Taller de implantes físicos en red team

Emmanuel Seoane

Diego Bruno

Javier Antunez

Hola!

Soy Emmanuel

Trabajo en desarrollo de software.

Muchos me conocen como DSR! De indetectables

Me gusta el hardware hacking

Hola!

Soy Diego

Trabajo entre otros temas planificando y ejecutando ejercicios de Red Team.

Instructor en Hackademy y EKO Trainings

You can find me at @Blackmantisec

Hola!

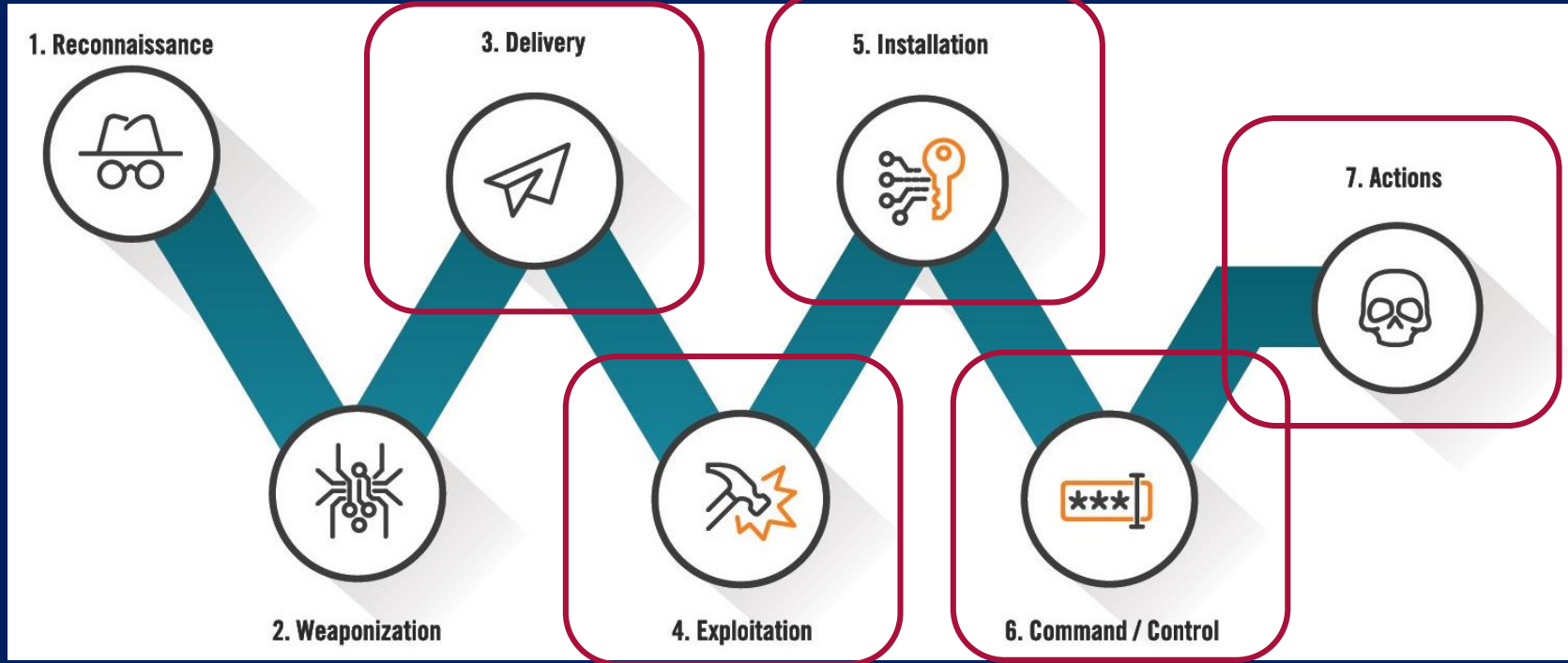
Soy Javier

Trabajo entre otros temas planificando y ejecutando ejercicios de Red Team.

