

XII STIC CCN-CERT CONFERENCES

Cybersecurity,
towards effective response and deterrence



Next-Gen HID Offensive Devices

How to bypass an ICS Air-Gapped
Environment



 @lucabongiorni

- Principal Offensive Security Engineer at



- After this presentation, you will:
 - Understand that FlashDrives are not the only threat within the ICS realm.
 - Be (even) more suspicious of USB devices and gadgets.
 - Learn about new tools for conducting Red Team engagements & scare CISOs.

**USB devices are still the #1
source of malware in
Industrial Control Systems!**

Tick Group Weaponized Secure USB Drives to Target Air-Gapped Critical Systems



By Kaoru Havashi and Mike H.

June 22, 2018 at 1:00 PM

Category: Unit 42



ICS Alert: USB Malware Attack

Wednesday December 20, 2017 @ 02:12

By Gregory Hale

Security provider Nyotron found an advanced malware attack targeting Middle Eastern critical infrastructure clients.

"On December 11, 2017 at 01:21 a.m., a night-shift employee working at an around-the-clock critical infrastructure facility located in the Middle East plugged a USB drive into a shared workstation that dozens of the company's employees use on a daily basis," said researchers at Nyotron. "The employee was watching the movie *La La Land* that he had recently downloaded to his USB during his break. After about 30 minutes, (the operator) was interrupted by a call and had to cut his break short. He didn't know that his actions had initiated a sequence of events that could have been disastrous for his organization. Along with the movie, he had launched a well-crafted attack now known as Operation Copperfield."

DHS: USB Drives Spread Malware in Control System Environment at Two Power Plants

01/17/2013 POWERnews



TECHNOLOGY NEWS

APRIL 27, 2016 12:05 AM / 2 YEARS AGO

German nuclear plant infected with computer viruses, operator says

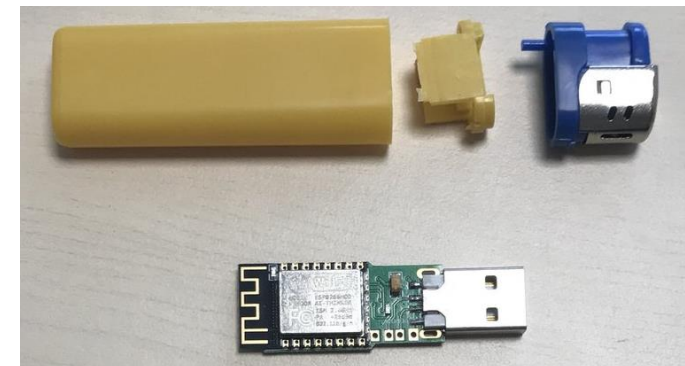


Common Misconception

USB devices are **NOT ONLY** Flash Drives!



≠



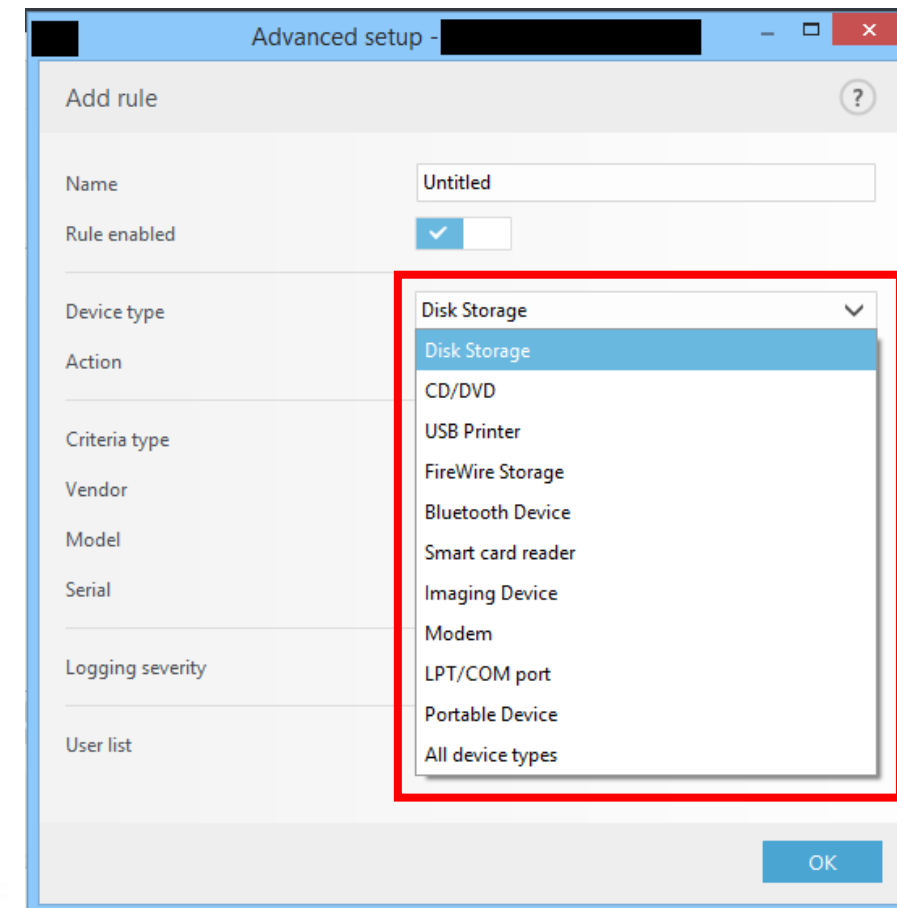
Human Interface Devices

“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

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

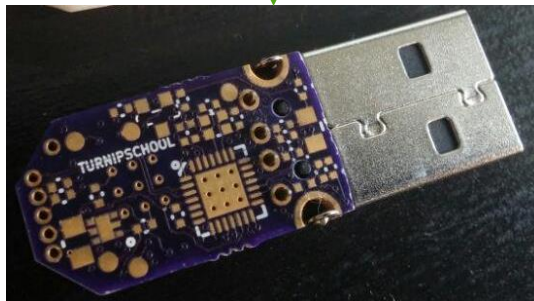
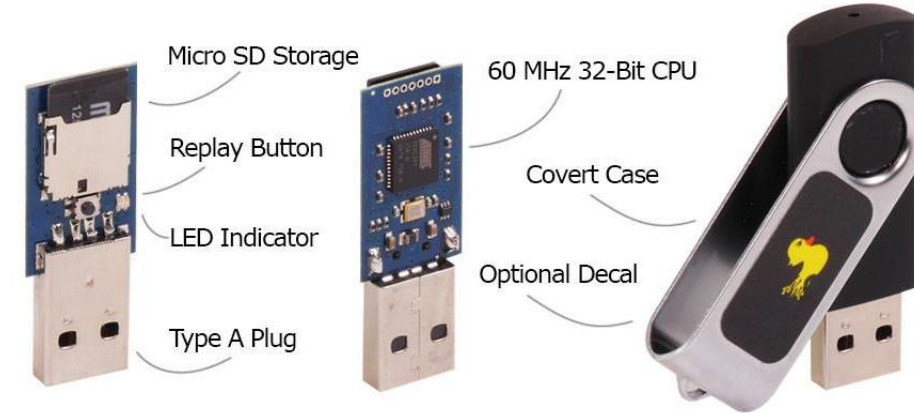
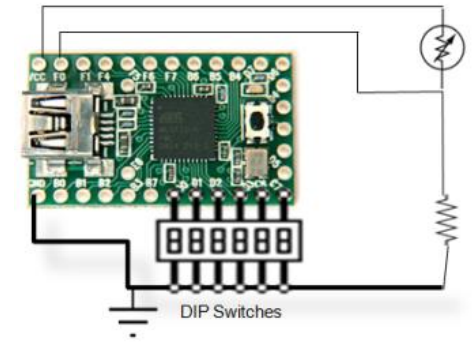


WHAT COULD POSSIBLY GO WRONG



Offensive Devices – 1st & 2nd Generations

- **Teensy – (PHUKD 2009 & Kautilya 2011)**
- **Rubberducky (2010)**
- **BadUSB (2014)**
- **TURNIPSCHOOL (2015)**

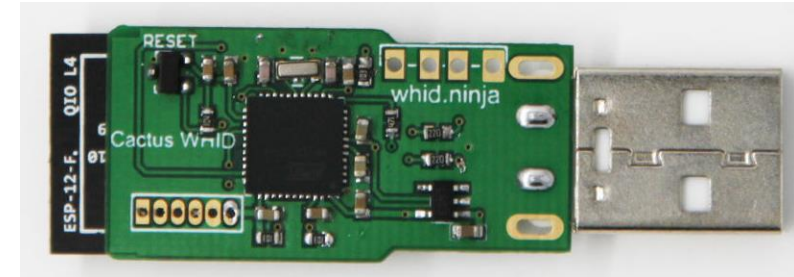


Offensive Devices – 3rd Generation



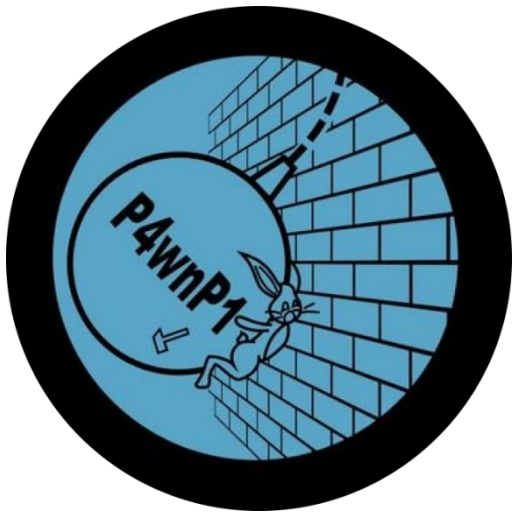
- **WHID Injector (2017) – A Rubberducky on Steroids**

