

# OSINT

## Beware your data is out there

Open Identity Summit 2024 - 20/06/2024



# \$whoami

- ▶ Pedro Vieira
- ▶ Cyber Security Engineer
- ▶ Certified Ethical Hacker
- ▶ Degree at University of Minho



# Disclaimer & Laws

# Disclaimer

## Boring but necessary

- ▶ Information in this presentation is intended for educational and awareness purposes only.
- ▶ **Live presentation.** Not a controlled environment and some contents may be inappropriate for some users.
- ▶ **I accept no responsibility** in any kind for the use, misuse, downloading, viewing in whatever way the links in this presentation.
- ▶ This presentation is **not related** to my work or employer.



# Disclaimer

## Avoid illegal activities

- ▶ Some links, websites, software or other items listed may or **may not be legal**, illegal, a felony, misdemeanor, or worse, in your country.
- ▶ Please make sure that you are **allowed** to browse the websites, download links and software **BEFORE USING!**
- ▶ Ignorance about laws or rules is **no excuse** for illegal activities or wrongdoing.
- ▶ Illegal activities may get you in **trouble or arrested**.
- ▶ Always check what is legal, and what laws apply.



# Laws

## Portuguese Law and Organizations

### ► Laws

- Diário República Eletrónico ([link](#))
- ANACOM ([link](#))

### ► Organizations

- CNCS - Centro Nacional de Cibersegurança ([link](#))
  - Incident Notification ([link](#))
  - CERT.PT ([link](#))
- Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) ([link](#))
- Ministério Público ([link](#))

# Awareness

# Awareness

## Internet knows and doesn't forget

- ▶ Posted information privately can get publicly and world available by someone else
- ▶ When information is posted
  - ▶ Shows when and where (habits & routines)
- ▶ Internet has memory
  - ▶ Arquivo.pt ([link](#))
    - ▶ Example ([link](#)) ➡
  - ▶ Internet Archive - Wayback Machine ([link](#))
    - ▶ Example ([link](#)) ➡



# Awareness Profile

- ▶ Mobile number (Same number longevity)
  - ▶ Sync.Me ([link](#))
- ▶ Username
  - ▶ WhatsMyName ([link](#)) ➡
- ▶ Email (Username reuse)
  - ▶ Gmail ([link](#))
- ▶ Social media (Username reuse)
  - ▶ Facebook ([link](#))
  - ▶ LinkedIn ([link](#))
  - ▶ Tinder ([link](#)) ([link](#)) ➡

# Awareness Maps

- ▶ Never been there. Know it like the back of my hand.
- ▶ Street view
  - ▶ Google Street View ([link](#)) ➡
- ▶ Map/ Satellite view
  - ▶ Google Maps ([link](#))
  - ▶ Overpass Turbo ([link](#)) ➡
    - ▶ Wizard: plant:source=nuclear
  - ▶ World Imagery Wayback example ([link](#)) ➡
- ▶ Tips, Tricks and Techniques ([link](#))

# Awareness Photos

- ▶ Photo analysis
  - ▶ Location
  - ▶ Date it was taken
  - ▶ Identifying elements in the photo
- ▶ Image search
  - ▶ Identify the castle ([link](#)) ➡



# Awareness Photos

- ▶ A picture is worth a thousand words.

- ▶ File analysis

- ▶ Metadata
- ▶ GPS ([link](#)) →
- ▶ Google Maps ([link](#)) →


- ▶ Tools

- ▶ CleanUp ([link](#))
- ▶ AperiSolve ([link](#)) →

**exifdata**

**SUMMARY**  
**DETAILED**  
**LOCATION**  
**UPLOAD**

IMG\_20190223\_163027.jpg



(click for original)