Instructor en Hackademy y EKO Trainings

You can find me at @javierantunez

Cyber Kill Chain



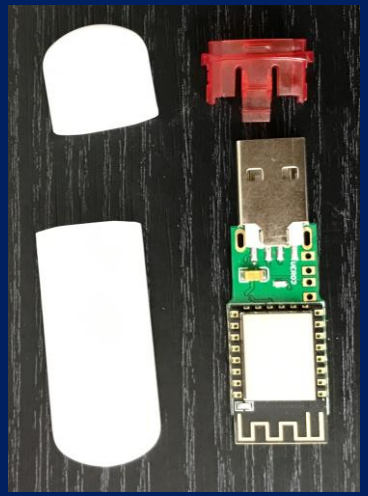
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Compromiso inicial

- Puede darse por diferentes vías:
  - Acceso físico (ej: Clonado/emulación de tarjetas de control de acceso –ej_ Proxmark, Flipper zero, Hunter Cat NFC-)

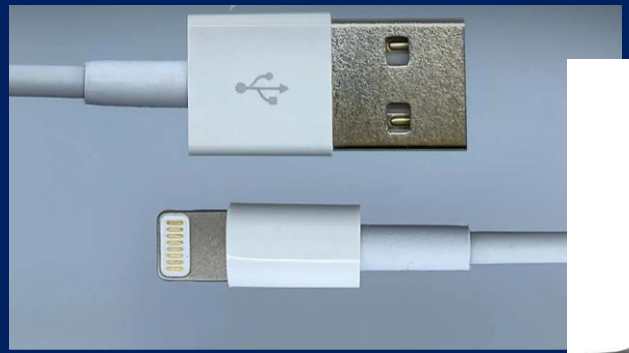
Compromiso inicial

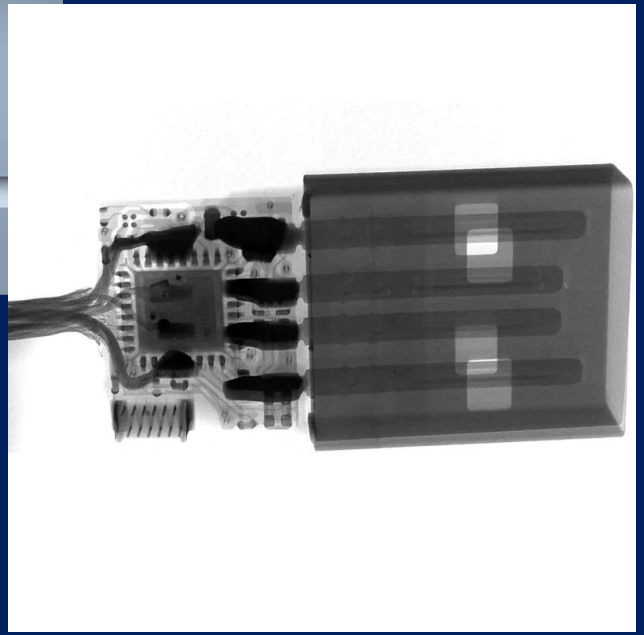
- Acceso físico a estaciones de trabajo
- Implantación de hardware (ej: WHID, WHID Elite, rubber ducky, pwnpi, etc).



Compromiso inicial

- Ocultandose a plena vista





Compromiso inicial

- Ataques de redes inalámbricas (Rogue APs, Evil Twin, etc)

Persistencia/C&C en el target

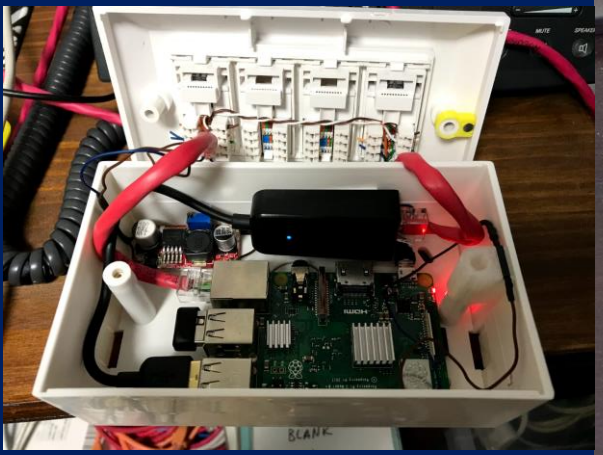
- Nos permite retomar el acceso sin volver a ingresar físicamente (ej: Wifi Pineapple, Raspberry Pi+4G, bashbunny, Lan turtle)

