clusil

USB Project

Experimental analysis of risks associated with USB keys

Table of Contents

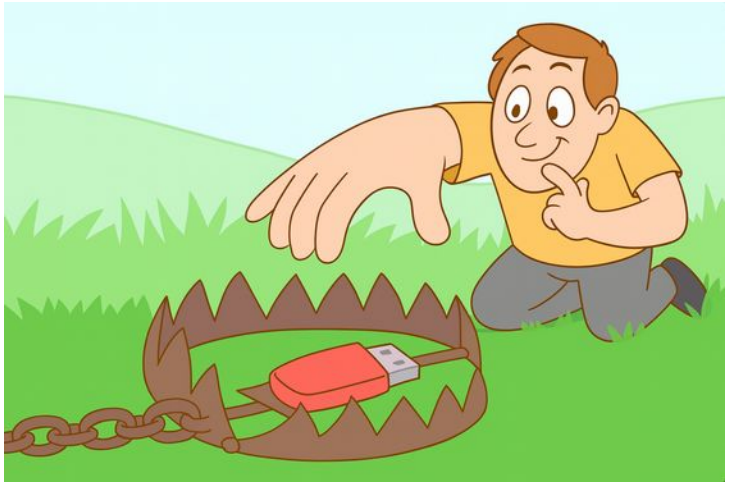
Project objectives

Testing in real-world conditions, human curiosity and behavior when faced with an unknown USB drive.

Measuring the risk posed by USB drives in 2025.

Raising awareness of the risks involved.

Improving community practices.



Universal Serial Bus

USB (Universal Serial Bus) was introduced in 1996 with USB 1.0.

When a USB device is inserted, the device provides the computer with:

- a Vendor ID (VID): the manufacturer's identifier
- a Product ID (PID): the product identifier
- a device class (e.g., Mass Storage, HID, Audio, etc.)

This information allows the operating system to identify which driver is needed.

Plug and Pray

The operating system

- Interprets USB descriptors.
- Searches for a corresponding driver:
  - either in its built-in driver database
  - or via an online database (e.g., Windows Update)

Manages:

- the detection of new hardware
- the VID/PID ↔ driver matching
- the automatic installation of the driver on the workstation

Identification – a security issue

The USB port isn't just for USB keys.

A USB device can be used as:

- a keyboard
- a mouse
- a Wi-Fi access point
- a virtual network adapter

The associated risks

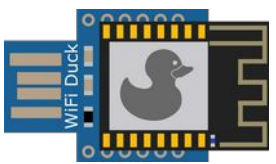
Associated risks:

- Execution of system commands without user interaction
- Creation of stealthy access points or network tunnels
- Propagation of malware without leaving identifiable files
- Bypassing security policies (e.g., proxy, antivirus)

USB Rubber Ducky

USB Killer

USB NOVA



WiFi Duck

The associated risks

I found this USB key, let's see what's on it!

Table of Contents

Precautions taken

Project verification with CERT.lu

Inform the Luxembourg CERTs

No malware on the USB drives

A “hidden” message on the USB drive refers to this project

No USB keys were harmed during this experiment.

Preparing the keys

Burning USB drives with a script:

- detect drive insertion
- format the drive
- copy the files
- put the unique hash in the file
- unmount the drive

=> 3 invalid drives out of 300

Key contents

- Seemingly harmless files (e.g., PowerPoint karaoke, documents, videos, images...)
- Technological artifact to track file openings (disclaimer.html)
  - Connection tracking via a web server
- Limitations:
- No tracking for key insertions without content viewing
- Only one file on the key contains the tracker: "Disclaimer.html"

Key operation

Technological artifact:

An HTML file (DISCLAIMER.html) with a URL to the USB project website containing a hash of the key's ID.

https://www.usbproject.lu/blank.png?ID=<<hash>>

This method will not be detected as a threat by security equipment.

Key operation

"Please insert this USB drive into your computer and open the DISCLAIMER.html file."

Key customization

A previous study showed that the appearance of keys does not significantly influence user interest.