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

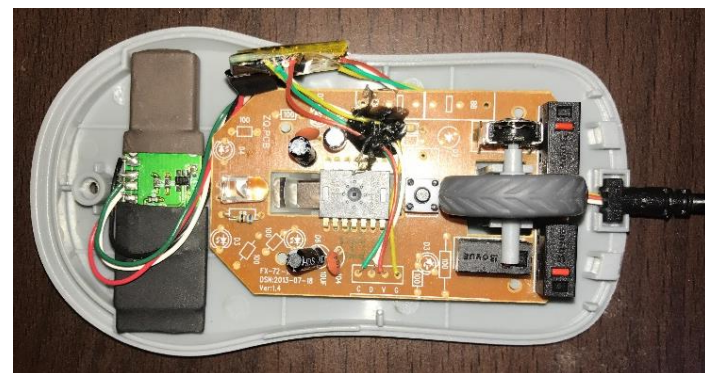


- **P4wnP1 (2017)** (by [Marcus Mengs](#)) – **A Bash Bunny on Steroids**

- 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
- NexMon WiFi Drivers ► Karma Attacks FTW
- Next Gen AirGap bypass ► <https://youtu.be/fbUBQeD0JtA>



Weaponizing USB Gadgets



Weaponizing USB Gadgets

- Test for Social Engineering weaknesses
- Bypass physical access restrictions to a target's device
- OR... You are Kim Jong-Un and wanna have fun pwning international delegates.

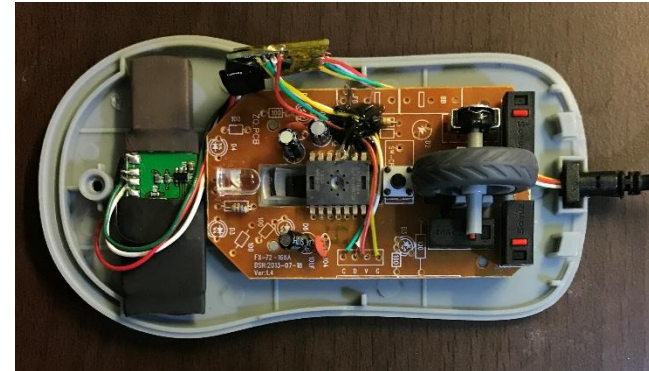
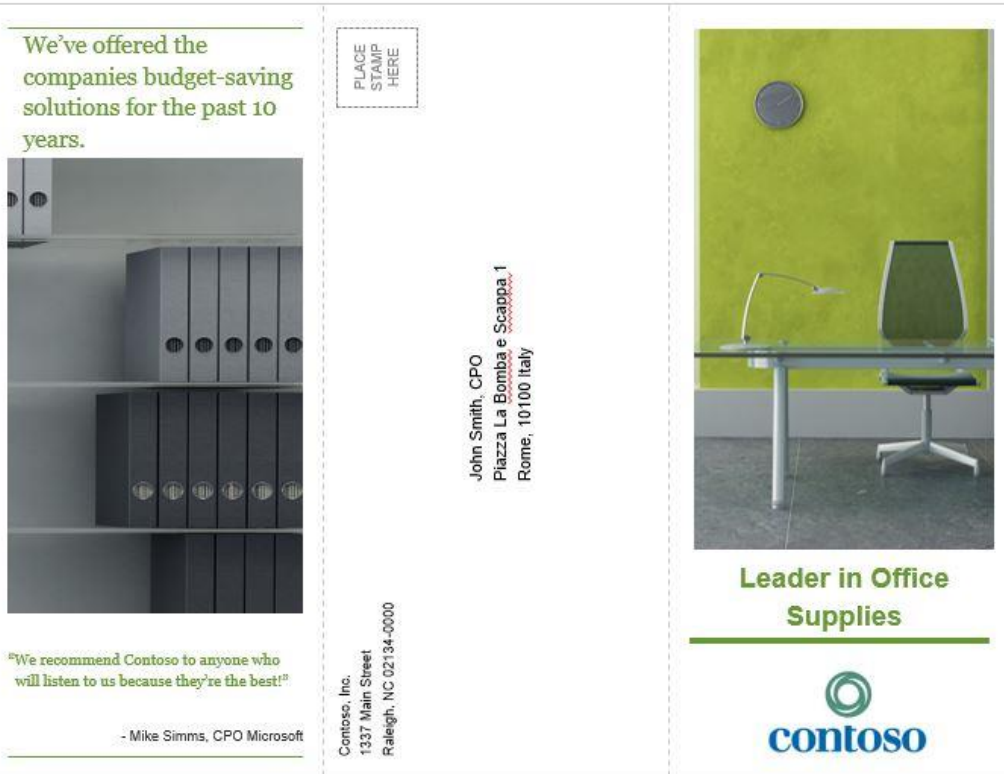


Inside press kit at #TrumpKimSummit:  not wasting the opportunity to promote e'thing fr its manufacturing sector to zoo & @SingaporeUSS. And oh, there's a mini USB fan for those not used to tropical weather  プレスキットの中身!! さすが 、広告いっぱい& ミニ扇風機 

 Translate Tweet

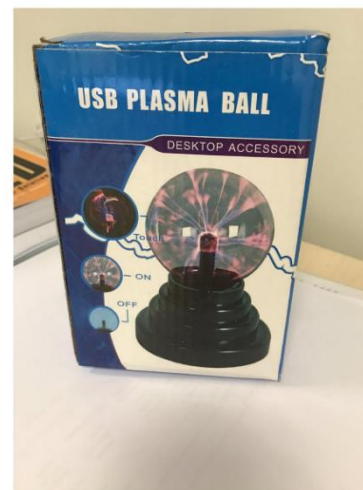
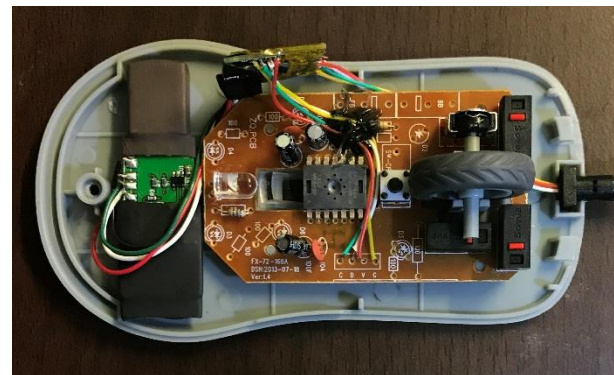


5:38 AM - 10 Jun 2018



Weaponizing USB Gadgets

- Test for Social Engineering weaknesses
- Bypass physical access restrictions to a target's device!
- **OR... You are Kim Jong-Un and wanna have fun pwning international delegates.**



Software Frameworks – ESPloitV2 GUI

- Evolution of WHID GUI
- Shipped w/ WHID Injector
- Hidden SSID (if needed)
- **ESPortal Creds Harvester + Karma**
- **Multi OS & Multi KB Language**
- AutoStart Function
- Change settings on-the-fly
- Live Payloads
- Duckyscript to WHID Converter
- OTA Update of ESP firmware
- **Changeable VID/PID**
- Reset ESP from Serial
- **AirGap Bypass through Serial**

ESPloit v2.7.41 - WiFi controlled HID Keyboard Emulator



by Corey Harding

www.LegacySecurityGroup.com / www.Exploit.Agency

File System Info Calculated in Bytes

Total: 2949250 **Free:** 2935947 **Used:** 13303

[Live Payload Mode](#) - [Input Mode](#) - [Duckuino Mode](#)

-
[Choose Payload](#) - [Upload Payload](#)

-
[List Exfiltrated Data](#) - [Format File System](#)

-
[Configure ESPloit](#)

-
[Upgrade ESPloit Firmware](#)

-
[Help](#)

Spoofing VID & PID

- Edit `boards.txt` in Arduino configuration directory
- Linux:
`/root/.arduino15/packages/arduino/hardware/avr/1.6.19/`
- Windows:
`C:\Users\USER\AppData\Local\Arduino15\packages\arduino\hardware\avr\1.6.19\`

