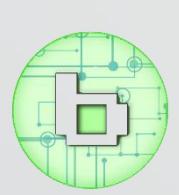


# WHID

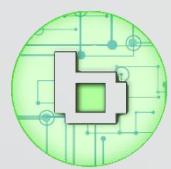


# Injector



Sono Francesco Ressa mi occupo di informatica dal 1990.

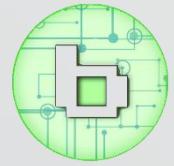
- Presidente di bit01
- Certificato Linux Essentials
- Teacher abilitato da LPI
- Moderatore di Ethical Hacker Italiani la più grande community italiana di hacking
- Sono un libero professionista e collaboro con aziende di cyber security



- Non inserire nei vostri dispositivi chiavette usb “trovate casualmente”.
- Diffidare da chi vi “regala” qualche oggetto usb senza un plausibile motivo.
- Non fare accedere fisicamente, se non in vostra presenza, al vostro dispositivo.
- Inserire una password di accesso al vostro PC.

# Gli attacchi informatici





# ESPERIMENTO SOCIALE

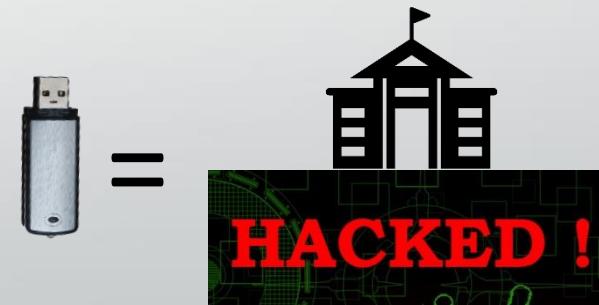
2016

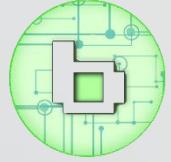


300



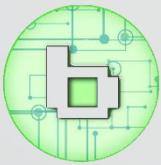
$$\frac{135}{45\%}$$





# PAYLOAD

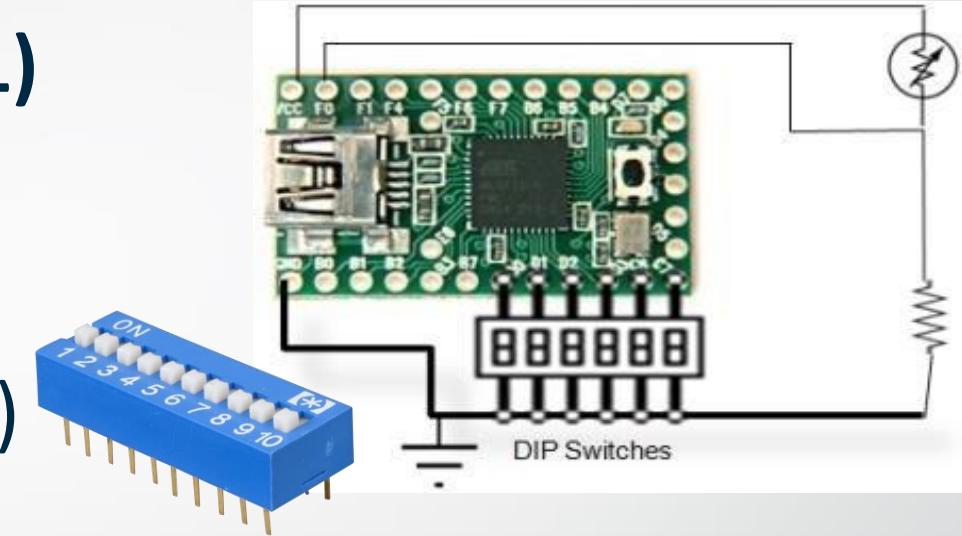
Quell'insieme di azioni che vengono eseguite dopo aver infettato o essere penetrati in un sistema.