We opted for **red** keys

Reference studies

Experiment 1 conducted in 2015	Experiment 2 conducted in 2015
Cyber Secure: A look at Employee Cybersecurity Habits in the Workplace	**Users Really Do Plug in USB Drives They Find**
200 anonymous USB drives were placed in public locations in business districts (airports, cafes, squares, etc.) across various US states. These drives contained text files prompting anyone who plugged them in to send an email to a specific address or click on a traceable link. Study results: 17% of the drives responded.	Researchers at the University of Illinois placed 297 keys on the university campus. The study's results showed that 98% of the keys were retrieved and 45% were accessed. Furthermore, the median access time was 6.9 hours.

Green IT

What is the environmental impact of a security risk?

- 300 USB drives: ≈ 1.8 kg of plastic + electronic components
- Manufacturing: ~70 g CO_2e per drive
- Transport & packaging: ~20 g CO_2e
- Estimated total: ~27 kg CO_2e for the entire experiment

- On the other hand: preventing just one security incident means…

Confidentiality of thousands of sensitive data points preserved

Cost avoidance: remediation, fines, loss of trust

Distribution and Instructions

Number of keys distributed: 240 USB keys.

Disposal locations: public spaces, public transportation, business centers, parks, tech events, etc.

Distribution throughout Luxembourg, taking into account the population density of each canton.

Period: May 1 to August 15, 2025.

Instructions: act discreetly and carry your mission letter with you.

Table of Contents

First contact

A student emailed us because he found one of our keys:

À **info**

Bonjour,

Je vous écris simplement pour vous signaler que j'ai trouvé l'une de vos clés USB près du Bistrot V'diterraneo à Belval.

En tant qu'étudiant passionné par la cybersécurité, j'ai trouvé l'idée brillante. C'est exactement le genre d'approche qu'il faut pour sensibiliser efficacement ;)

Dois-je la remettre à son endroit initial, ou la conserver/supprimer selon vos instructions ?

Merci pour ce projet, et bravo pour l'exécution !

Bien à vous,

The SOC gets involved

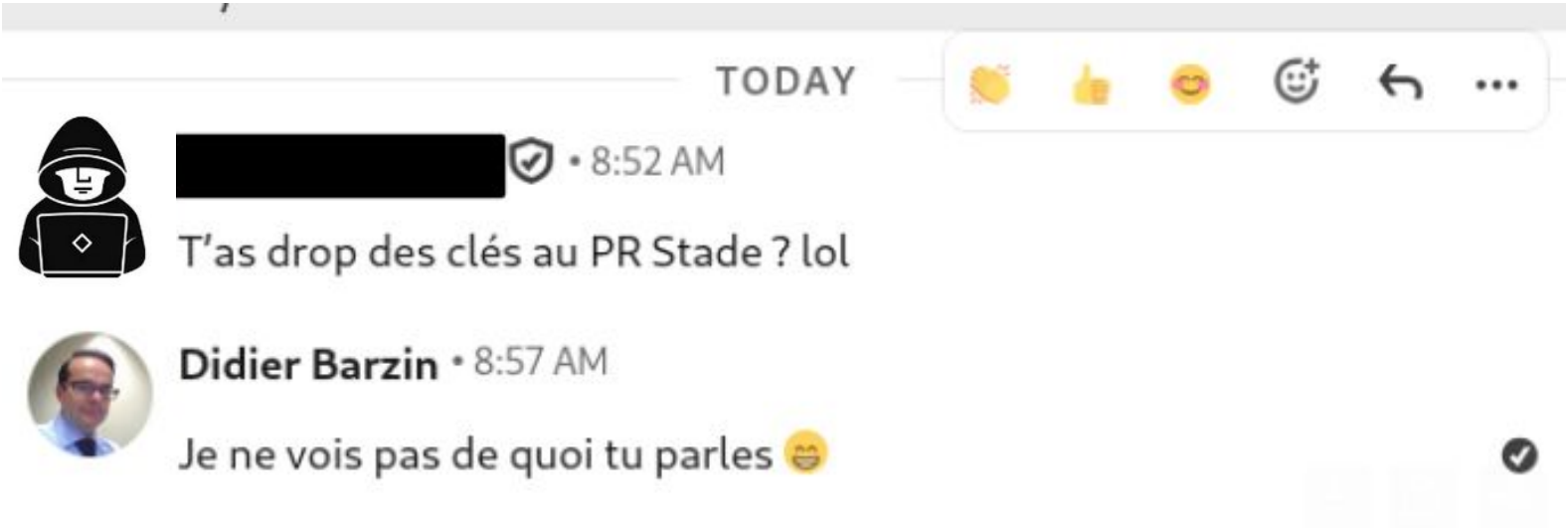
When a SOC Analyst discovers a USB key upon returning home.

