En cybersécurité aussi, le savoir n'a de valeur que si il est partagé.

In Cybersecurity too, knowledge only increases in value once shared.

www.wocsa.org

Bad USB presentation

Disclaimer

Disclaimer

The following demonstration is for educational purposes only.

We do not promote or encourage illegal activities.

Knowing your enemy is a half-won battle

La connaissance n'est réellement profitable que lorsqu'elle est partagée

What is Bad USB?

- Like a normal USB key
- When plugged in, performs predefined action
- Can be the source of a compromise if not monitored closely
- PlugX malware was distributed in a campaign through badUSBs

Malduino, from Maltronics

Why does it work?

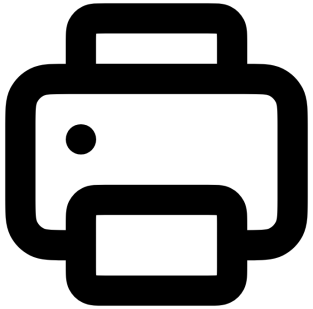
- Peripherals announce their type when connected
- The computer has no choice but to **trust** them

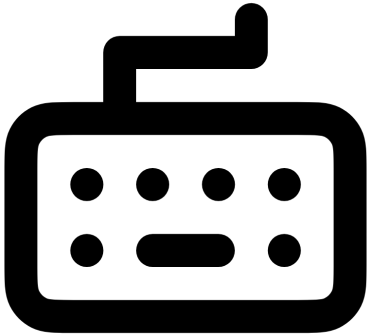
In cybersecurity, **hardware and the human factor** are the **MOST VULNERABLE** parts.

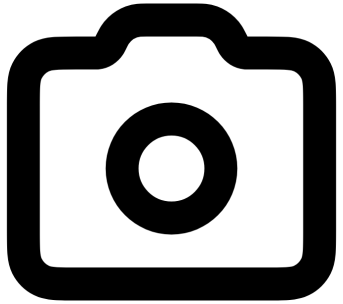
Combining them, a user plugging an USB key is a **deadly method**

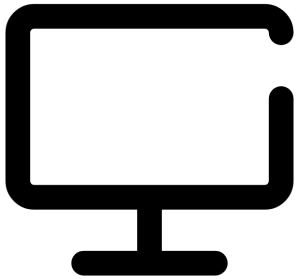
Rubber ducky

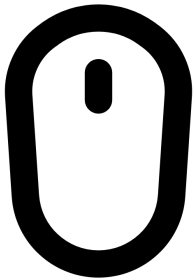
How it's being exploited





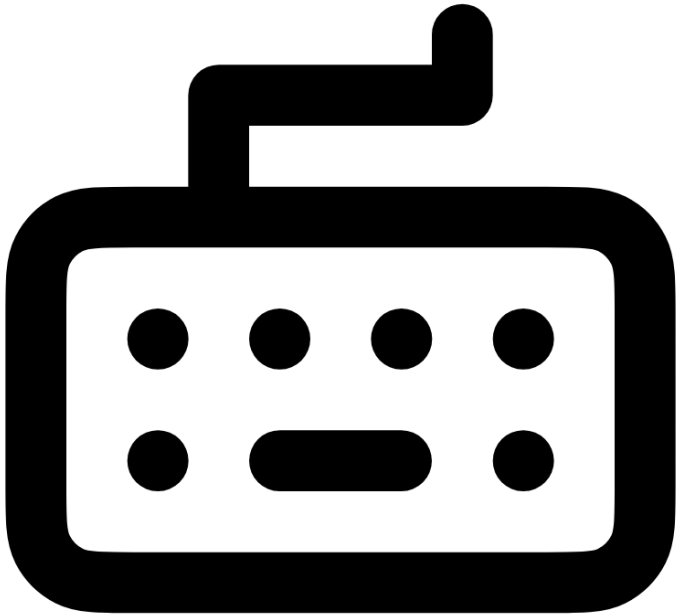






Which peripheral should the badUSB pretend to be?

