

---

# WHID



# Injector

# Gli attacchi informatici



# ESPERIMENTO SOCIALE

2016



30



135  
45%



=



**HACKED !**

# Human Interface Devices

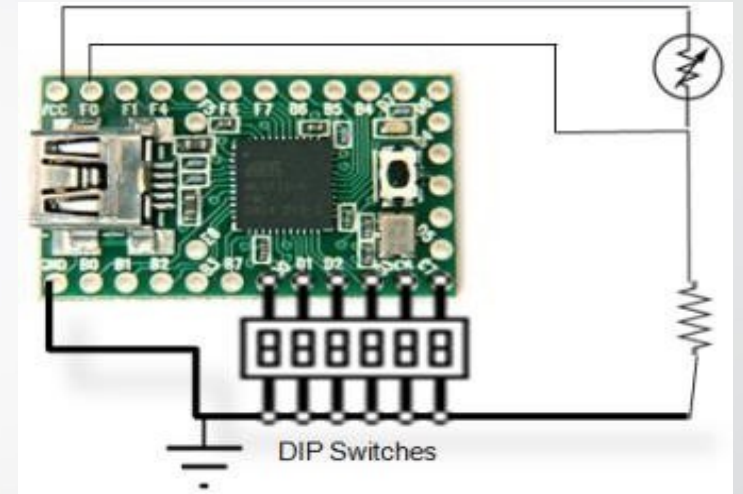
“A **human interface device** or **HID** is a type of computer device usually used by humans and takes input and gives output to humans.”

- 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

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

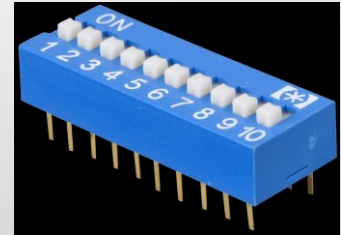
- **Teensy 2008**

- DIY Solution
- Multiplatform (Win, \*nix, OSx)
- Arduino-IDE programmable
- Multipayload (through DIP-Switches)