He sends a text message to his boss

and opens the key to check what it contains.

Feedback from experience

Always denying it, even in the face of evidence:



Any resemblance to real persons is purely coincidental.

Crisis management

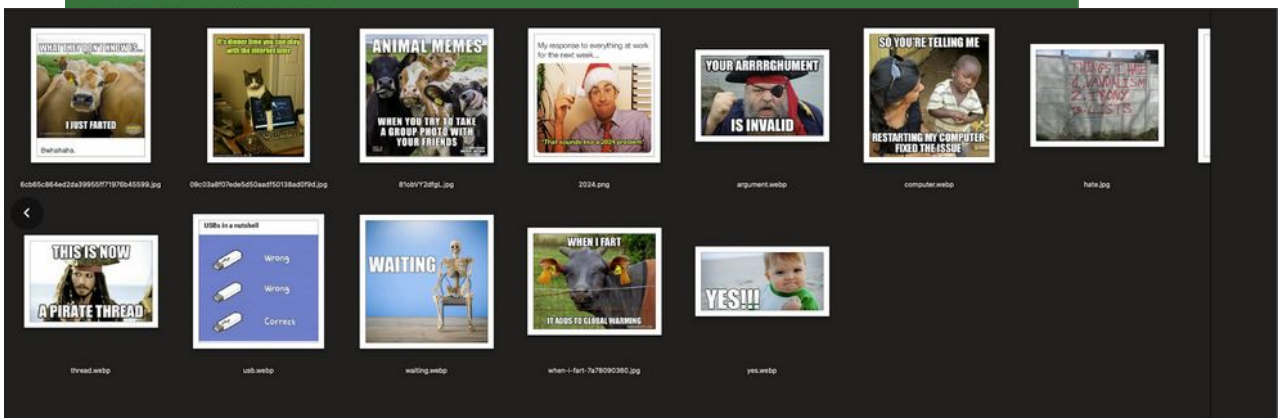
- *We were not discreet enough… and this triggered a crisis within an organization, with a forensic analysis as a result.*

```
<!--
This USB drive is part of a cybersecurity awareness project supported by the CLUSIL
(Club de la Sécurité de l'Information — Luxembourg).

Its content is intentionally crafted for research and educational purposes and does not contain any malicious code.
If you have discovered this file as part of a security check, digital forensics operation, or by sheer curiosity:

👉 Please report the detection or analysis of this USB device to the project team at:
info@usbproject.lu

No personal data is collected and no individuals or organizations are targeted.
```



Crisis management

Here are their actions:

1. The Facilities Management department located four USB drives […].
2. An emergency meeting was held […].
3. An official communication was sent […].
4. A follow-up announcement was posted on the intranet.
5. The contents of the USB drives were copied to a dedicated SSD to back up all digital assets. This was done by mounting the devices in a controlled and secure environment to prevent the execution of potentially malicious files.
6. The SSD and USB drives were placed in a secure safe.
7. We contacted you after noticing an HTML warning on one of the devices.

These actions were taken in approximately 45 minutes.

We are contacted by a CERT

À **info**

Hello,

We received a mail signaling the finding of one of your usbkey. The purpose of the mail is to forward the alert.