# Offensive Devices – 1<sup>st</sup> Generation

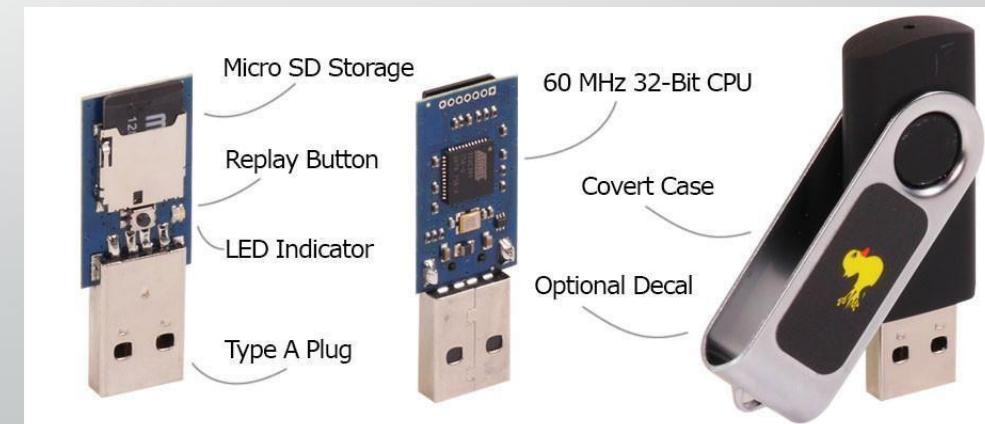
- **Teensy – (PHUKD 2009 & Kautilya 2011)**

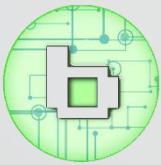
- DIY Solution
- Multiplatform (Win, \*nix, OSX)
- Multipayload (through DIP-Switches)



- **Rubberducky (2010)**

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





# Piccolo approfondimento sulla Rubberducky

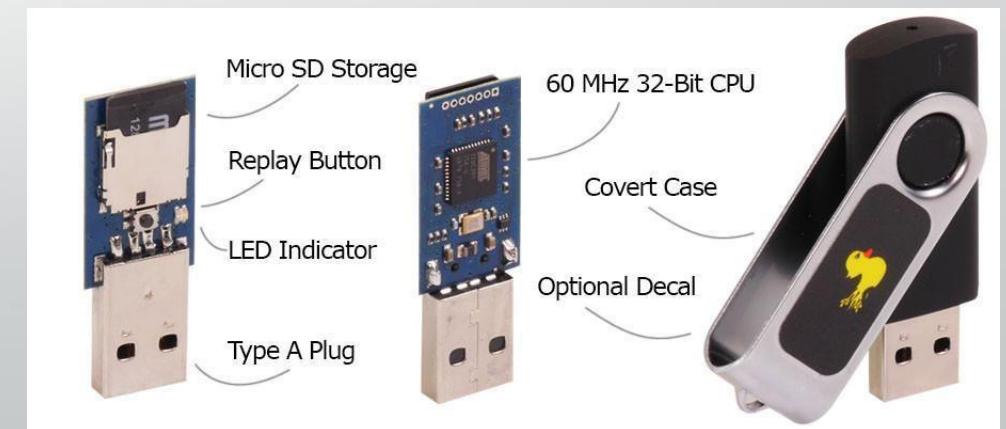
## Rubberducky (2010)

**inject.bin - payload predefinito (verrà sempre eseguito per primo)**

**inject2.bin - NUM\_LOCK**

**inject3.bin - CAPS\_LOCK**

**inject4.bin – INS**



# Offensive Devices – 2<sup>nd</sup> Generation

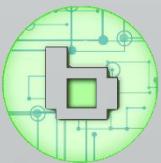
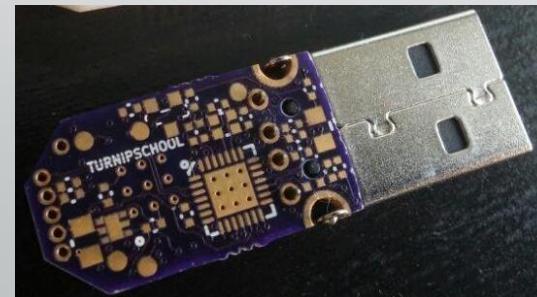
- **BadUSB (2014)**

