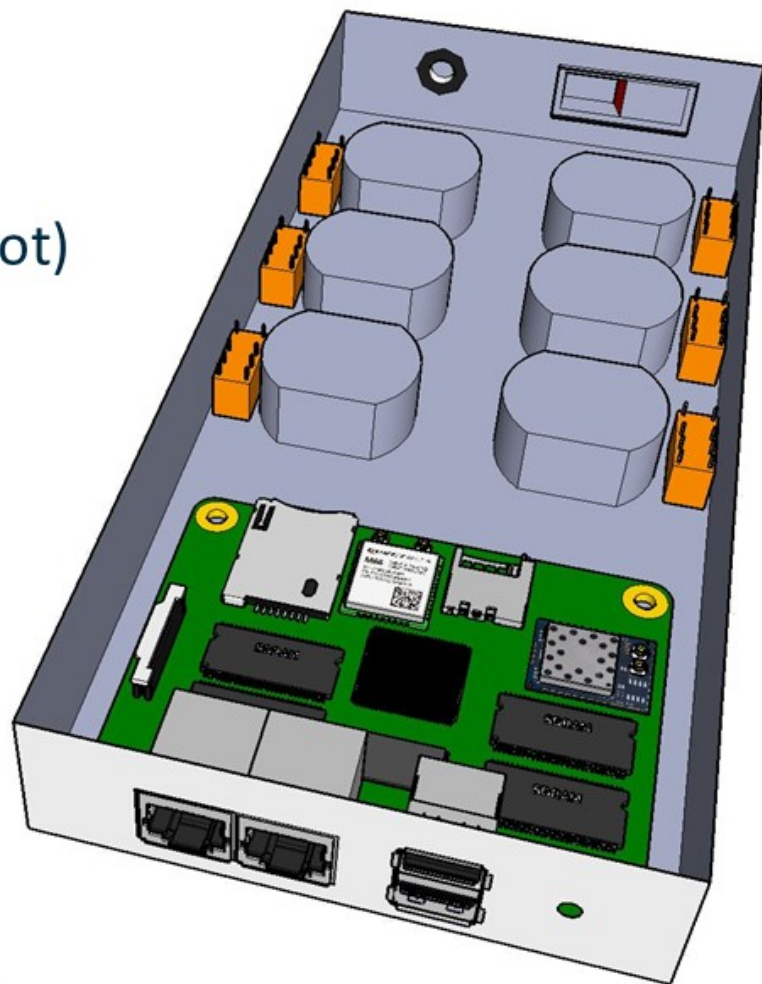
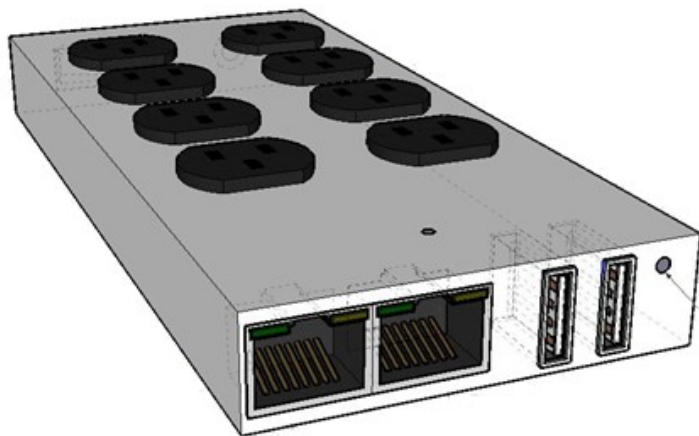
## Example:

- I prefer having a SBC with 2GB RAM, but well maintained LTS OS... and use it for the next 2 years....
- Rather than use it 6 months and then buy another SBC with 4GB RAM with no LTS OS.

