

# OSINT

Beware. Your data is out there.

# 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](#))
- ▶ It's about digital footprint. Gathering information from:
  - ▶ search engines (Google, ...)
  - ▶ social media (Facebook, ...)
  - ▶ government sites
  - ▶ ...
- ▶ The constant battles:
  - ▶ Privacy vs Publicly available information
  - ▶ Convenience vs Security

# 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](#)) ➡

# OSINT GEO

# OSINT - Photos

## Lots of Information

- ▶ Where was this image taken?
  - ▶ Have you been there?
- ▶ When?
  - ▶ Date stamp on photo
  - ▶ Filename with date
  - ▶ Metadata
- ▶ What else?
- ▶ Image search
  - ▶ Identify the castle?






# OSINT - Photos Metadata

- Metadata
- GPS ([link](#)) ➡
- Google Maps ([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

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 Format	0 mm
Scene Capture Type	Standard
Gain Control	Low gain up
ISO	100
Compression	JPEG (old-style)

**SUMMARY**

# Search

## Geolocation

- ▶ Digital Cameras/Mobile Phones
  - ▶ Metadata
  - ▶ Geolocation
  - ▶ Camera Model
- ▶ Breasts lead to arrest of Anonymous hacker ([link](#)) ➡
  - ▶ Police allege that an Anonymous hacker posted a picture of his presumed girlfriend's breasts as a taunt to U.S authorities. The picture allegedly contained GPS information that led the FBI to her.
- ▶ Stolen goods being sold online can eventually be tracked

# OSINT

## (Reverse) Image search

- ▶ One image is worth 1000 words, maybe more.
  - ▶ What information can be extracted from a photo ?
- ▶ Google Images ([link](#))
- ▶ Bing Images ([link](#)) ➡
- ▶ Yahoo Images ([link](#))
- ▶ TinEye ([link](#))
- ▶ Yandex ([link](#))
- ▶ The professionals (video explaining) ([link](#))

# OSINT

## Street View

- ▶ Google Street View ([link](#))
  - ▶ Identify house by address
  - ▶ Assess security (cameras, fences, ...)
  - ▶ Parked cars (timeline, ...)
  - ▶ People's habits/routines, timetables, ...
- ▶ View the past – timeline ([link](#)) ➡
- ▶ Instant Street View ([link](#))

# OSINT Maps

- ▶ Google Maps ([link](#))
- ▶ Bing Maps ([link](#))
- ▶ Wikimapia ([link](#))
- ▶ Tips, Tricks and Techniques ([link](#))

# Search

## Satellite View

- ▶ Zoom Earth ([link](#))
- ▶ Satellites Pro ([link](#))
- ▶ World Imagery ([link](#))
  - ▶ Wayback ([link](#))
  - ▶ Wayback example ([link](#)) ➡
- ▶ View the past - timeline

# OSINT MEMORY

# Wayback Machine

## Internet in the past

- ▶ Wayback Machine ([link](#))
  - ▶ Example ([link](#)) ➡
- ▶ Archive.is ([link](#))
- ▶ Cached Pages ([link](#))
- ▶ Cached View ([link](#))
- ▶ OldWeb.Today ([link](#))
- ▶ Time Travel ([link](#))
  
- ▶ Github commits 😊



# OSINT IOT

# Shodan

## Search Engine for Internet Of Things

- ▶ Internet Exposure Observatory
  - ▶ Exposure Dashboard ([link](#))
- ▶ Explore
  - ▶ Shodan explore ([link](#))
- ▶ Images
  - ▶ Shodan images ([link](#))
- ▶ Maps
  - ▶ Shodan maps ([link](#))

# Shodan

## Internet of Things

- ▶ Remote Desktop ([link](#))
  - ▶ Total results: 3,482,756
  - ▶ Braga ([link](#)) ➡
- ▶ Images
  - ▶ Braga ([link](#))
  - ▶ VNC Remote Access and Loggedin ([link](#)) ➡
- ▶ Authentication Disabled
  - ▶ Portugal ([link](#)) ➡
  - ▶ Primavera ([link](#))
- ▶ Contabilidade ([link](#)) ➡