- It exploits the controllers 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 – 3<sup>rd</sup> Generation



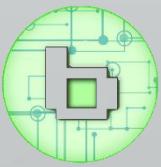
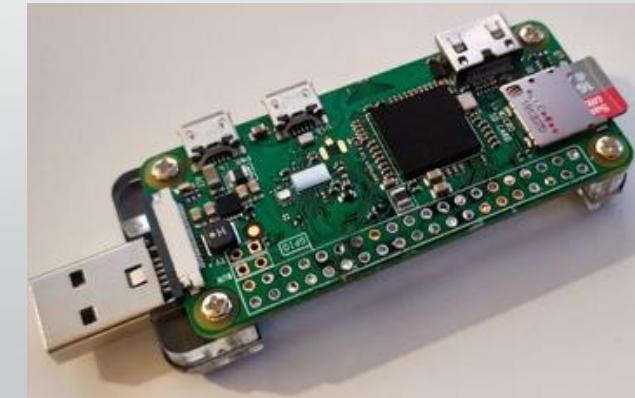
- **WHID Injector (2017) – A Rubberducky evolution**

- Dedicated Hardware
- Open source
- Multiplatform (Win, \*nix, OSX)
- Changeable VID/PID
- Has WiFi and USB



- **P4wnP1 (2017) – A Bash Bunny on Steroids**

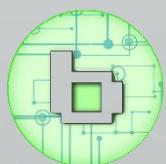
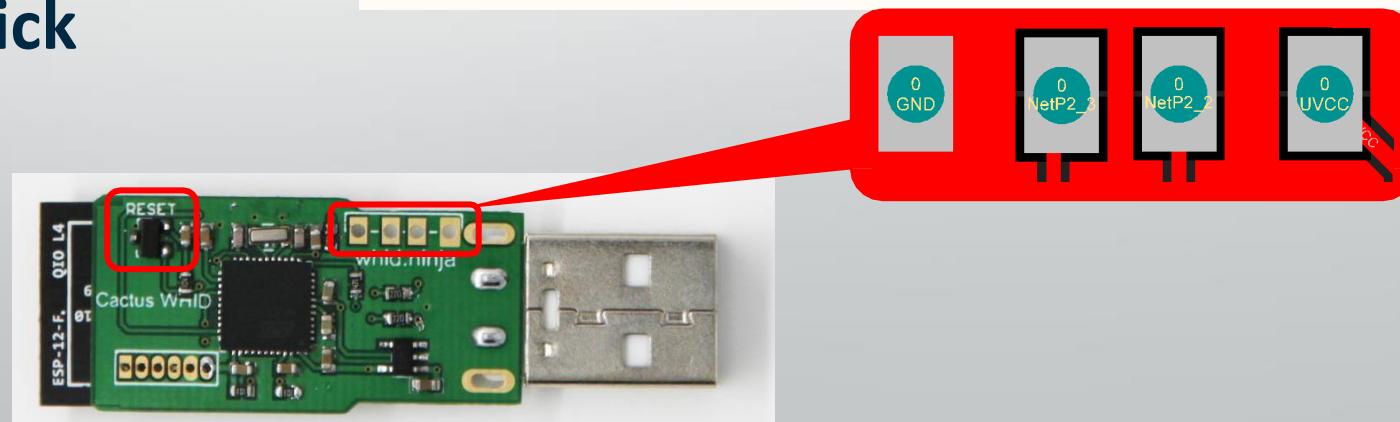