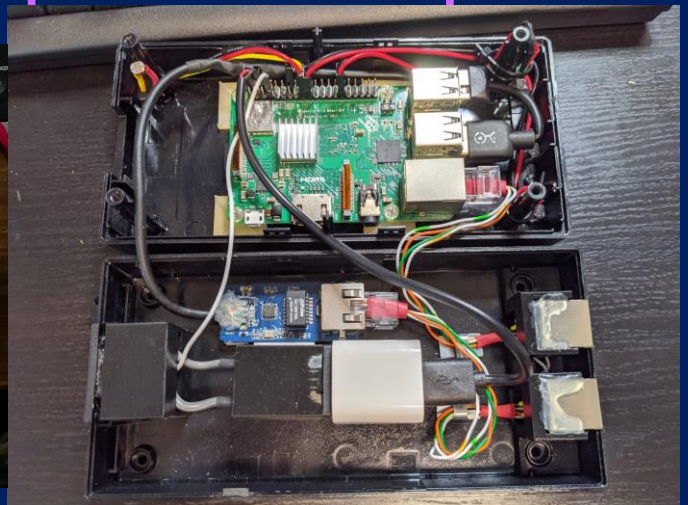
Persistencia/C&C en el target

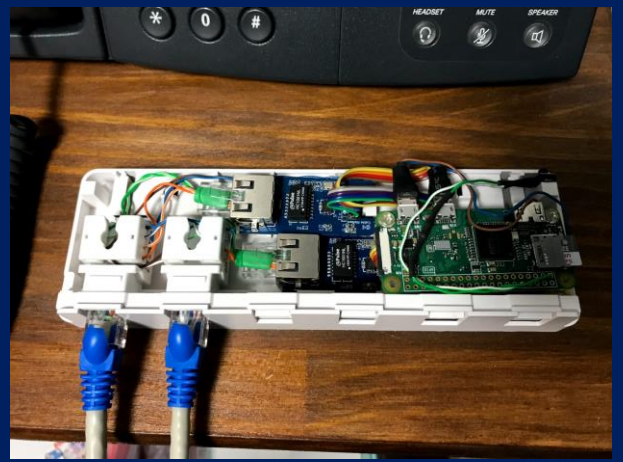
- Para no perder el acceso una vez logrado el ingreso físico a instalaciones del target.
- Buscamos pasar desapercibidos:

Persistencia/C&C en el target

- Para no perder el acceso una vez logrado el ingreso físico a instalaciones del target.
- Buscamos pasar desapercibidos:



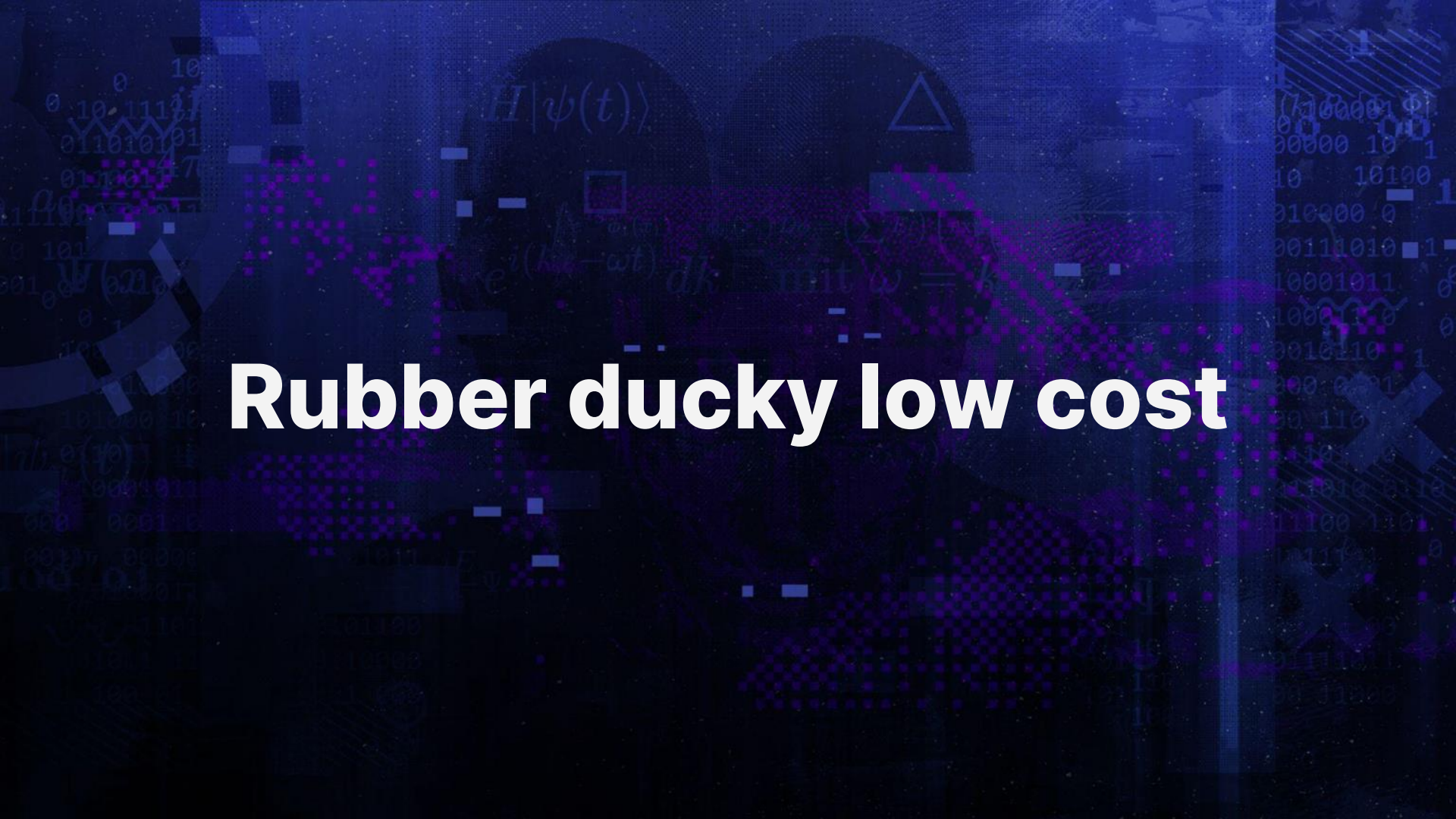




Pineapple

TERMIDOR

https://github.com/xchwarze/wifi-pineapple-cloner


Rubber ducky low cost

Requerimientos

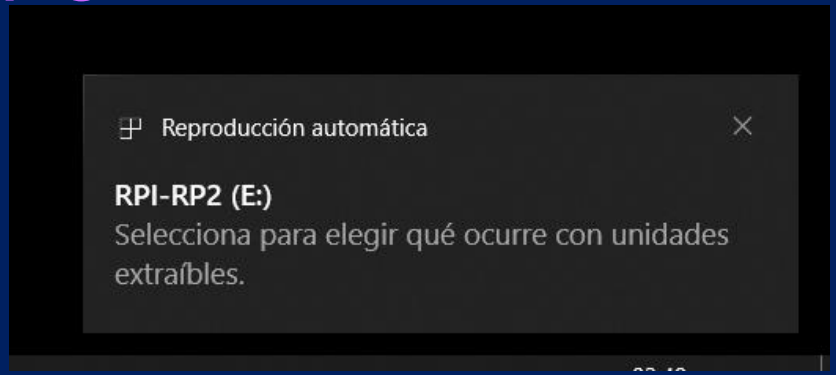
- Raspberry Pi pico (RPI2040)
- Cable micro USB
- Algunas descargas (a continuación)

Requerimientos

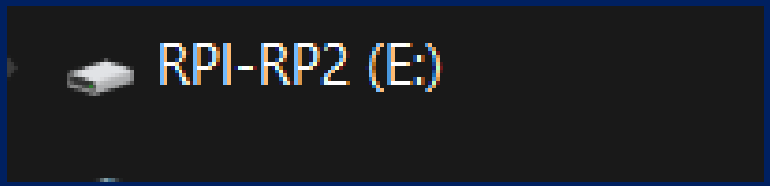
- https://github.com/dbisu/pico-ducky/releases/download/v1.4/pico-ducky-v1.4_win_es.zip