#####

```
CactusWHID.name=Cactus WHID
CactusWHID.vid.0=0x1B4F
CactusWHID.pid.0=0x9207
CactusWHID.vid.1=0x1B4F
CactusWHID.pid.1=0x9208
```

```
CactusWHID.upload.tool=avrdude
CactusWHID.upload.protocol=avr109
CactusWHID.upload.maximum_size=28672
CactusWHID.upload.maximum_data_size=2560
CactusWHID.upload.speed=57600
CactusWHID.upload.disable_flushing=true
CactusWHID.upload.use_1200bps_touch=true
CactusWHID.upload.wait_for_upload_port=true
```

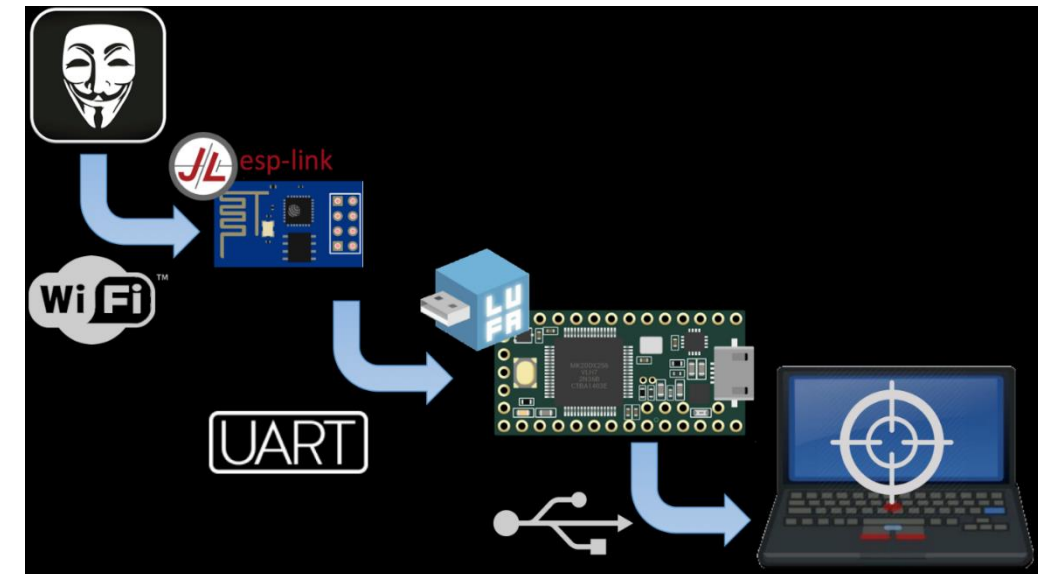
```
CactusWHID.bootloader.tool=avrdude
CactusWHID.bootloader.low_fuses=0xff
CactusWHID.bootloader.high_fuses=0xd8
CactusWHID.bootloader.extended_fuses=0xcce
CactusWHID.bootloader.file=caterina-LilyPadUSB/Caterina-LilyPadUSB.hex
CactusWHID.bootloader.unlock_bits=0x3F
CactusWHID.bootloader.lock_bits=0x2F
```

```
CactusWHID.build.mcu=atmega32u4
CactusWHID.build.f_cpu=8000000L
```

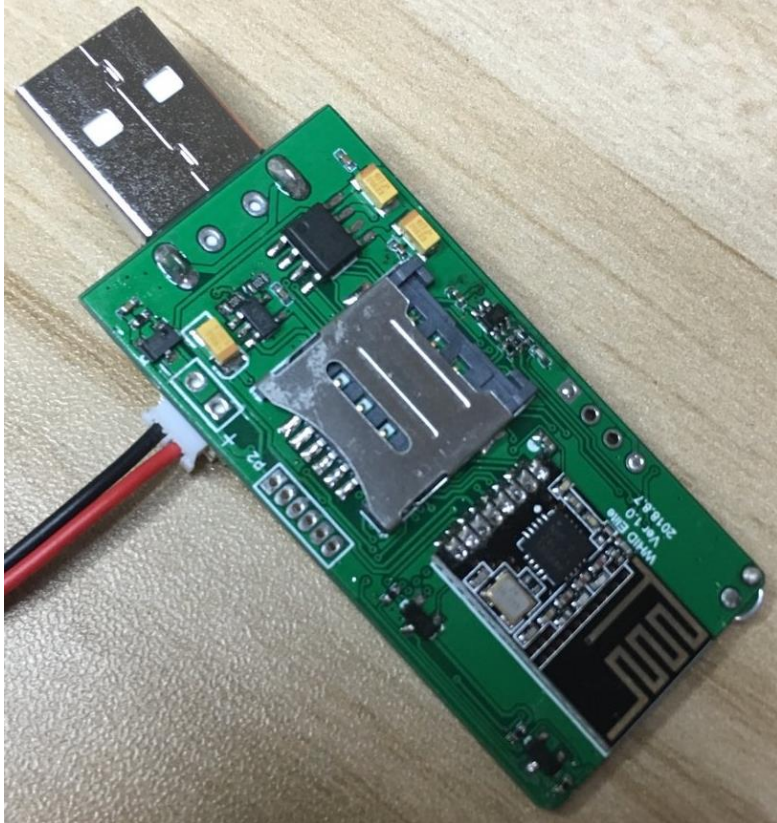
```
CactusWHID.build.vid=0x0000
CactusWHID.build.pid=0xFFFF
CactusWHID.build.usb_product="Cactus WHID"
CactusWHID.build.usb_manufacturer="April Brother"
CactusWHID.build.board=AVR_LILYPAD_USB
CactusWHID.build.core=arduino
CactusWHID.build.variant=leonardo
CactusWHID.build.extra_flags={build.usb_flags}
```

Software Frameworks – USaBuse

- Developed by [@RoganDawes](#)
- 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
- Video Demo
<https://youtu.be/5gMvtUq30fA>



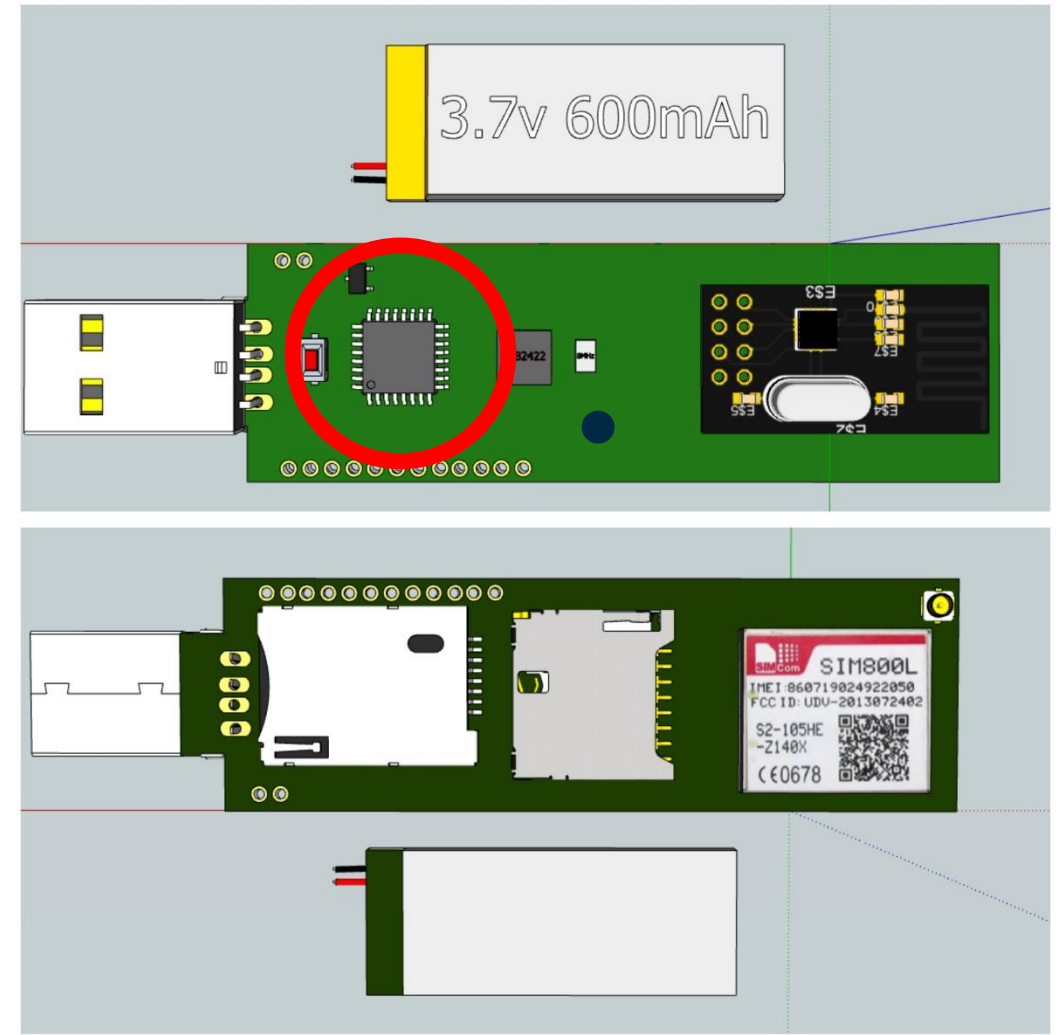
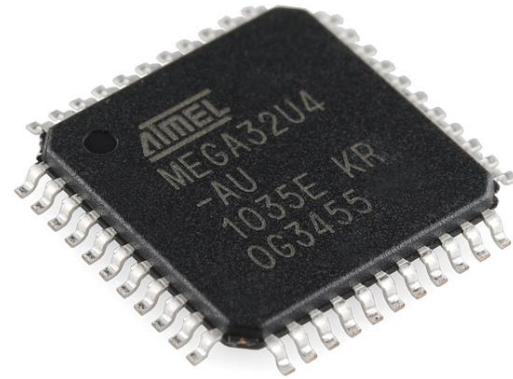
WHID Elite