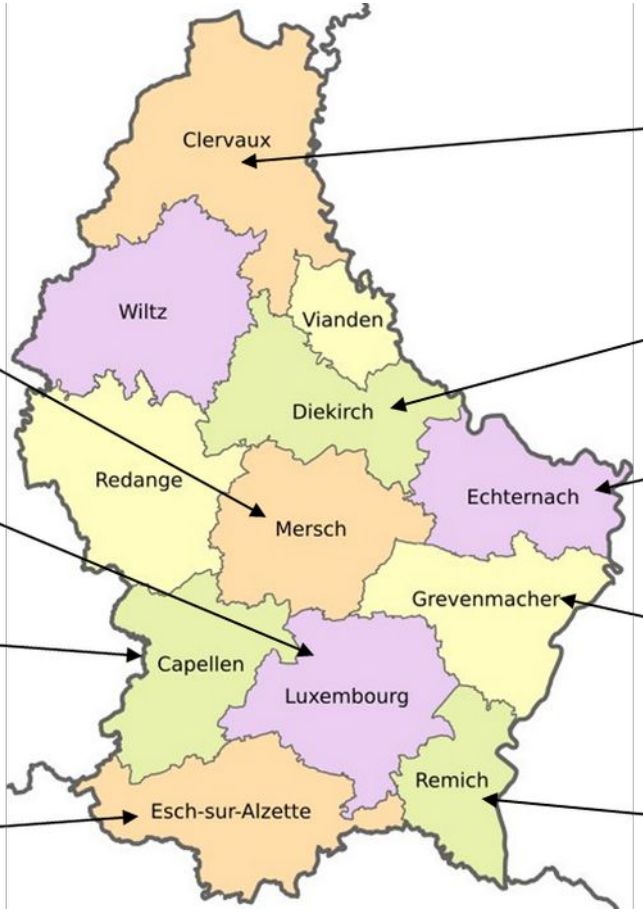
At this stage, we simply acked the message saying we will document on our side, with some further basic recommendation as a closing sentence. But, we were not sure how much we could communicate with the reporter of the usbkey finding (that conducted apparently a proper analysis) !

Best regards,

Table of Contents

Geographical coverage

Keys dropped	Nb	%
Keys taken	Nb	%



1	2.6 %
5 1	2 % 2.6 %
128 17	53.3 % 43.5 %
11 0	4.6 % 0 %
64 13	26.7 % 33.3 %

1.3 % 2.6 %	3 1
2 % 2.6 %	5 1
2.9 % 5.2 %	7 2
3 % 5.2 %	7 2
4.2 % 2.6 %	10 1

Location coverage

Nb Hits / key	Nb Keys taken	Location
1	18	17 standard + 1 unkown
2	8	8 standard
3	5	5 standard
4	3	2 school + 1 standard
5	3	1 school + 1 standard
8	1	1 school
9	1	1 school

School place – keys dropped	School place – keys taken
16	5

Analysis

- 16% of victims! Of the 240 keys dropped, 39 were taken. This result is consistent with Study 1, which reported a recovery rate of 17% for 200 dropped keys.
- A higher hit rate and a greater number of taken keys (31%) were observed for keys dropped near schools. This result is consistent with Study 2.
- The time between the drop and the hit varies from 30 minutes to 133 days, with a median to 3 days.
- 8 keys were consulted on the day they have been dropped.

Analysis

- Only 16% of the keys were taken, why?
  - The key was either not inserted or connected to a device without internet access,
  - The DISCLAIMER.html file was not viewed,
  - The key was destroyed or analyzed by a SOC team.
- People's motivation?
  - Study 1 concluded that altruism and curiosity were the reasons,
  - Given the significant delays in viewing the keys, the most likely reason in our study would be curiosity.

Hypothesis

We put forward only hypothesis due to the constraints of the experiment,

- At least 16% of people seem willing to take risk only for curiosity,
- Today people are more exposed to cyber risks and the media report even more on exploits, this experience suggest it seems to have no real improvement in people’s behaviour in 10 years,
- Are young people more vulnerable to cyber risks?

Table of Contents

USB key security

Behind the apparent simplicity of a USB drive lie real dangers.

The risks include:

- Identity or data theft,
- Virus transmission.

Nowadays data is a valuable asset,

protecting it from threats remains a priority.

Advices

- In modern organisations :
  - USB attacks must be considered in risk assessments,
  - Security measures must be implemented,
  - Crisis management
  - Plans must be in place and
  - Users awareness must be enhanced.

clusil

Questions ?