Procedimiento

- Conectar la raspi a la PC



- Se detectara como medio de almacenamiento



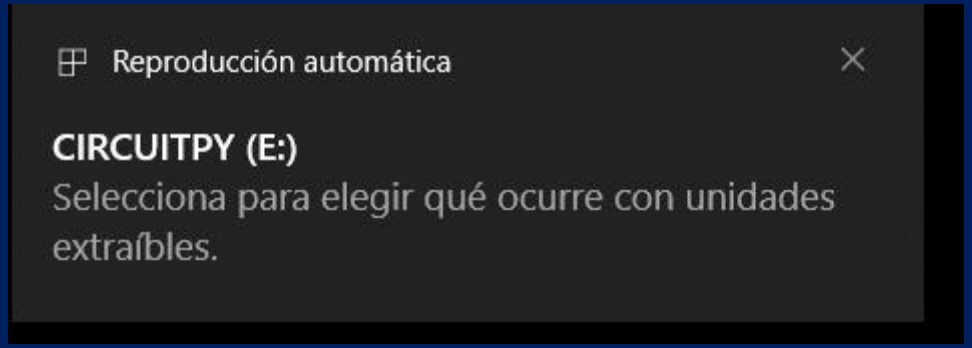
Procedimiento

- Descomprimir el ZIP descargado
- Copiar el archivo de circuit Python * al raíz de la unidad nueva.