COMING SOON

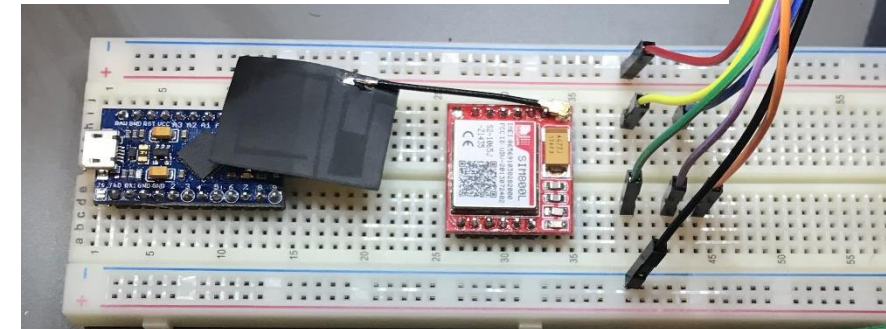
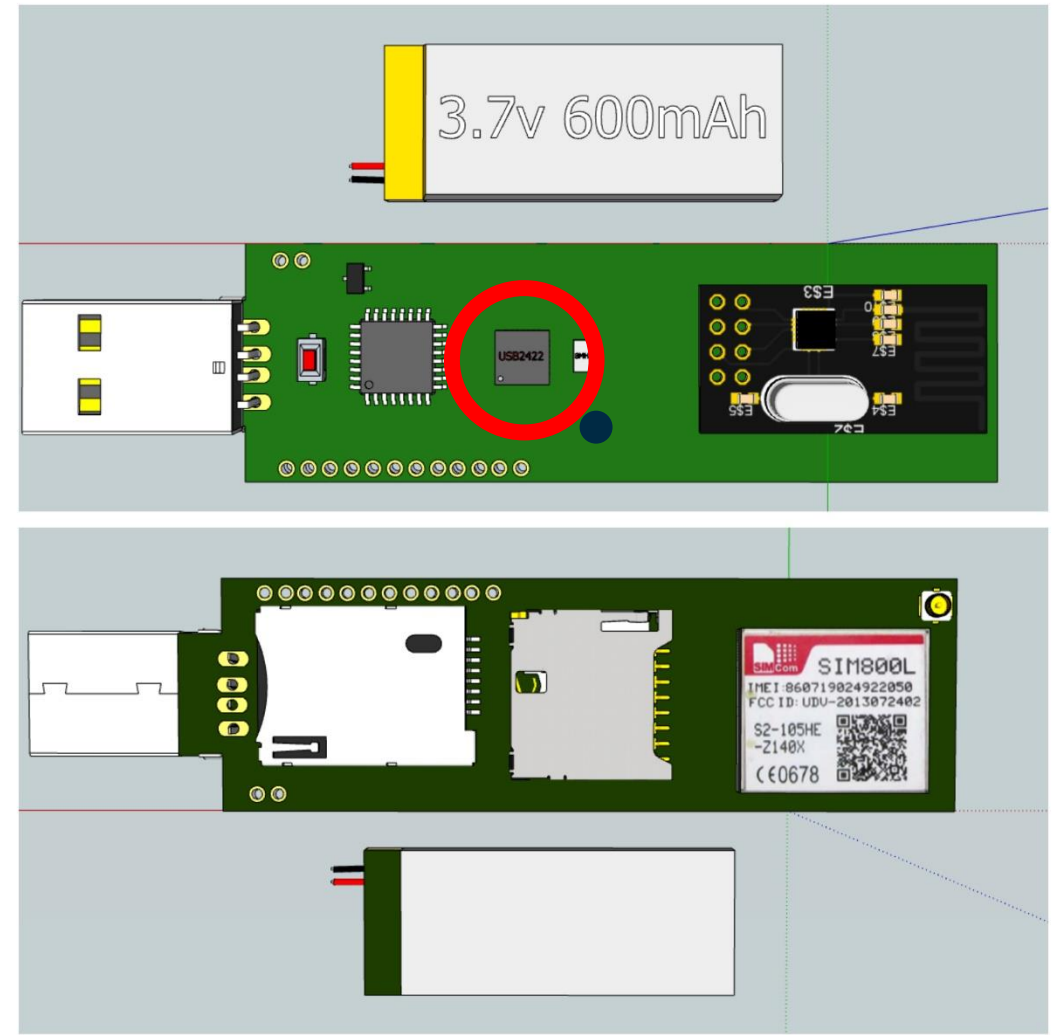
WHID Elite

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



WHID Elite

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



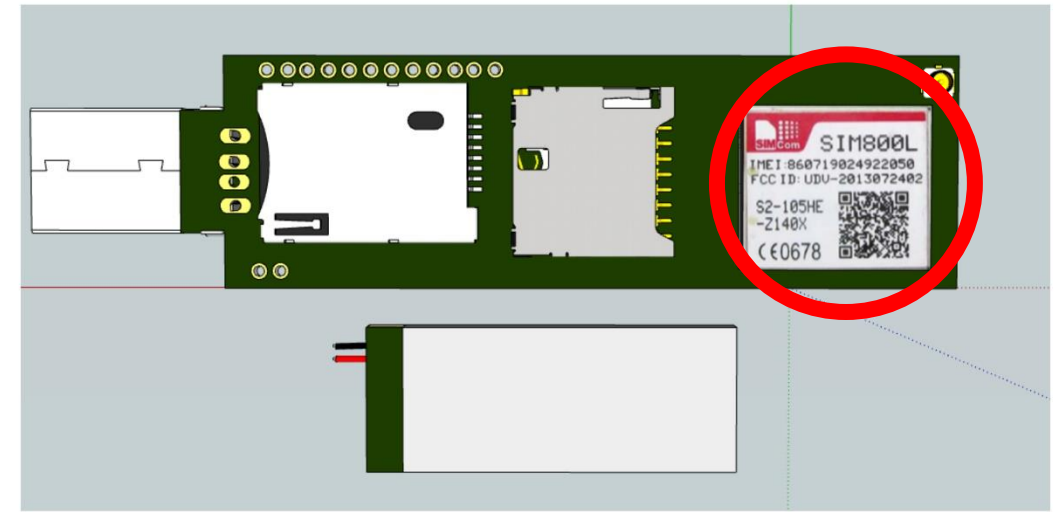
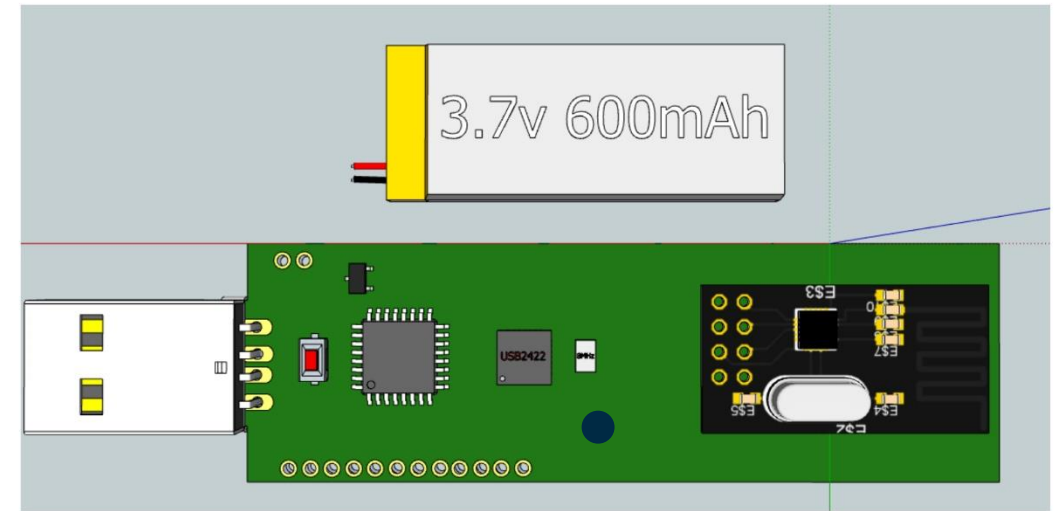
WHID Elite