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

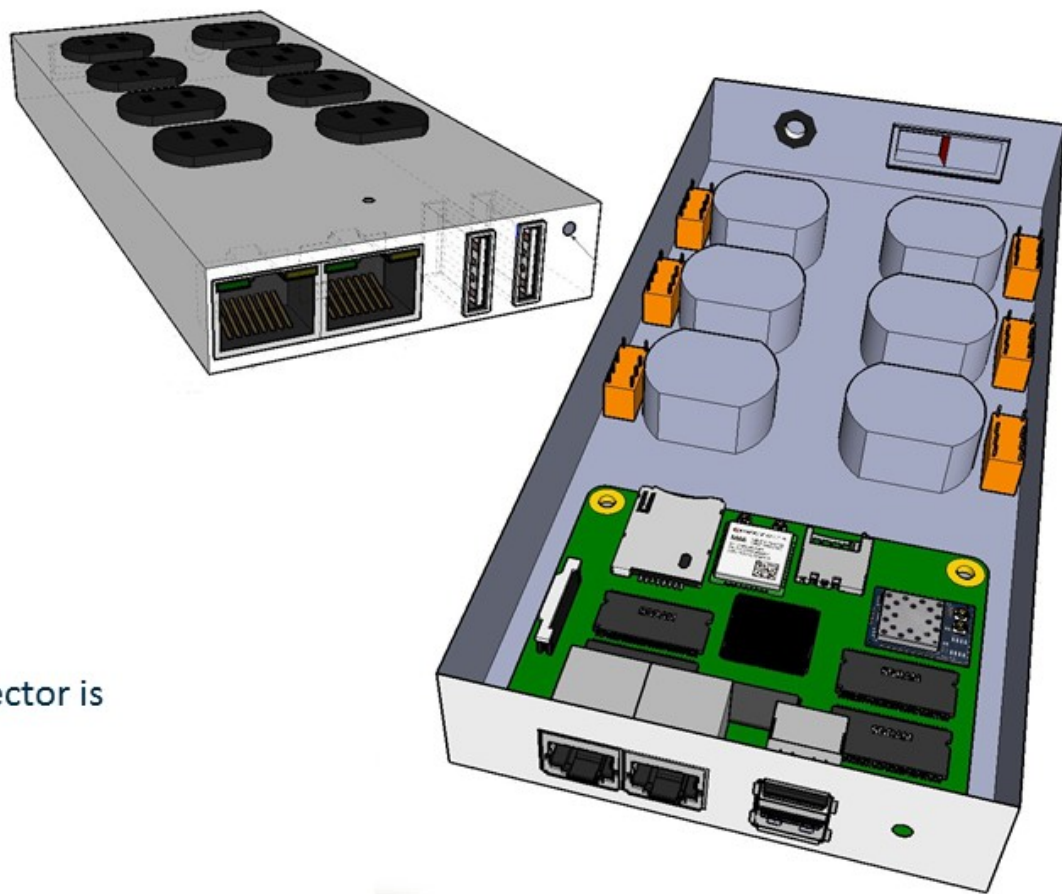
## POTÆbox Purposes:

- 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



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

- **Allwinner Quad-core CPU ARM** (H5 or H6)\*\*
- **2gb RAM**
- **8gb NAND**
- **2x Gigabit Ethernet Ports** (e.g. RTL8363SB)
- **2x USB 2.0 Ports**
- **1x USB 2.0 OTG Port**
- **1x USB 3.0 Port** (if H6 is used)
- **1x mini-pcie** (if H6 is used)
- **Embedded Microphone**
- **CSI Camera connector**
- **2G/3G Module (w/ SIM card slot)**
- **uSD card slot**
- **Atheros Wifi Chipset 2.4/5 GHz** ( 2x space permitting)
  - AR9580 mini-pcie (if H6 is used and a minipcie connector is available on PCB)
  - AR9344 (connected through USB 2.0)
- **Relays** (controlled by PCB's GPIOs)
- **[OPTIONAL] Wireless Attacks** (NRF2401L, CC1101, etc.)

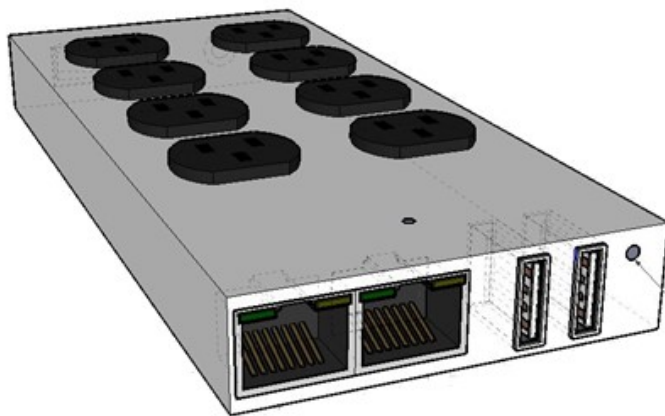


\*\*Need to check if CDC USB Gadgets are supported well



# Covert Cases

- Power Socket
- Charging Station
- Bluetooth Speaker
- Smoke Alarm
  - Battery powered & connected to RJ45 (offensive eth & wireless attacks)
  - Male power socket (wireless only attacks)