- **PHUKD 2009**

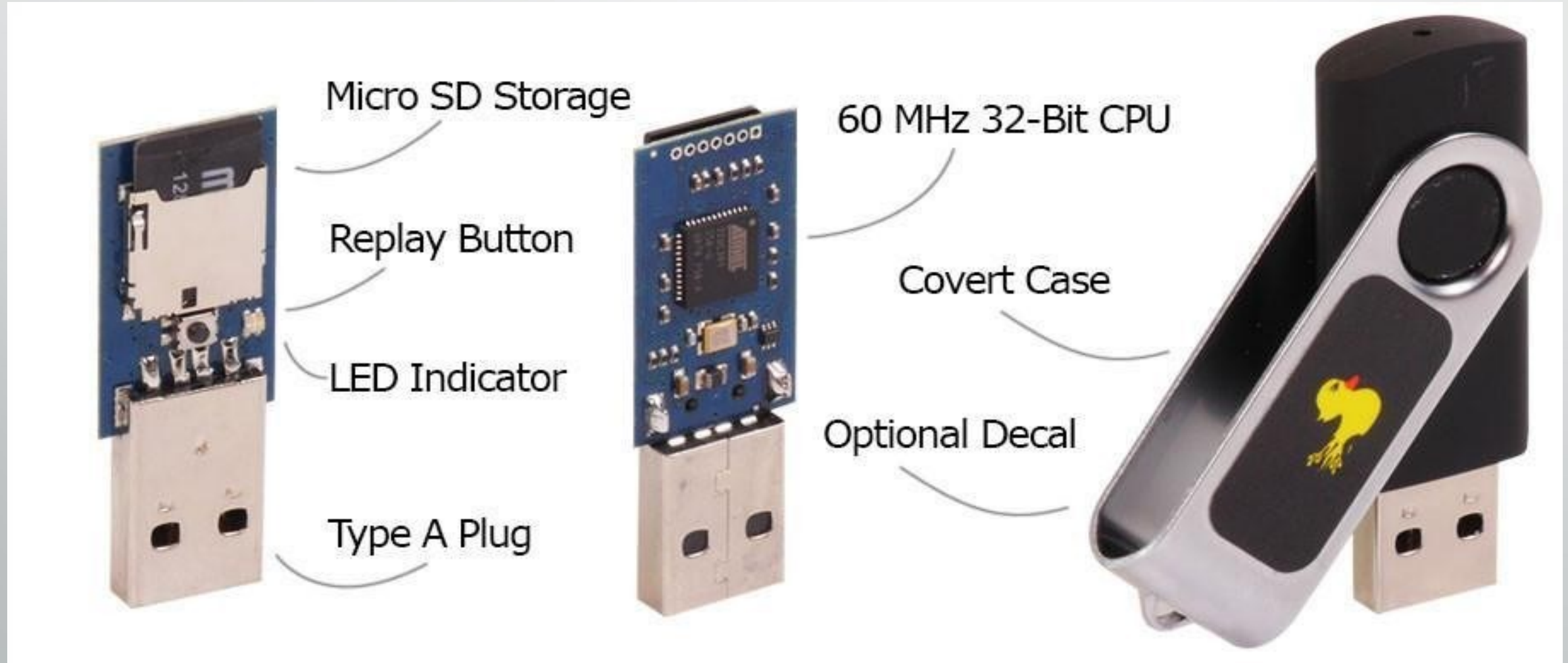
- Programmable HID USB Keystroke Dongle



- **Kautilia 2010**

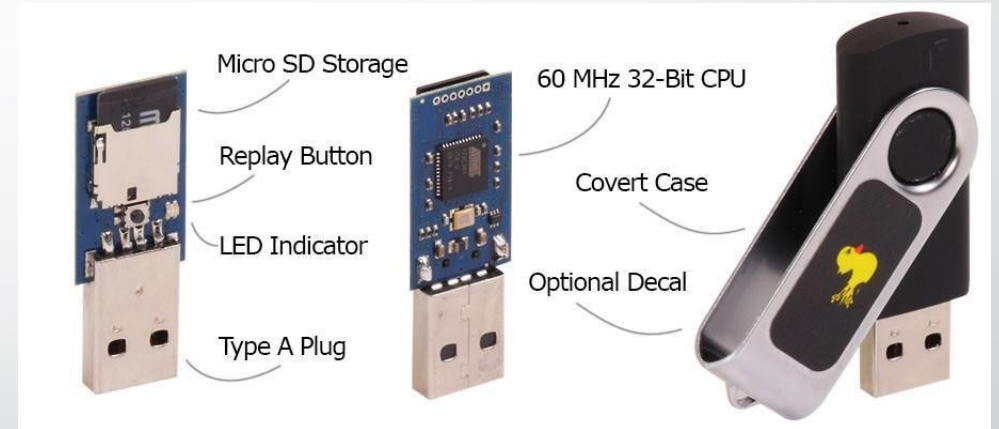
- Framework di payload

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



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

- **Rubberducky (2010-2011)**
  - Dedicated Hardware
  - Multiplatform (Win, \*nix, OSX)
  - Can emulate Keyboard & USB Disk
  - Changeable VID/PID
  - Multipayload (CAPS-INS-NUM)