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

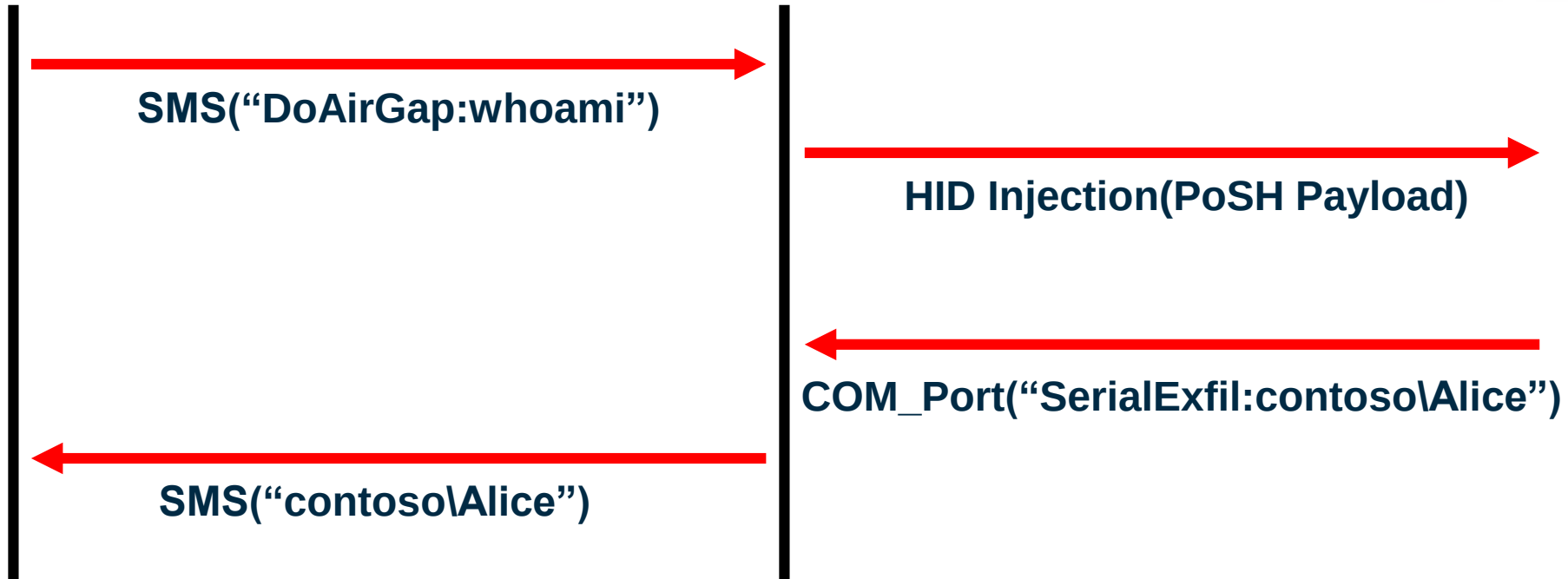
V.1.0 – 2G



V.2.0 – NB-IoT



2G/NB-IoT C&C Workflow



Air-Gapped Machines Vs. Threat Actors

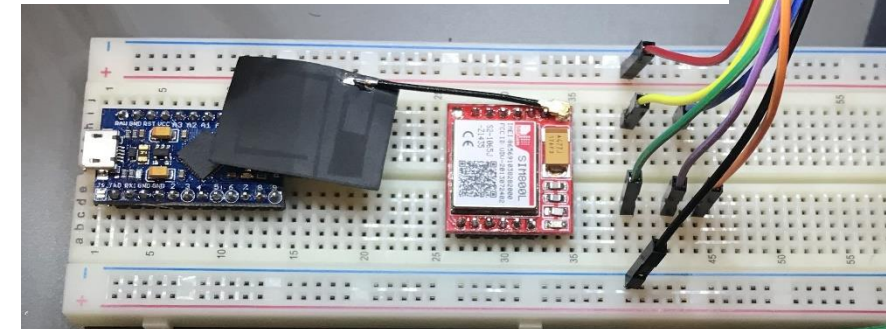
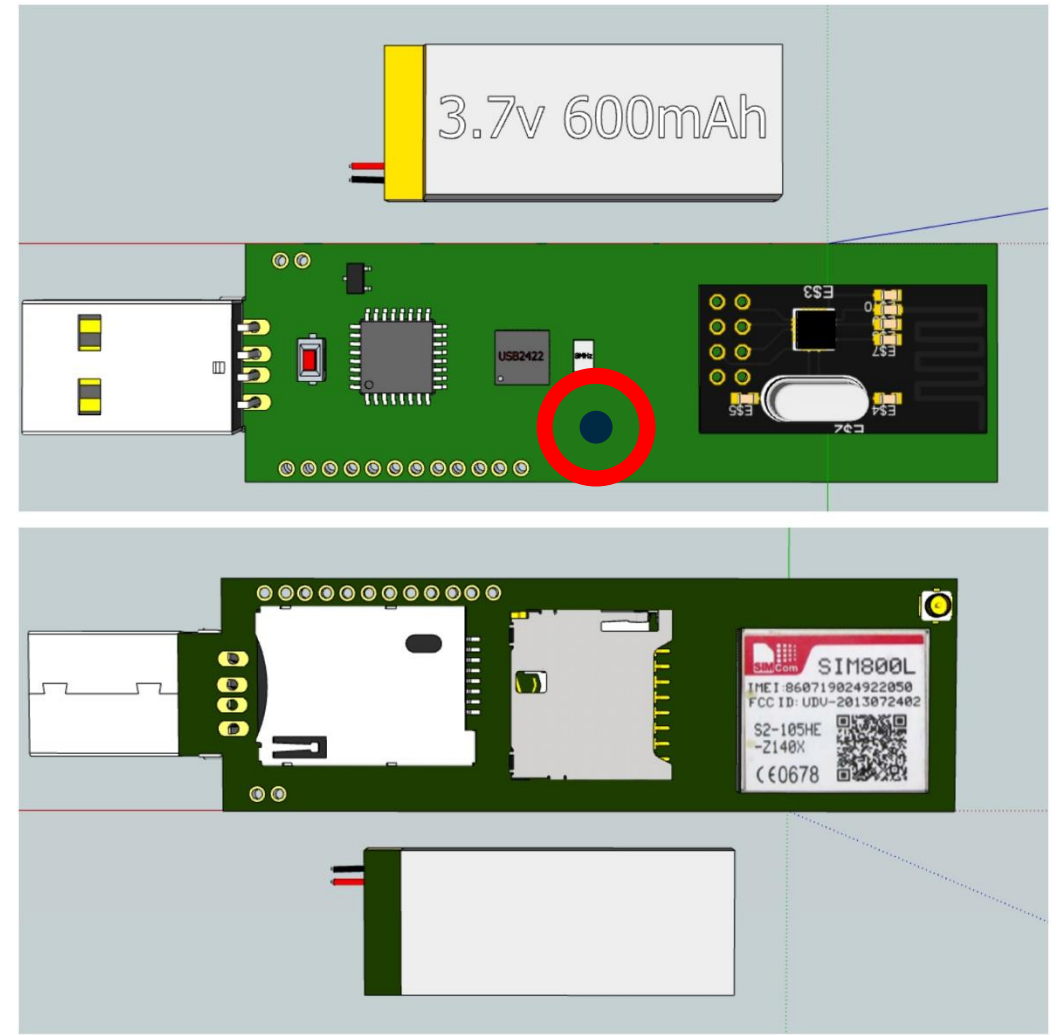
- An **Air-Gapped machine** is a computer that is so heavily secured that **it has no physical or digital connections to any networks.**
- They are usually also **heavily physically secured** in datacenters and server rooms **with carefully monitored physical access.**
- Typically a **cybercriminal** would have to physically breach the **facility** that it's in and **use some sort of external or removable media** for their attack.
- Air-Gapped machines are really inconvenient to maintain, so **computers are usually only Air-Gapped if they handle very, very sensitive data.**

