SYNACKTIV

BadUSB forensic

PTS 2026 - RUMP

2026/07/01

BadUSB

SYNACKTIV

- **Evil fake USB devices**
  - Teensy, Rubber Ducky, WHID, Flipper Zero…
  - But also fake charging cable!

Fake charging cable

SYNACKTIV

Home / All Products / Red Team Tools / Evil Crow Tools / Evil Crow Cable Pro (USB C) – Professional Bad USB Device

Evil Crow Cable Pro (USB C) – Professional Bad USB Device

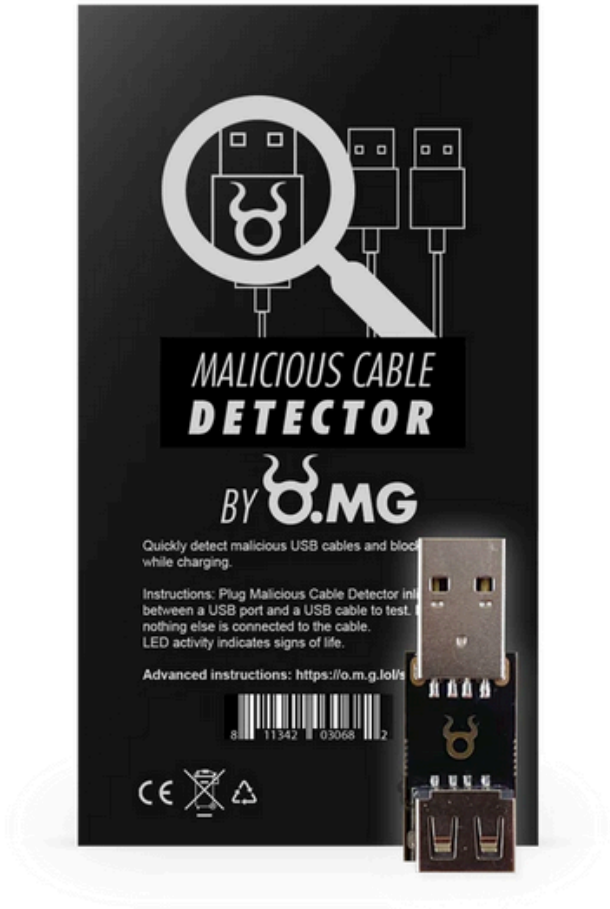
€39,74

★ Purchase & earn 66 Points!

How to check if a cable is malicious?

SYNACKTIV

- **Comercial way**
  - https://lab401.com/fr/products/o-mg-malicious-cable-detector
  - ~ 80 €



How to check if a cable is malicious?

SYNACKTIV

- **Hardware needed**
  - (old) Raspberry Pi
  - One or two Wi-Fi dongles
  - Bluetooth dongle
  - USB power consumption (Doctor charger)
  - Optional: USB C to USB A adapter

How to check a suspicious cable?

SYNACKTIV

- **Power consumption**
- **USB communication**
  - DMESG
  - Wireshark
- **Wi-Fi detection**
- **BLE detection**

Power consumption

- Charger doctor

DMESG

SYNACKTIV

- Run `dmesg -W` and check message when the suspicious devices is plugged

```
[  341.809712] usb 1-4: new full-speed USB device number 16 using xhci_hcd
[  341.961033] usb 1-4: New USB device found, idVendor=239a, idProduct=cafe, bcdDevice= 1.00
[  341.961044] usb 1-4: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[  341.961049] usb 1-4: Product: Pico
[  341.961052] usb 1-4: Manufacturer: Raspberry Pi
[  341.961055] usb 1-4: SerialNumber: E6652862CB731E24
[  341.964088] cdc_acm 1-4:1.0: ttyACM0: USB ACM device
[  341.965740] input: Raspberry Pi Pico as /devices/pci0000:00/0000:00:14.0/usb1/1-4/1-4:1.2/0003:239A:CAFE.0007/input/input31
[  342.089995] hid-generic 0003:239A:CAFE.0007: input,hidraw0: USB HID v1.11 Keyboard [Raspberry Pi Pico] on usb-0000:00:14.0-4/input2
```

Wireshark & USBMon

SYNACKTIV

- Run wireshark and check traffic when the suspicious devices is plugged
  - `sudo modprobe usbmon` needed

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 1]
2	0.000022	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 1]
3	0.000029	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 2]
4	0.000037	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 2]
5	0.000040	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 3]
6	0.000047	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 3]
7	0.000050	host	1.1.0	USBHUB	64	CLEAR_FEATURE Request [Port 3: C_PORT_CONNECTION]
8	0.000057	1.1.0	host	USBHUB	64	CLEAR_FEATURE Response [Port 3: C_PORT_CONNECTION]
9	0.000061	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 4]
10	0.000068	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 4]
11	0.000071	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 5]
12	0.000080	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 5]
13	0.000083	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 6]
14	0.000091	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 6]
15	0.000097	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 7]
16	0.000104	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 7]
17	0.000107	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 8]
18	0.000114	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 8]
19	0.000117	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 9]
20	0.000126	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 9]
21	0.000129	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 10]
22	0.000137	1.1.0	host	USBHUB	68	GET_STATUS Response [Port 10]
23	0.000141	host	1.1.0	USBHUB	64	GET_STATUS Request [Port 11]

False positive

SYNACKTIV

- Using a USB Hub to plug the suspicious device

```
[   56.840677] usb 2-3: new SuperSpeed USB device number 2 using xhci_hcd
[   56.870231] usb 2-3: New USB device found, idVendor=05e3, idProduct=0626, bcdDevice= 6.63
[   56.870236] usb 2-3: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[   56.870237] usb 2-3: Product: USB3.1 Hub
[   56.870238] usb 2-3: Manufacturer: GenesysLogic
[   56.872494] hub 2-3:1.0: USB hub found
[   56.873373] hub 2-3:1.0: 4 ports detected
[   56.988569] usb 1-3: new high-speed USB device number 5 using xhci_hcd
[   57.139228] usb 1-3: New USB device found, idVendor=05e3, idProduct=0610, bcdDevice= 6.63
[   57.139232] usb 1-3: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[   57.139234] usb 1-3: Product: USB2.1 Hub
[   57.139235] usb 1-3: Manufacturer: GenesysLogic
[   57.140145] hub 1-3:1.0: USB hub found
[   57.140447] hub 1-3:1.0: 4 ports detected
```

False positive

SYNACKTIV

- Moving a wireless mouse for the first time

```
[  223.134756] logitech-hidpp-device 0003:046D:4008.0006: HID++ 2.0 device connected.
```

Wi-Fi

SYNACKTIV

- **Configure the interface to be in monitor mode**
  - `sudo airmon-ng start wlan0`
- **Start the monitoring**
  - `sudo airodump-ng --band abg -a -z wlan0mon`
    - `-a -z` hide associated/unassociated stations
- **Wait in order to detect the Wi-Fi noise**
- **Then plug the suspicious device**

Bluetooth

SYNACKTIV

- **Scan for Bluetooth using bleak**
  - `pip install bleak`
  - `sudo rfkill unblock bluetooth`
  - Scan for Bluetooth device before power on the suspicious device
  - Then power on, rescan and compare

```
import asyncio
from bleak import BleakScanner

async def main():
    print("Scanning 10s...\n")
    devices = await BleakScanner.discover(timeout=10)
    for d in devices:
        print(f"  {d.address}  {d.name or 'Unknown'}")

asyncio.run(main())
```

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://x.com/synacktiv

https://bsky.app/profile/synacktiv.com

https://synacktiv.com