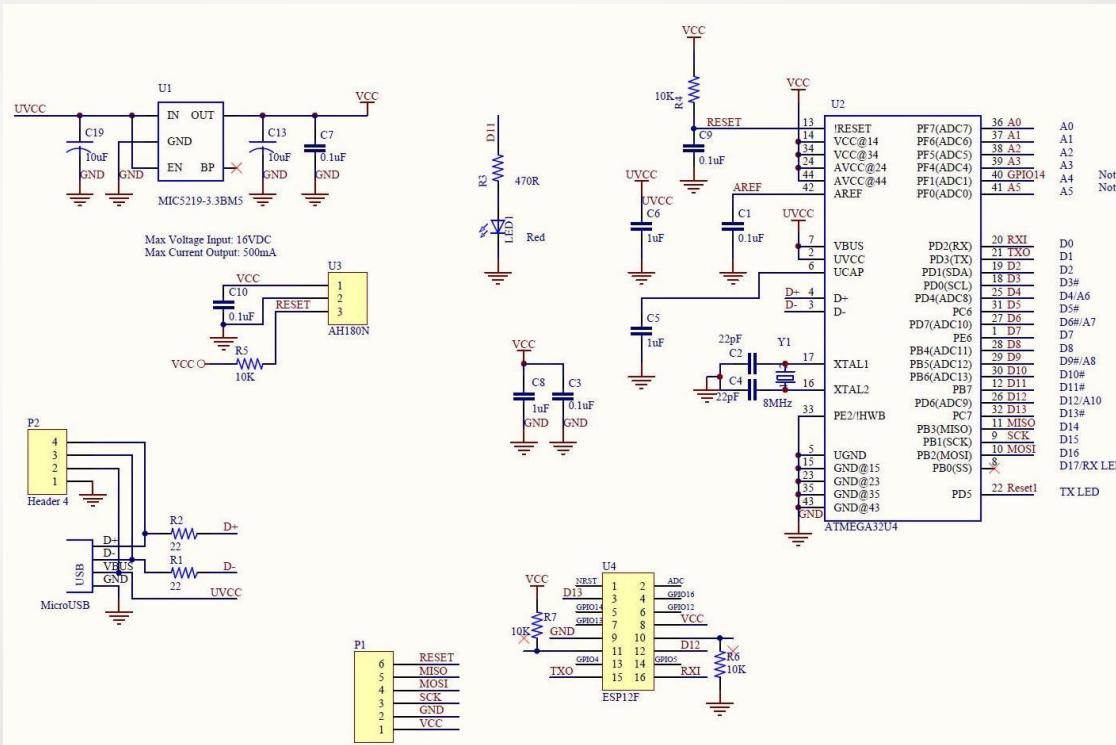
- Based on RPi Zero W (~15 €)
- Has WiFi and USB
- It can emulate USB Key FileSystem
- Changeable VID/PID
- NexMon WiFi Drivers
- Next Gen AirGap bypass



Ressa F.

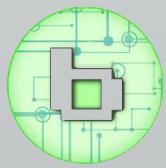
# WHID Injector – Schematics & Specs

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

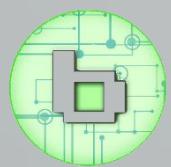
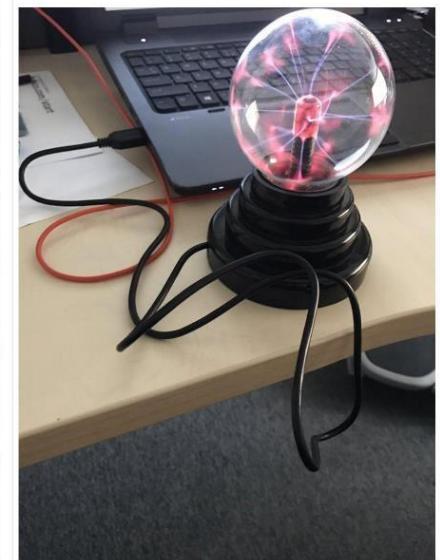


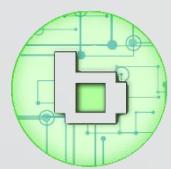
Ressa F.