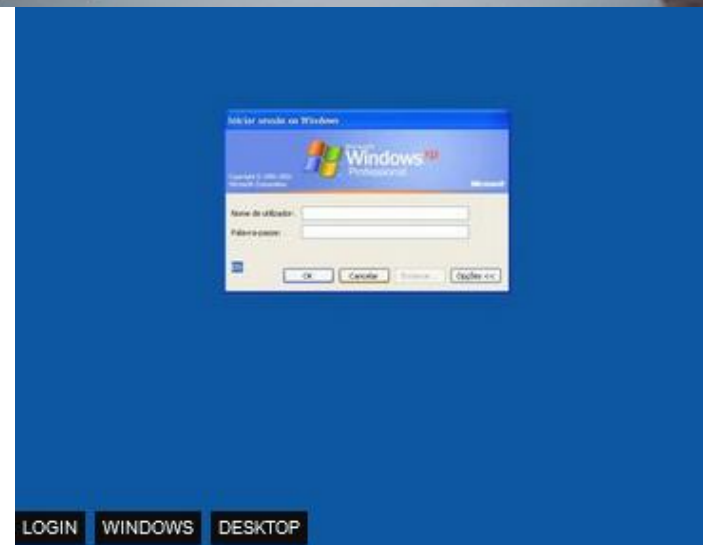
# Shodan

## Internet of Things

- ▶ Fotos
  - ▶ Portugal ([link](#)) ➡
- ▶ IP Cameras
  - ▶ Portugal ([link](#)) (default credentials?)
  - ▶ **Webcams** ([link](#)) ➡

# Shodan

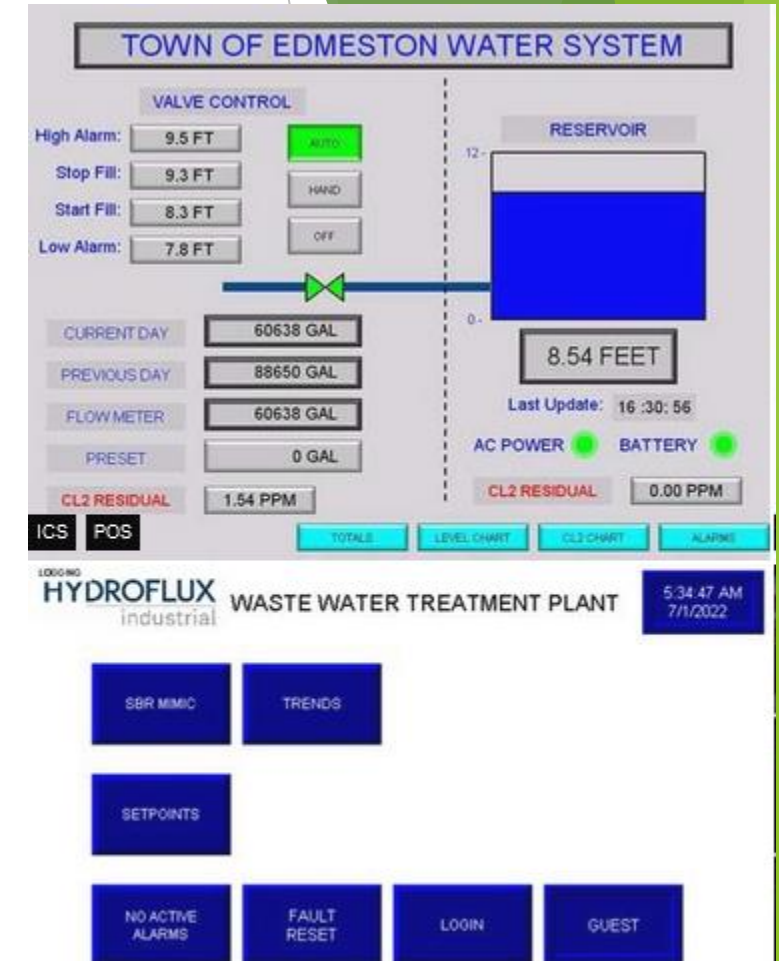
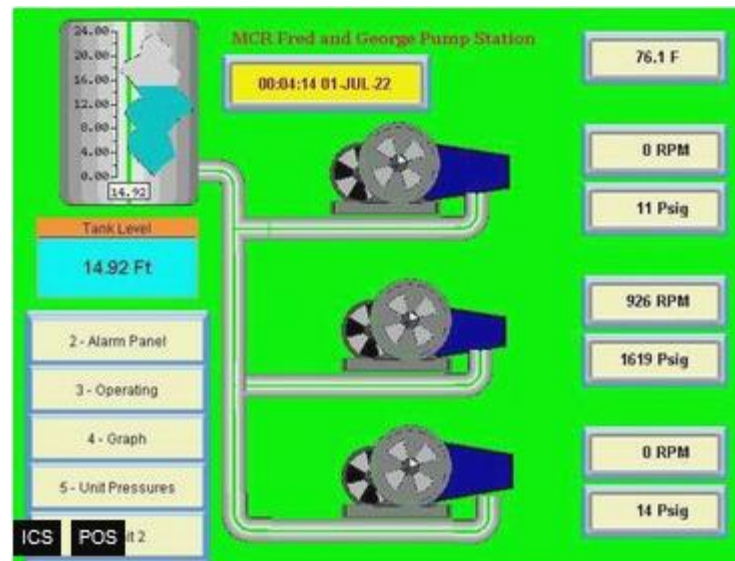
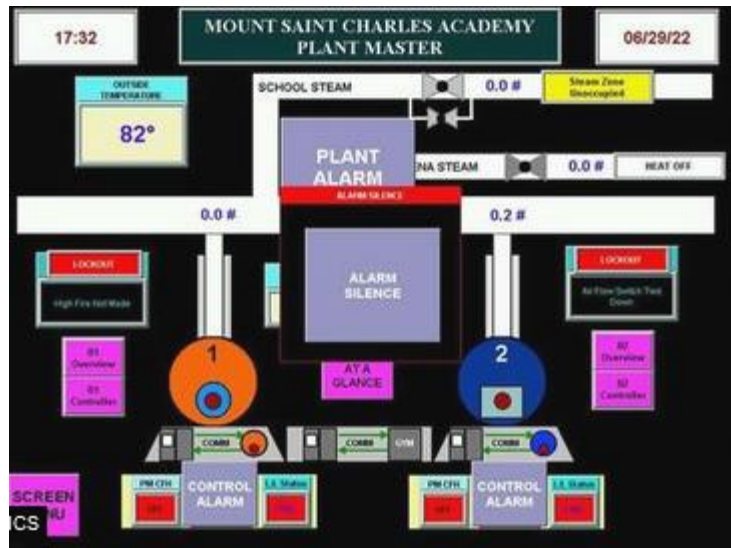
## Internet of Things - Images