How it's being exploited



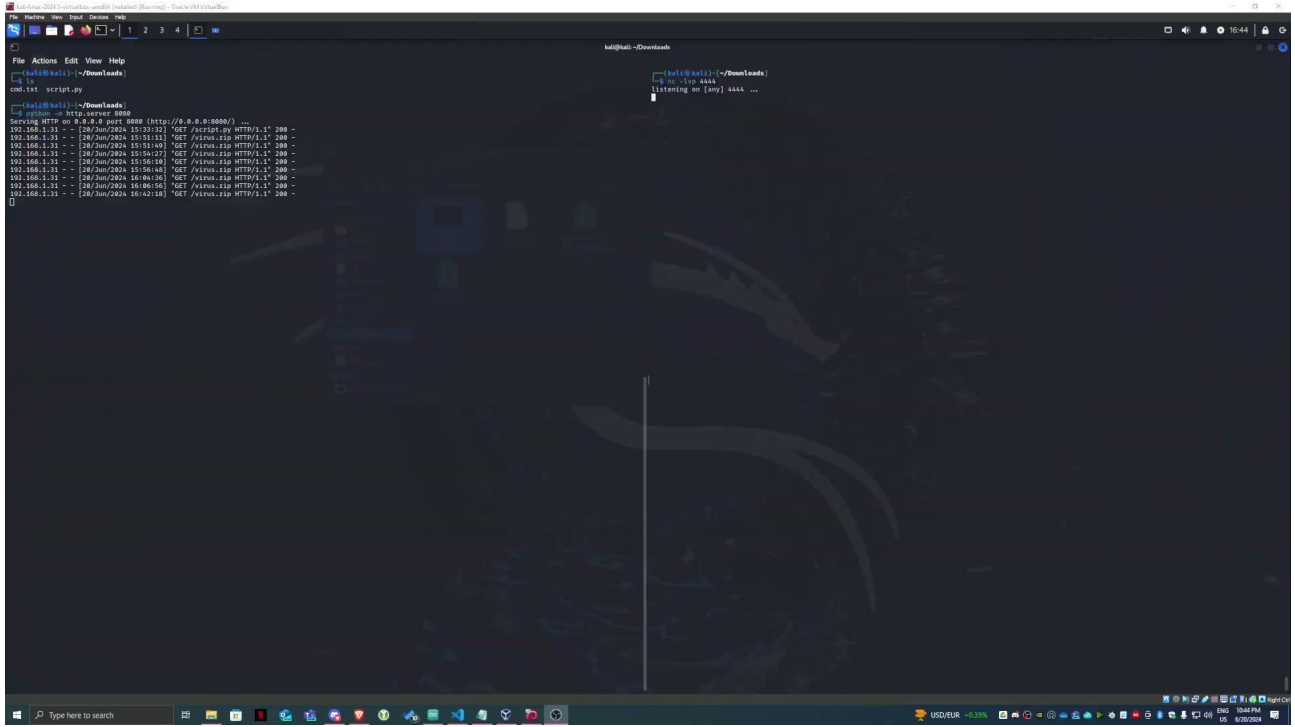
A keyboard enables it to send keystrokes to the computer!

The human factor

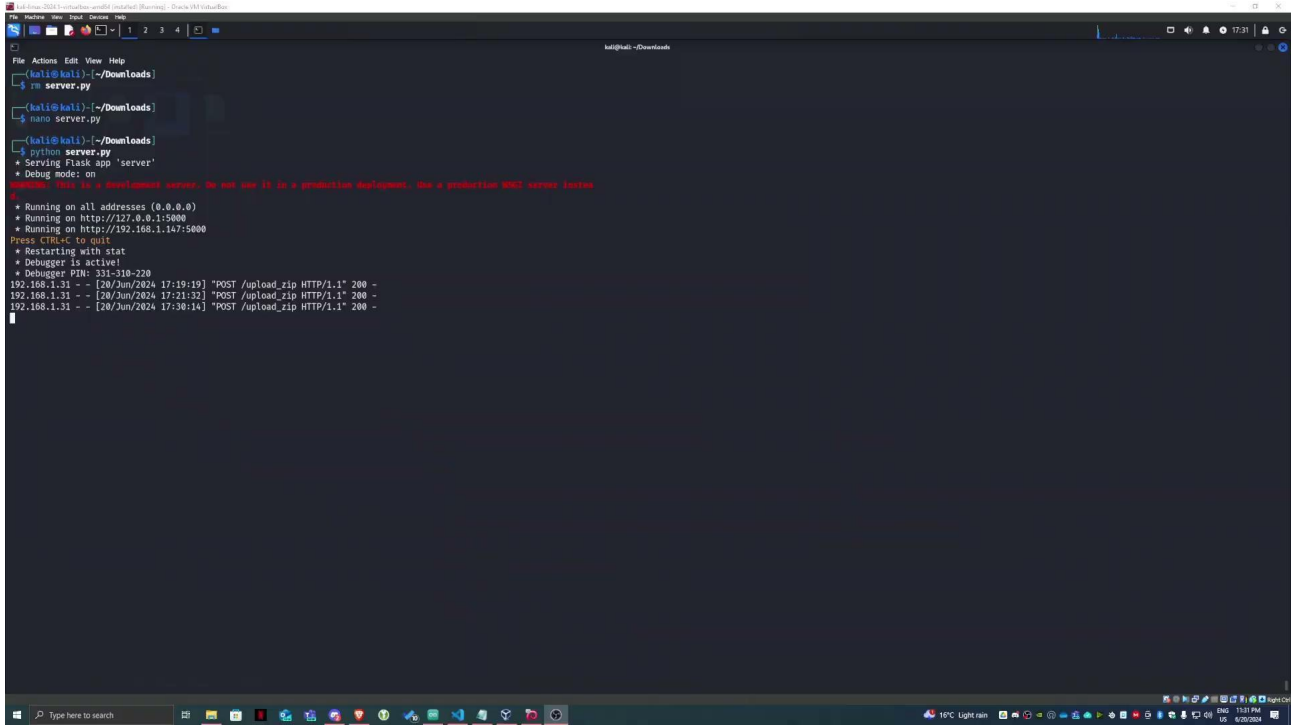
As this attack is hardware-based, a human needs to perform the attack, and another has to make a mistake

- The victim can leave the computer unlocked
- The attacker can perform social engineering to make the victim plug the computer

Example 1



Example 2



How to protect ourselves

- Never plug an untrusted USB key
- Lock your computer when you need to leave it for some time
- You can use an “USB condom” or plug untrusted devices on an isolated machine first to check its behavior

WOCSA

Join Us!

www.wocsa.org

contact@wocsa.org

@WOCSA-rx2mn

https://discord.gg/pDunje3tpb

@wocsa

@wocsa_asso

@wocsa

Join us to change the digital world: https://www.helloasso.com/associations/wocsa/adhesions/bulletin-d-adhesion-2

Please provide your feedback for our quality check process: https://www.wocsa.org/qcheck.php