# Weaponizing USB Gadgets



# Weaponizing USB Gadgets





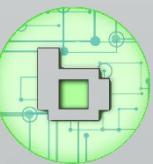
## Cos'è?

- WHID Injector usb è, detto in parole semplici, una Rubber duck di Hak5 con connessione Wi-Fi, quindi più evoluta.
- In pratica è una chiavetta USB che utilizza un modulo WiFi ESP-12S con una connessione ad un microcontrollore 32u4.
- Questo dispositivo consente l'invio di sequenze di tasti e script interattivi tramite WiFi a una macchina di destinazione, e quindi compie delle azioni nel pc della vittima
- Il dispositivo ha 4 MB (ne possiamo utilizzare fino a 3) di memoria flash che servono sia a memorizzare il firmware sia payload.
- Quando viene inserita in un pc esso la rileva come Tastiera HID.

# 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 tools DLP
- Not detected by Antiviruses



# Software Frameworks – ESPloitV2 GUI

Si controlla con interfaccia web

**ESPloit v2.7.41** - WiFi controlled HID Keyboard Emulator



by *Corey Harding*

[www.LegacySecurityGroup.com](http://www.LegacySecurityGroup.com) / [www.Exploit.Agency](http://www.Exploit.Agency)

-----  
File System Info Calculated in Bytes

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

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

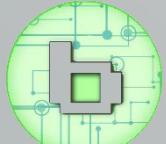
-  
[Choose Payload](#) - [Upload Payload](#)

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

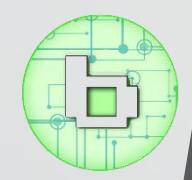
-  
[Configure ESPloit](#)

-  
[Upgrade ESPloit Firmware](#)

-  
[Help](#)



Ressa F.



# Live payload mode

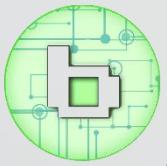
[<- BACK TO INDEX](#)

[List Payloads](#)

[Upload Payload](#)

Payload:

[Run Payload](#)



# Input mode

[-> BACK TO INDEX](#)

## InputMode

Note: On configuration page set "Delay Before Starting a Live Payload:" to "0" under "Payload Settings:" to avoid a delay when using Input Mode.

Print:

Mouse    Up              Left Click      ArrowKeys    Up              Tab  
Left    Click    Right      Left            Enter    Right    Alt+Tab  
Down             Right Click      Down            Shift+Tab

PrintLine:

Function Keys: F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12

Misc Keys: ESC HOME END INSERT DEL BACKSPACE SPACE BAR PAGE UP PAGE DOWN

Win: GUI-Key GUI+r cmd+EnterKey osk+EnterKey Alt+F4 Ctrl+Alt+Del Ctrl+Shift+Esc

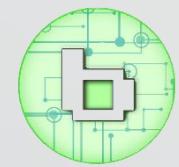
Mac: Right of Left Shift Key, z Left of Right Shift Key, /

Linux: Alt+F2, Application Finder gnome-terminal+EnterKey CTRL+c CTRL+x

Bios: F1 F2 F8 F12 DEL ESC



Linux Day 2022



# Duckuino Mode

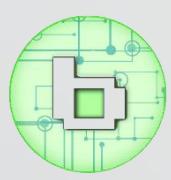
<- BACK Convert

Run Payload

```
DELAY 750
GUI r
DELAY 1000
STRING powershell Start-Process notepad -Verb runAs
ENTER
```

```
CustomDelay:750
Press:131+114
CustomDelay:1000
Print:powershell Start-Process notepad -Verb runAs
Press:176
```

i - Done parsed 6 lines in 2ms



# Choose Payload

[<- BACK TO INDEX](#)