Bypassing AirGapped Environments with WHID Elite

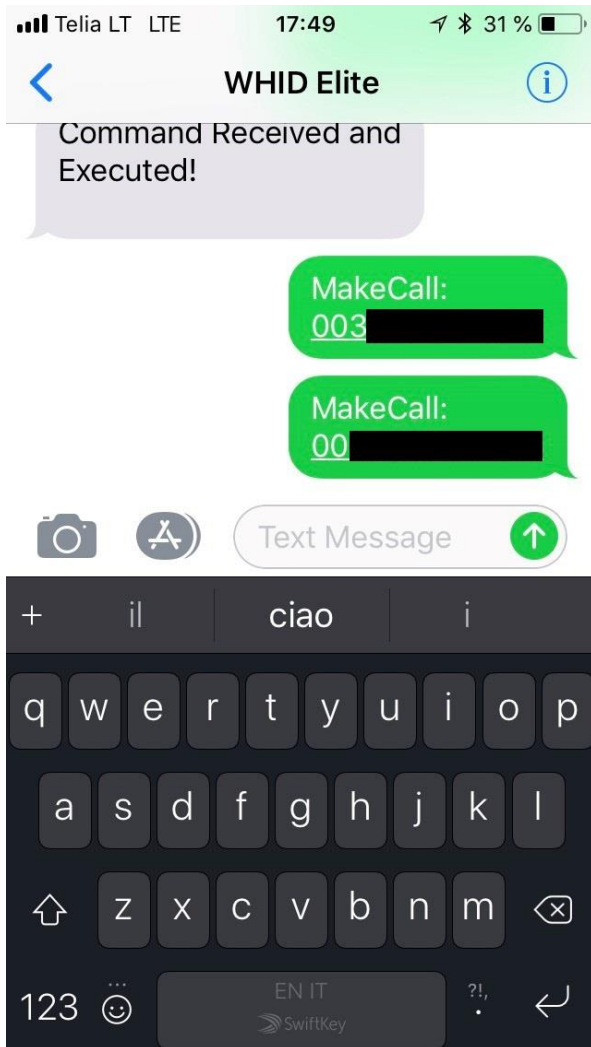


WHID Elite

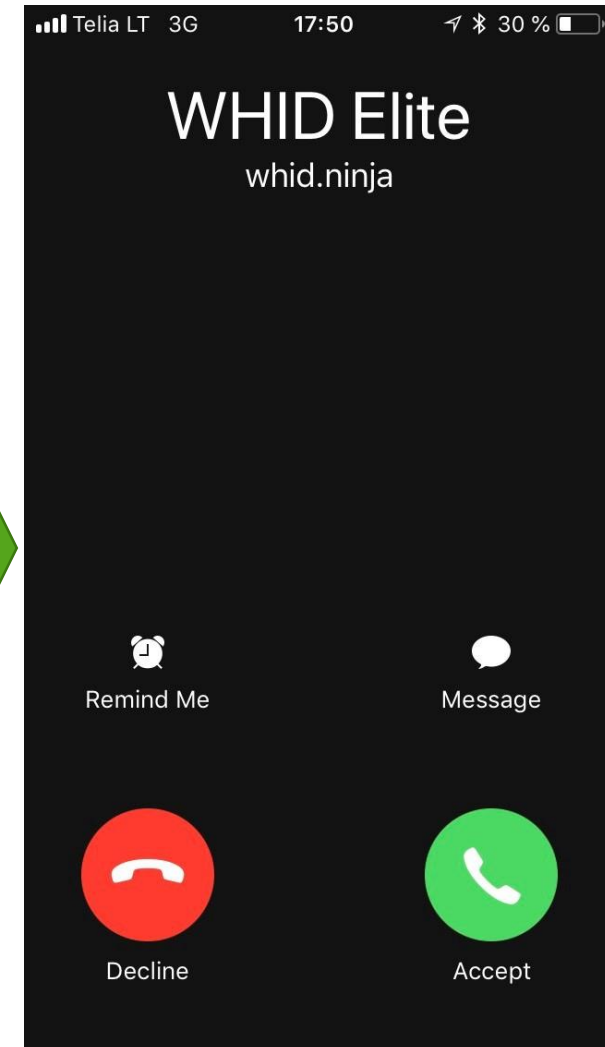
- Atmega 32u4
- USB2422 Controller
- sed 's/ESP/SIMxxxx/'
- **Microphone**
- NRF24L01+



Acoustic Surveillance

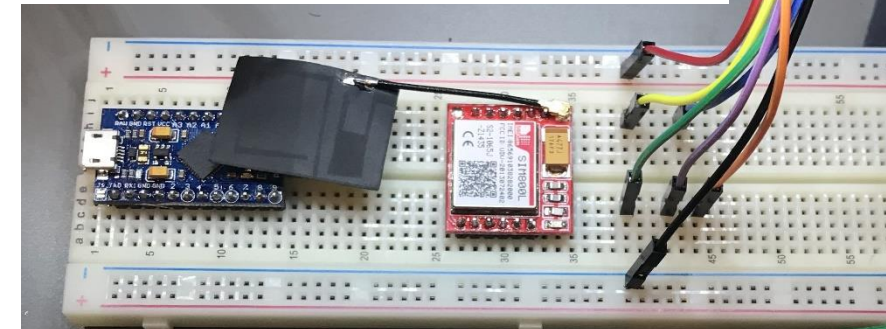
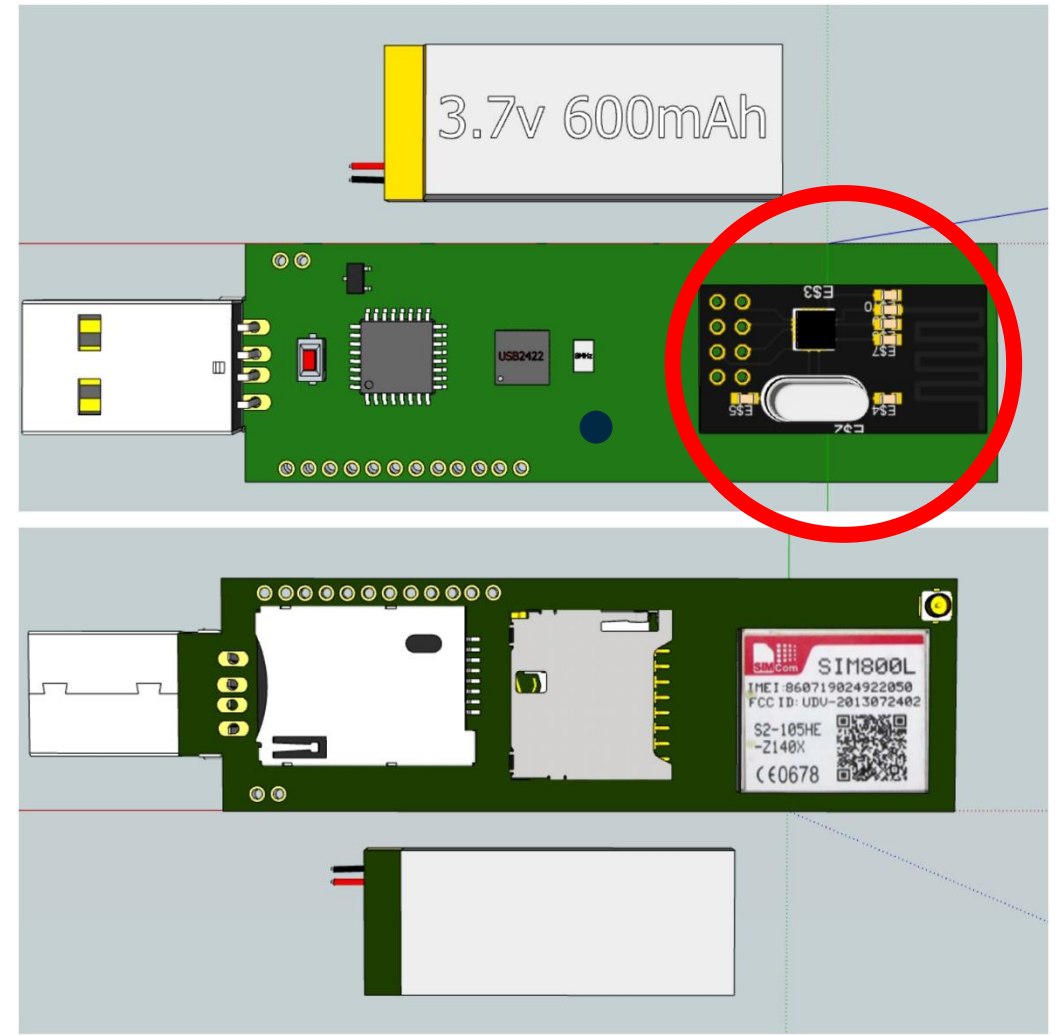
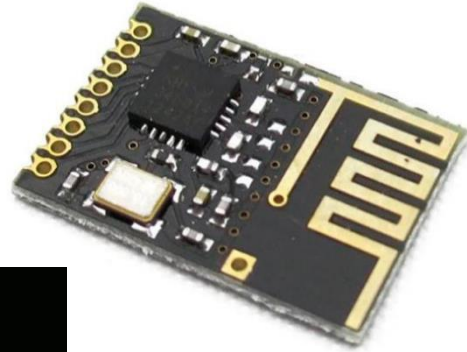


```
+CMTI: "SM",5
slot: 5
----> AT+CMGF=1
<---- OK
----> AT+CSDH=1
<---- OK
AT+CMGR=5
+CMGR: "REC UNREAD","+37[redacted]","[redacted]","18/06/09,17:49:51+12",145,4,0,0,"+3[redacted]",145,22
FROM: +3[redacted]
----> AT+CMGF=1
<---- OK
----> AT+CSDH=1
<---- OK
AT+CMGR=5
+CMGR: "REC READ","+3[redacted]","[redacted]","18/06/09,17:49:51+12",145,4,0,0,"+3[redacted]",145,22
MakeCall:003[redacted]
TEXT: MakeCall:003[redacted]
----> AT+CHFA=1
<---- OK
Mic Enabled!
----> AT+CMIC=1,10
<---- OK
Calling:
----> ATD003[redacted]:
<---- OK
Calling succesful!
### STARTING ACOUSTIC SURVEILLANCE ###
Sending reponse...
----> AT+CMGF=1
<---- OK
----> AT+CMGS="+3[redacted]"
<---- >
> Command Received and Executed!
^Z
```