**Camera**  
Xiaomi Redmi 3

**GPS Position**  
40.989952 degrees N, 7.395051 degrees W

**Date of Creation**  
2019:02:23 16:30:27

**Resolution**  
4160x3120

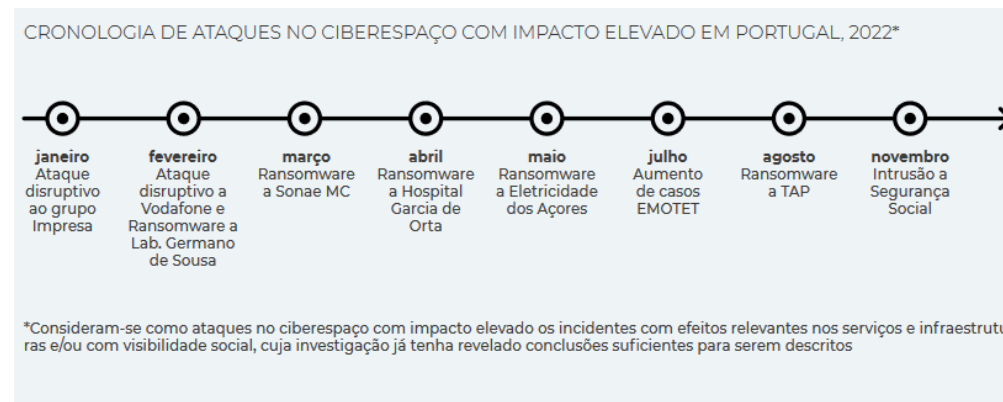
**SUMMARY**

Make	Xiaomi
Model	Redmi 3
Aperture	2
Exposure Time	1 / 1506 (0.00066401062416999 sec)
Focal Length	4.2 mm
Flash	Auto, Did not fire
File Size	1447 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	4160
Image Height	3120
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	72
Y Resolution	72
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
YCbCr Positioning	Centered
Exposure Program	Not Defined
Date and Time (Original)	2019:02:23 16:30:27
Metering Mode	Center-weighted average
Color Space	sRGB
Exposure Index	140
Sensing Method	Unknown (0)
Exposure Mode	Auto
Focal Length In 35 mm	0 mm
Format	
Scene Capture Type	Standard
Gain Control	Low gain up
ISO	100
Compression	JPEG (old-style)

# Awareness

## When companies are hacked

- ▶ When companies are hacked, private data is exposed. Private data becomes “public”.
- ▶ Troy Hunt
  - ▶ HavelBeenPwned ([link](#)) ➡
  - ▶ Pwned websites ([link](#)) ➡
  - ▶ Domain search ([link](#))
- ▶ CNCS Report
  - ▶ Cybersecurity in Portugal 2024 ([link](#))
  - ▶ Cybersecurity in Portugal 2023 ([link](#))



Fonte: CNCS

# Awareness

## IOT Search engines

- ▶ Shared folders accessible to 8 thousand million people ([link](#)) →

- ▶ Contabilidade - 6
- ▶ Clientes - 3
- ▶ Faturacao - 1
- ▶ Faturacao - 2
- ▶ Primavera - 6
- ▶ SAGE - 13
- ▶ Winrest - 148

Shares			Shares		
Name	Type	Comments	Name	Type	Comments
Web	Shares		ADMIN\$	Disk	Remote Admin
Public	Name	Type	C\$	Disk	Default Share
homes			IPC\$	Printer	
SCAN	Multimedia		Printer	IPC	
SERVER	Download	Shares			
Multimedia	Web	Name			
Recordings	Public				
home	homes	Multimedia			
MBPT	TESTE	Download			
PLOUTOS	JOAO	Web			
TGS	DUDA	Public			
MIRUS	SEGMENTO_POPULAR	homes			
USB	SOFTWARE	BackupR			
IPC\$	home	IPC\$			
	IPC\$				

Shares		
Name	Type	Comments
IPC\$	IPC	IPC Service ("")
Carlos	Disk	Carlos Pessoal
TTT	Disk	Todo Tipo Terre
SAIG	Disk	SAIG
Zonesoft	Disk	Clientes Zoneso
FTP	Disk	FTP
Clientes_Sage	Disk	Clientes Sage
Clientes_XD	Disk	Clientes XD
XD Extreme	Disk	XD Extreme
video	Disk	System default
photo	Disk	System default
music	Disk	System default
admin	Disk	...