File System Info Calculated in Bytes

**Total:** 2949250 **Free:** 2919381 **Used:** 29869

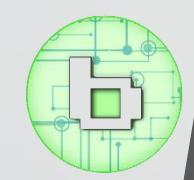
[Upload Payload](#)

[Live Payload Mode](#)

Display Payload Contents	Size in Bytes	Run Payload	Download File	Delete Payload
<a href="#">/payloads/inject.bin</a>	106	<a href="#">Run Payload</a>	<a href="#">Download File</a>	<a href="#">Delete Payload</a>
<a href="#">/payloads/infomation.bin</a>	9982	<a href="#">Run Payload</a>	<a href="#">Download File</a>	<a href="#">Delete Payload</a>
<a href="#">/payloads/information.txt</a>	6217	<a href="#">Run Payload</a>	<a href="#">Download File</a>	<a href="#">Delete Payload</a>
<a href="#">/payloads/duck_text.txt</a>	7912	<a href="#">Run Payload</a>	<a href="#">Download File</a>	<a href="#">Delete Payload</a>
<a href="#">/payloads/prova2.txt</a>	100	<a href="#">Run Payload</a>	<a href="#">Download File</a>	<a href="#">Delete Payload</a>
<a href="#">/payloads/pay.txt</a>	1479	<a href="#">Run Payload</a>	<a href="#">Download File</a>	<a href="#">Delete Payload</a>



Linux Day 2022



# Upload Payload

[<- BACK TO INDEX](#)

[List Payloads](#)

[Live Payload Mode](#)

**Upload Payload:**

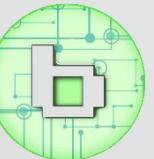
Sfoglia...

Nessun file selezionato.

Upload



Linux Day 2022



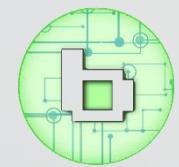
# Format File System

[<- BACK TO INDEX](#)

This will reformat the SPIFFS File System.

Are you sure?

[YES - NO](#)



# Configure ESPloit

## ESPloit Settings

[Restore Default Configuration](#)

### WiFi Configuration:

#### Network Type

Access Point Mode:  Join Existing Network:

#### Hidden

Yes   
No

SSID: Exploit

Password: ██████████

Channel: 6

IP: 192.168.0.1

Gateway: 192.168.0.1

Subnet: 255.255.255.0

### ESPloit Administration Settings:

Username: admin

Password: ██████████

### FTP Exfiltration Server Settings

Changes require a reboot.

Enabled   
Disabled

FTP Username: ftp-admin

FTP Password: ██████████

### ESPortal Credential Harvester Settings

Changes require a reboot.

When enabled ESPloit main menu will appear on <http://IP-HERE/esploit>

Do not leave any line blank or as a duplicate of another.

Enabled   
Disabled

Welcome Domain: ouraccesspoint.com

Welcome Page On: /welcome

Site1 Domain: fakesite1.com

Site1 Page On: /login

Site2 Domain: fakesite2.com

Site2 Page On: /sign-in

Site3 Domain: fakesite3.com

Site3 Page On: /authenticate

Catch All Page On: /user/login

### Payload Settings:

Delay Between Sending Lines of Code in Payload:

2000  milliseconds (Default: 2000)

Delay Before Starting a Live or Auto Deploy Payload:

2998  milliseconds (Default: 3000)

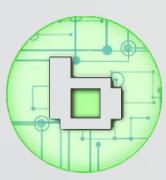
### Automatically Deploy Payload Upon Insertion

Yes   
No

Automatic Payload: /payloads/payload.txt

[Apply Settings](#)

[Reboot Device](#)



# Oggi vedremo in azione quest'oggetto con vari payload

- Esfiltrazione credenziali social in particolare Facebook
- Spegnimento schede di rete su pc vittima
- Disabilitare antivirus del pc vittima
- Svuotamento cestino del pc vittima
- Otttenere informazioni sul pc vittima

Grazie