# Piccolo approfondimento sulla Rubberducky

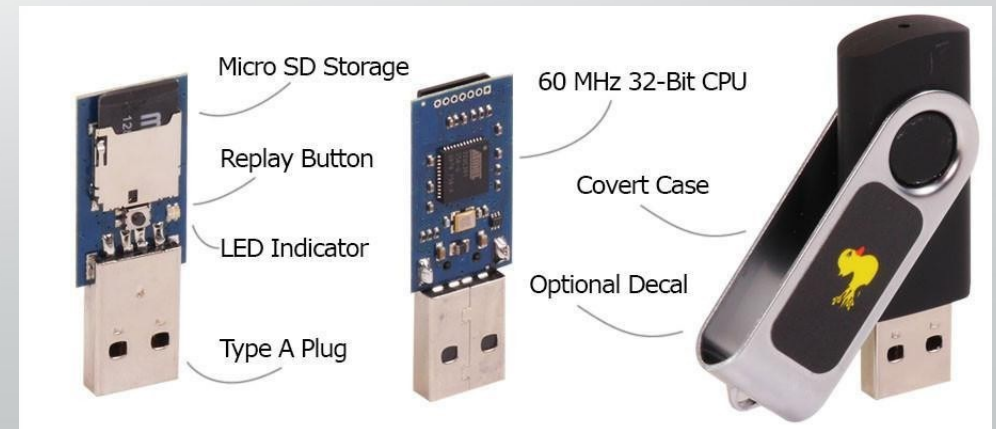
## Rubber Ducky (2010)

**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

- **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

- **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

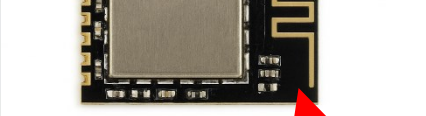


- **WHID Injector (2017) – A Rubber Ducky evolution**

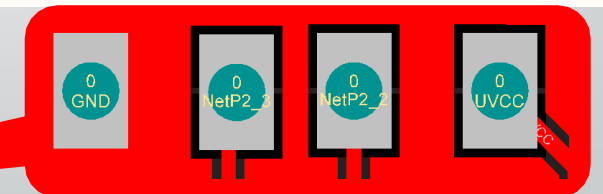
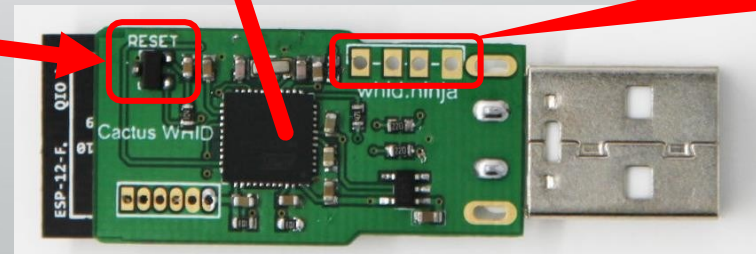
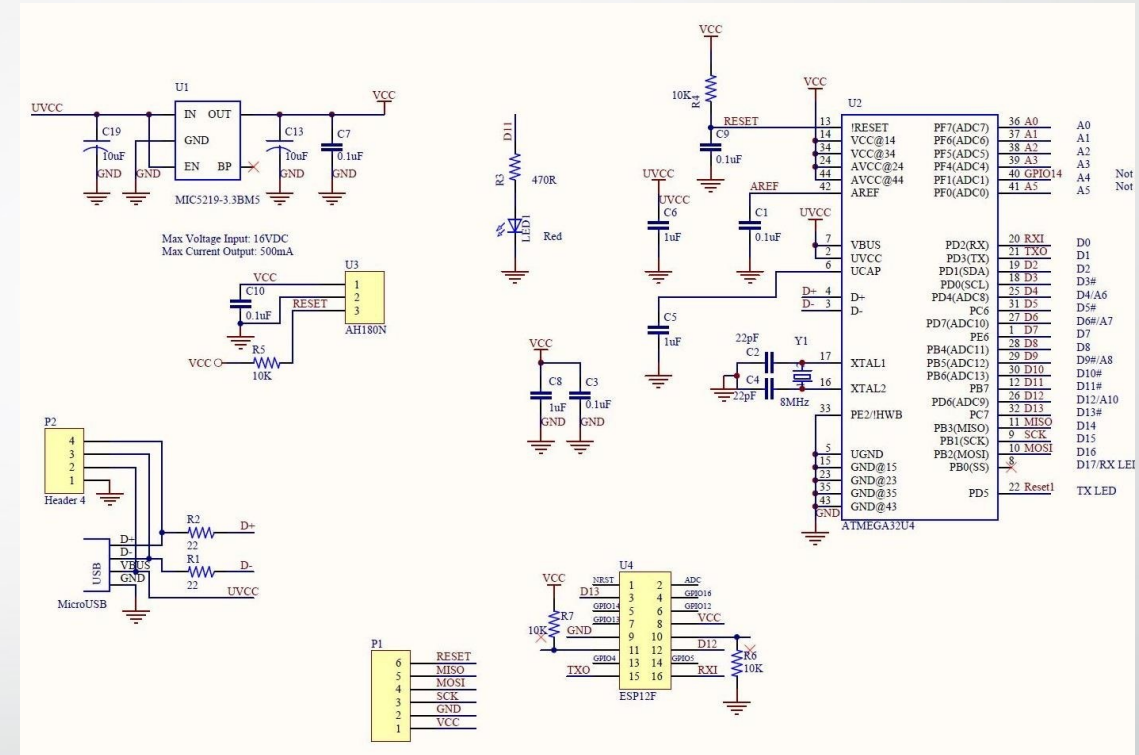
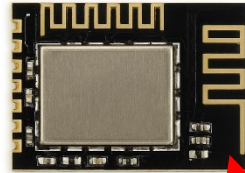
- Dedicated Hardware
- Open source
- Multiplatform (Win, \*nix, OSX)
- Changeable VID/PID
- Has WiFi and USB