adafruit-circuitpython-raspberry_pi_pico-es-7.3.2.uf2

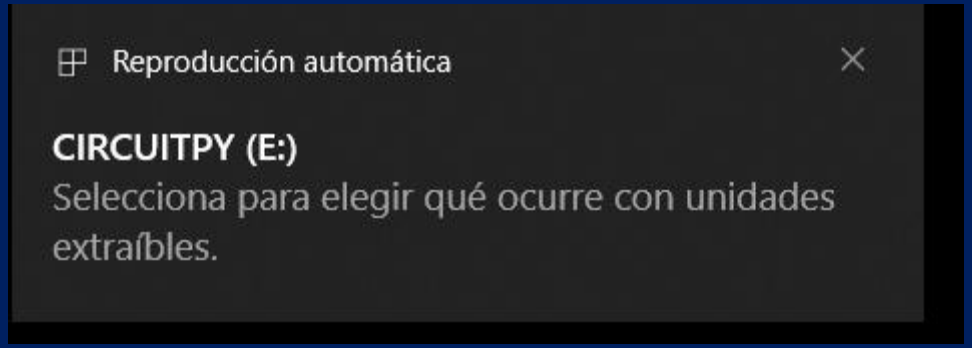
Procedimiento

- La raspi se va a rebootear inmediatamente y arracara con un Nuevo nombre



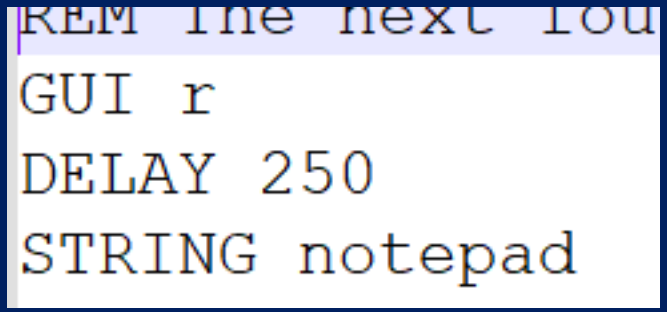
Procedimiento

- La raspi se va a rebootear inmediatamente y arracara con un Nuevo nombre



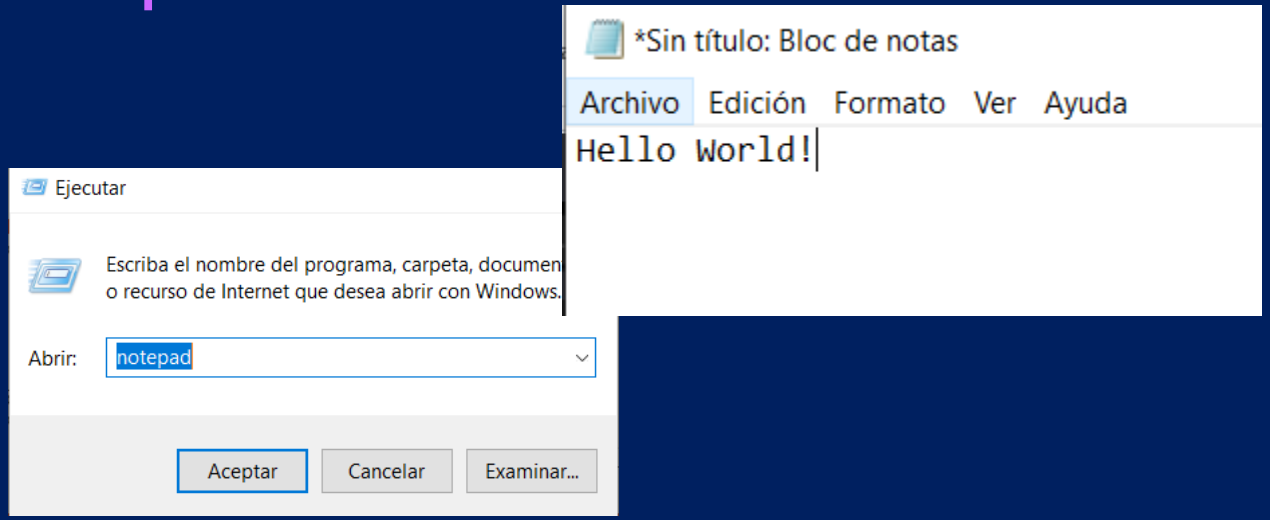
Procedimiento

- Copiar la carpeta lib del zip al raiz de la raspi
- Copiar code.py del zip al raiz de la raspi
- Modificar payload.dd y agregar el siguiente texto “DELAY 250” luego de “GUI r” y antes de la palabra “notepad”
- Salvar los cambios



Procedimiento

- Copiar la payload.dd modificado al raiz de la raspi

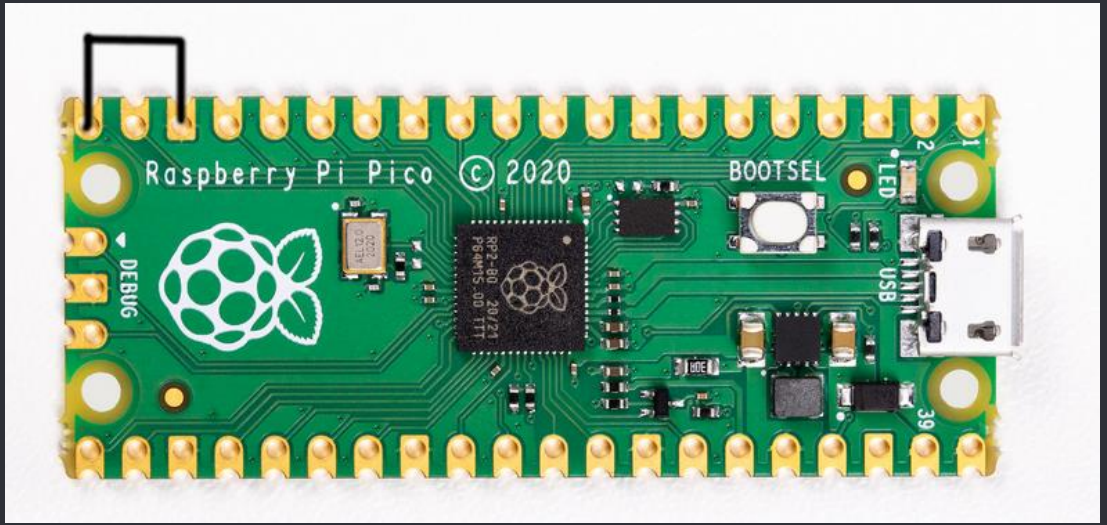


Procedimiento

- Para evitar que se ejecute el payload para reconfigurar puentear (Pin 1 y 3)

Procedimiento

- Modo stealth
- No muestra el almacenamiento (jump pines 18 y 20)



Payloads variados para arrancar

- https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads

Ducky script reference

- https://docs.hak5.org/hak5-usb-rubber-ducky/ducky-script-quick-reference

EKOPARTY

THANKS! GRACIAS!

@EKOZONAREDTEAM