# OSINT Time

“Information is not knowledge”

Albert Einstein



# OSINT - Open-source intelligence

## Digital Footprint

- ▶ Open-source intelligence (OSINT) is the collection and analysis of data gathered from open sources (overt and publicly available sources) to produce actionable intelligence. ([Wikipedia](#))
- ▶ Gathering information from:
  - ▶ search engines (Google, ...)
  - ▶ social media (Facebook, ...)
  - ▶ government sites
  - ▶ maps
  - ▶ ...
- ▶ And then extract/relate/infer new information with greater value/potential.



# Who Am I?

## Search, and then search again

- ▶ Starting with just a name
  - ▶ Pedro António Oliveira Vieira
- ▶ Google ([link](#)) ➡
- ▶ Google “Improved Search” ([link](#)) ➡
- ▶ Google “Improved Search” + Company ([link](#)) ➡
- ▶ LinkedIn ([link](#)) ➡
  - ▶ Public profile was showing way too much (audit is needed)
- ▶ Certified Ethical Hacker ([link](#))
- ▶ My github notes ([link](#))



# Search Engines

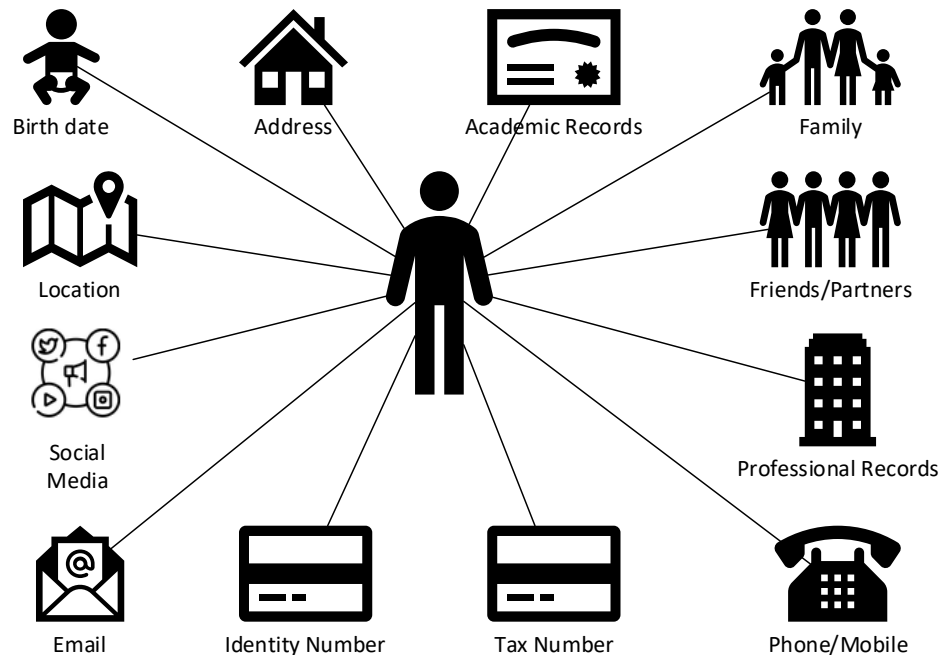
## Internet is more than Google

- ▶ Different search engine → different rules/crawlers → different results
- ▶ Google ([link](#))
- ▶ Bing ([link](#)) ➡
- ▶ Yahoo ([link](#))
- ▶ DuckDuckGo ([link](#)) ➡
- ▶ Baidu (China) ([link](#))
- ▶ Yandex (Russia) ([link](#))
- ▶ SAPO (Portugal) ([link](#)) ➡
- ▶ You may ask to be removed from one search engine, not all ☹ ([link](#))

# Who are YOU?

## Search, and then search again

- ▶ Search your name and analyze the results
  - ▶ As you saw the search can be improved



- ▶ That is typically information to **verify your identity** over a phone call.

# True stories

# True stories

## Portugal

### Store credit

- Buying a book for almost no money
- Customer Card
- Right intel: mobile number and full name
- Credito on card

### Customer data

- Invoice request with NIF
  - Name
  - Address
- Updating customer data at the counter without documents

# True stories

## Message from Ella | Without Consent



Deutsche Telekom  
Message from Ella | Without Consent

# THANK YOU

## Q&A