# WHID Injector – Schematics & Specs

- **Atmega 32u4**
    - Arduino
  - **ESP-12F**
    - WiFi (both AP and Client modes)
    - 4MB Flash
  - **Pinout for weaponizing USB gadgets**
  - **HALL Sensor for easy unbrick**
- 
- A small black microcontroller board, likely an ATmega32u4, is shown in the top right corner. It has a square chip in the center and various pins along the edges. A red arrow points from the right side of the image towards the board.

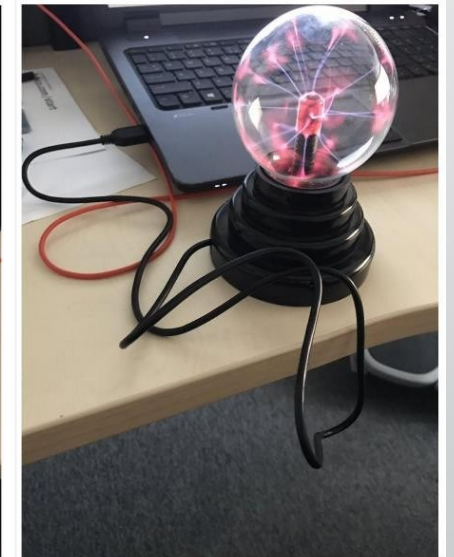
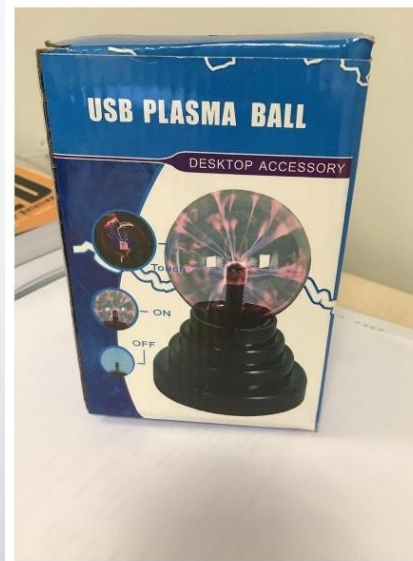
**ESP-12F = modulo ESP8266  
(chip + flash + antenna)**



# Weaponizing USB Gadgets



# Weaponizing USB Gadgets



# Software Frameworks – ESPloitV2 GUI

Si controlla con interfaccia web

**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](#)

# Comandi chiave

- **PrintLine**: digita il testo e invia un Invio (newline) alla macchina.
- **CustomDelay**: sospende l'esecuzione per un intervallo specificato (ritardo personalizzato).
- **Print**: digita il testo senza premere Invio.
- **Press**: simula la pressione di uno o più tasti.
- **Rem**: commento; la linea viene ignorata dallo script.
- **BlinkLED**: fa lampeggiare il LED del dispositivo.