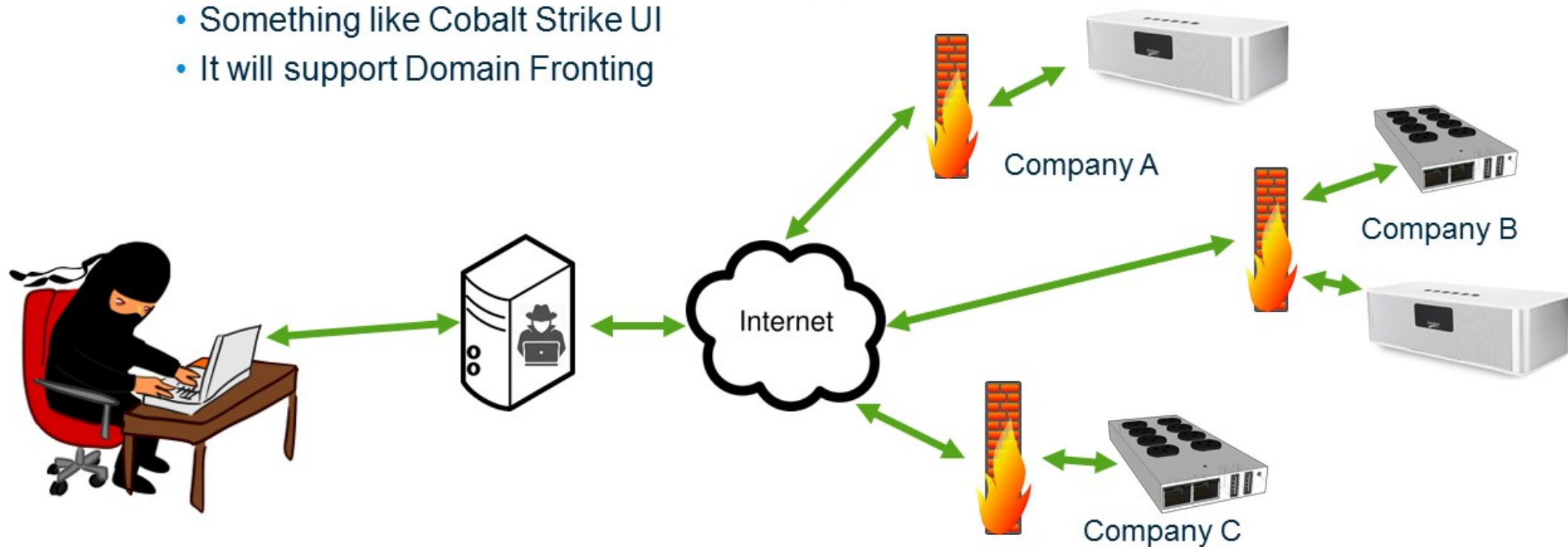


## Software Orchestrator (within POTAExbox device)

- Easy-to-Use GUI (e.g. FruityWifi)
- Multiple channels/tunnels to call home the aggregator (e.g. DNS, ICMP, SSH, HTTPS, Gmail, Twitter, etc.)
- NAC/802.1x bypass techniques
- MANA + Bettercap + New EAP Relay Attack
- Ice Breaker + Deathstar
- Remote Wireless Attacks with NRF2410L & CC1101 (e.g. Mousejacking, YardstickONE style attacks: Disabling Alarm Systems, Fuzzing ASK/FSK/MSK RF controllers, etc.)

# SaaS DropBoxes Aggregator

- Dockerized VPS (+Domain Fronting) that acts as the Attacker's C2
  - It aggregates all the POTAEboxes deployed in one single GUI
    - Something like Cobalt Strike UI
    - It will support Domain Fronting



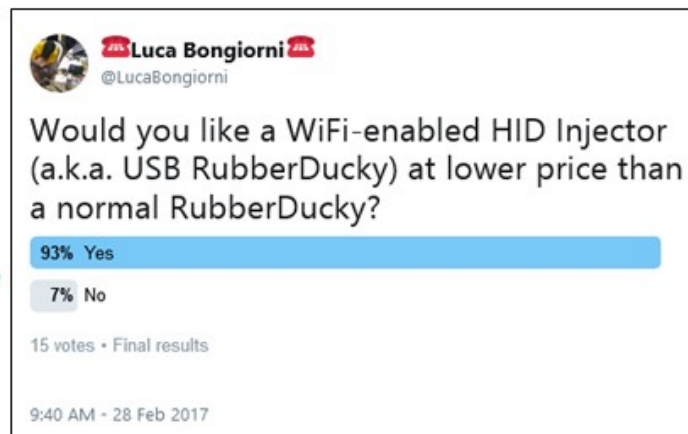


# Personal (Un)Business Model [Real Deal Example]

- No Profit Based.
  - At most, repay for expenses due to SBCs/Cases Evaluation phase.
- Being Recognized as principal author of the idea.
- Maintain POTAEbox Name and Logo.
- Be Affordable. (i.e. <150~300 USD)
- Besides the above requirements:
  - **Make all the profit you want!**
  - Crowdfunded Campaign is more than welcome! I always loved the idea, but no time, nor interest in it.

# To Recap

- **Have an Idea for a new device?**
- **Wanna release it in OpenSource and w/o Profit?**
  - Prepare a Prototype or a Concept
  - Hunt for Manufacturers
  - **First Impression is Everything!**
    - Well planned email
    - Supported by Visual material (i.e. ConceptArts, PoCs, Videos, etc)
    - Supported by Market Analysis (even a simple one can be a game-changer)
    - Straight to the Proposal
      - A.k.a. Business (Un)deal
  - **Beta Test**
    - Select Wisely Beta Testers
    - Do Not Set High Expectations anyway (people are busy)
    - Prepare easy-to-digest Documentation (How To 101)
  - **Stay Away from People that Wanna Profit out of your Inventions!**



Fin