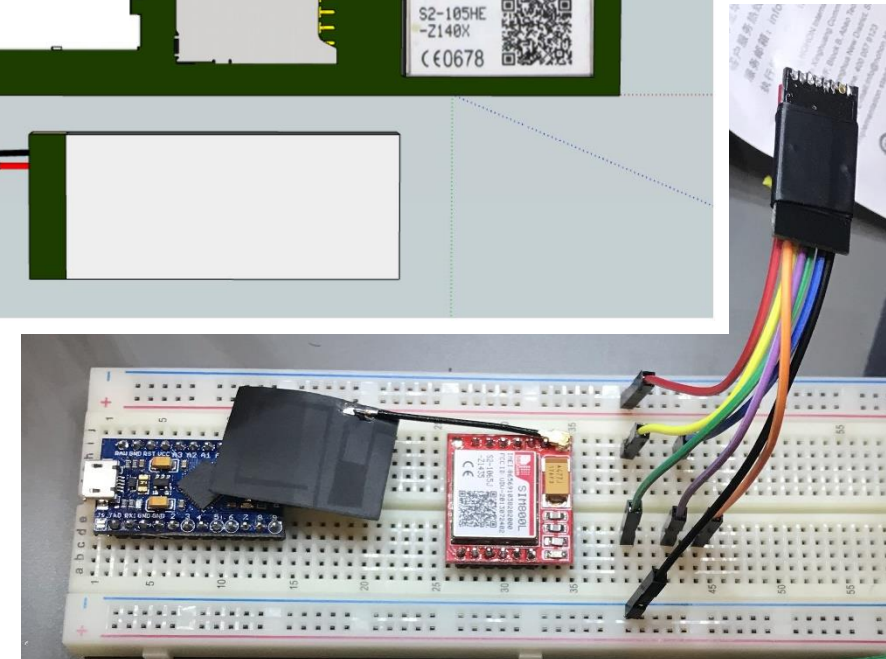
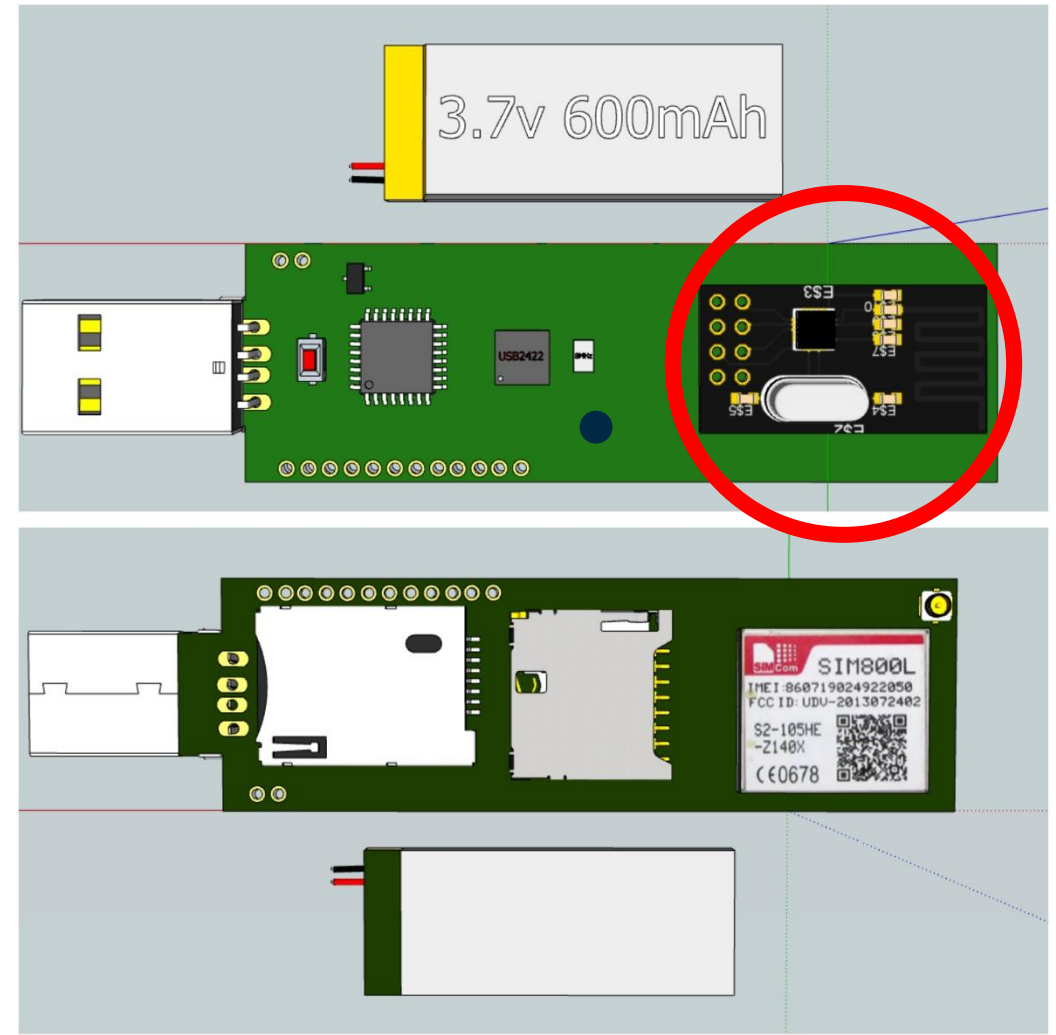
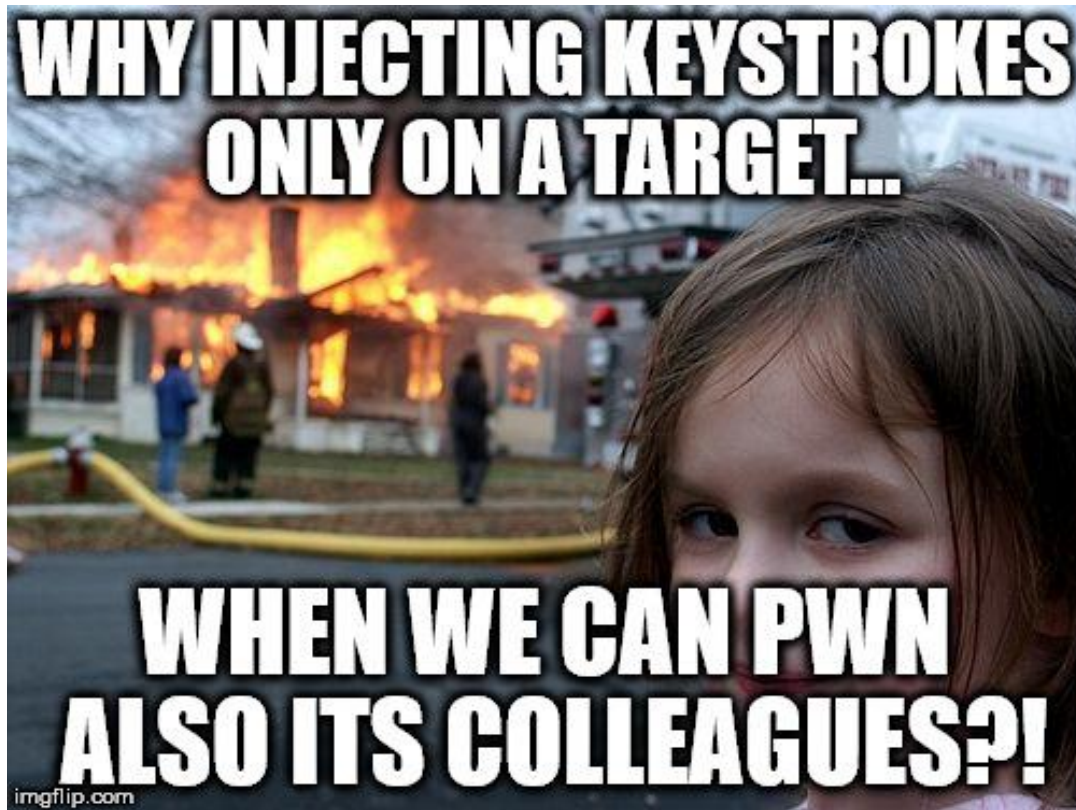
WHID Elite