# Codici HID

## Tabella Codici e Tasti in fase Press

| Codice / Combinazione | Tasto |
|-----------------------|-------|
| 131                   | win   |
| 114                   | r     |
| 128                   | ctrl  |
| 116                   | t     |
| 179                   | tab   |
| Press:126             |       |
| Press:96              | \     |
| Press:129+236         | >     |

**Win+r = Press:131+114**

# Codici HID

## Tabella Codici e Tasti in fase Print

| Codice / Combinazione | Tasto / Simbolo |
|-----------------------|-----------------|
| ]                     | +               |
| }                     | *               |
| @                     | "               |
| >                     | :               |
| -                     | ,               |

"c:\Users\Public\ps.txt "

Print:@C>

Press:96

Print:Users

Press:96

Print:Public

Press:96

Print:ps.txt@

# 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:

Send Text

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

PrintLine:

Send Text+Enter

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

# 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           | Run Payload | Download File | Delete Payload |
| <a href="#">/payloads/infomation.bin</a>  | 9982          | Run Payload | Download File | Delete Payload |
| <a href="#">/payloads/information.txt</a> | 6217          | Run Payload | Download File | Delete Payload |
| <a href="#">/payloads/duck_text.txt</a>   | 7912          | Run Payload | Download File | Delete Payload |
| <a href="#">/payloads/prova2.txt</a>      | 100           | Run Payload | Download File | Delete Payload |
| <a href="#">/payloads/pay.txt</a>         | 1479          | Run Payload | Download File | Delete Payload |

# Upload Payload

[<- BACK TO INDEX](#)

[List Payloads](#)

[Live Payload Mode](#)

**Upload Payload:**

Sfoggia...

Nessun file selezionato.

Upload

# 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:

Password:

Channel:

IP:

Gateway:

Subnet:

### ESPloit Administration Settings:

Username:

Password:

### FTP Exfiltration Server Settings

Changes require a reboot.

Enabled ☒

Disabled ☐

FTP Username:

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:

Welcome Page On:

Site1 Domain:

Site1 Page On:

Site2 Domain:

Site2 Page On:

Site3 Domain:

Site3 Page On:

Catch All Page On:

### Payload Settings:

Delay Between Sending Lines of Code in Payload:

milliseconds (Default: 2000)

Delay Before Starting a Live or Auto Deploy Payload:

milliseconds (Default: 3000)

### Automatically Deploy Payload Upon Insetion

Yes ☐

No ☒

Automatic Payload:

Apply Settings

Reboot Device

## Vantaggi

- **Plug-and-play:** Nessun driver richiesto, riconosciuta subito come tastiera
- **Facilità di scripting:** Payload testuali editabili rapidamente
- **Cross-platform:** Funziona su Linux – Windows - MacOS

## Svantaggi

- **Sessione bloccata:** Se il pc è bloccato i payload non possono eseguire azioni
- **Accesso fisico necessario:** La WHID richiede collegamento USB diretto
- **Comandi e azioni visibili:** Apertura finestre, digitazioni ecc. sono visibili

# Contromisure

- **Controllo fisico: limitare l'accesso ai PC al personale autorizzato;**
- **Disabilitare porte a livello firmware/BIOS;**
- **Whitelist VID/PID: consentire solo device di classe HID con VID/PID registrati.VID\_XXXX&PID\_YYYY;**
- **Bloccare il pc quando ci si allontana;**
- **Blocchi fisici porte USB: usare port blocker ;**



# Grazie

Th3Pr0f