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



WHID Elite

Mousejacking Wireless Keyboards & Mice





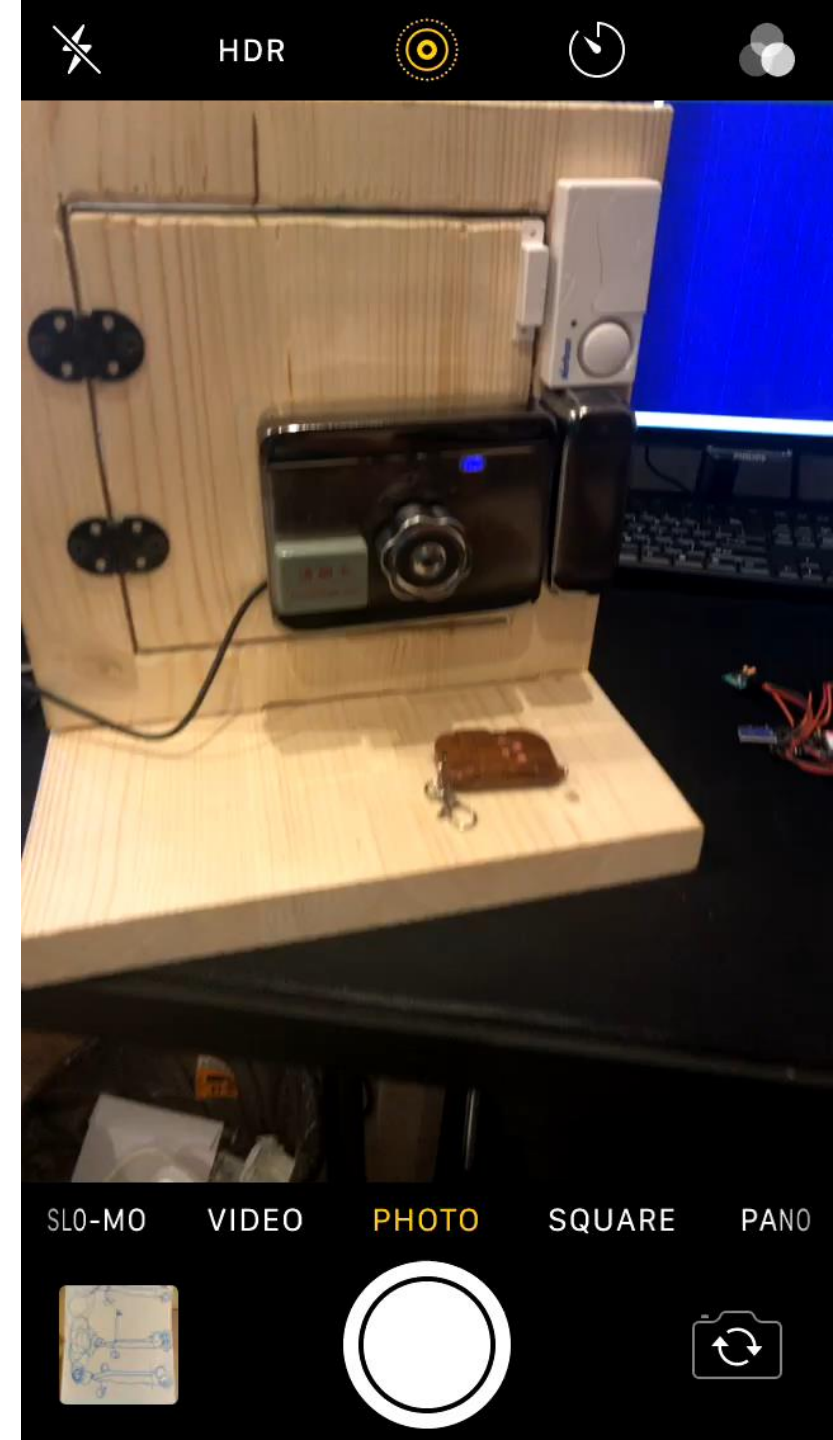
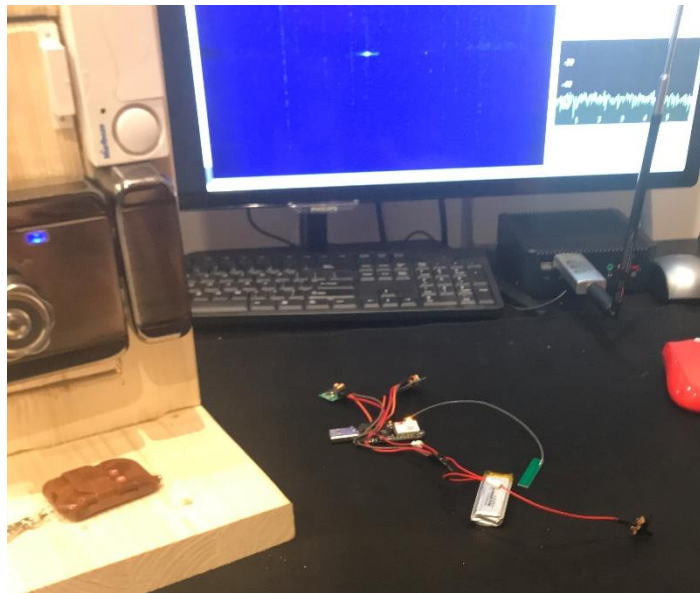
SOON...

SLO-MO VIDEO **PHOTO** SQUARE PANO



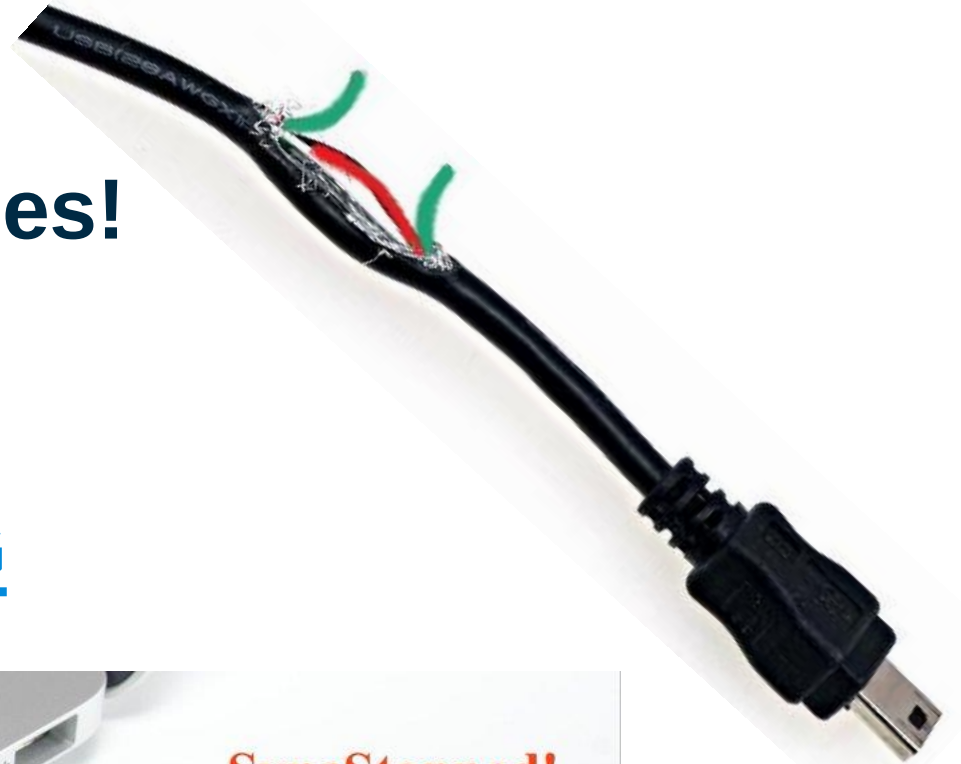
Remote Radio Hacking

- Embedded cheap 315/433MHz transmitters to:
 - Replay Attacks
 - Fuzzing
 - Bruteforcing
 - Jamming



Mitigations 101

- **Do Not Trust unknown USB Devices!**
- **At Most, Use an USB Condom!**
 - Or Create your own DIY version
- <https://github.com/robertfisk/USG>



Mitigation Tools – Linux

- <https://github.com/trpt/usbdeath>
 - Anti-forensic tool that writes udev rules for known usb devices and do some things at unknown usb insertion or specific usb device removal
- <https://github.com/USBGuard/usbguard>
 - Software framework for implementing USB device authorization policies



Mitigation Tools – Windows



- <https://github.com/pmsosa/duckhunt>

- **Four Operational Modes:**

- **Paranoid:** KB input is disallowed until a password is input. Attack will also be logged.
- **Normal:** KB input will temporarily be disallowed. Attack will also be logged.
- **Sneaky:** A few keys will be dropped. Attack will also be logged.
- **LogOnly:** Simply log the attack.

- <https://github.com/JLospinoso/beamgun>

- When a malicious HID is inserted it blocks keystrokes injection by continuously stealing focus (and eventually locking the workstation)

Fin

XII STIC CCN-CERT CONFERENCES

Cybersecurity,
towards effective response and deterrence



➤ Email

- info@ccn-cert.cni.es
- ccn@cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- oc.ccn.cni.es

➤ Follow us on