# Shodan

## Industrial Control Systems

- Industrial Control Systems ([link](#))



# Shodan

## Portugal - Internet Exposure

- ▶ Internet Exposure Dashboard ([link](#))
- ▶ Top Vulnerability
  - ▶ CVE-2015-0204 – CVSS2 4.3 Medium ([link](#))
- ▶ BlueKeep Unpatched ([link](#))
  - ▶ 107 ([link](#))
- ▶ Industrial Control Systems
  - ▶ 516
- ▶ SMB (shared folders)
  - ▶ Authentication Disabled: 2898

# ONLINE SAFETY



# Helping Tools

## Privacy

- ▶ VPN (Different country, different advertisements, what else ?)
  - ▶ ProtonVPN ([link](#)) ➡
- ▶ Temporary Email (Need to register? Activate software?)
  - ▶ 10 minute email ([link](#)) ➡
  - ▶ 20 minute email ([link](#))
- ▶ Disposable Email
  - ▶ 60 minute email ([link](#))
- ▶ Internet Access (DarkWeb included)
  - ▶ Tor ([link](#)) (internet browser) ➡
  - ▶ Tails ([link](#)) (OS that runs on usb or VM) ➡

# Helping Tools Safety

- ▶ VirusTotal
  - ▶ Check received files ([link](#)) ➡
    - ▶ (**don't upload Personal or Company related information**)
- ▶ Netcraft
  - ▶ Sitereport ([link](#)) (check for suspicious sites)
- ▶ Ransomware
  - ▶ No More Ransom ([link](#)) ➡
- ▶ Virtual Credit Card (online shopping)
  - ▶ Mbnet ([link](#)) ➡
  - ▶ Revolut ([link](#))
  - ▶ PayPal ([link](#))

# Helping Tools

## Reverse Tracking

- ▶ Gmail Plus Address ([link](#)) example email: mypersonalemail@gmail.com
  - ▶ If you append a “plus” sign to your email username, Gmail will ignore anything written between the + and @ sign in the email address and still deliver the message to the same mailbox.
- ▶ Any email address sent to
  - ▶ mypersonalemail+linkedin@gmail.com
  - ▶ mypersonalemail+continente@gmail.com
  - ▶ mypersonalemail+financas@gmail.com
- ▶ Will still reach the Gmail inbox of mypersonalemail@gmail.com inbox though, technically, they are three different email aliases.
- ▶ Know who is sharing your email 😊

# Passwords / Credentials

## Please don't share

- ▶ Kaspersky
  - ▶ Check your password ([link](#)) ➡
    - ▶ **(or maybe not)**
  - ▶ Check last name – “vieira” or “Vieira” or “Vieira123”
- ▶ Top 10 passwords
  - ▶ “qwerty”, “password”, ...
  - ▶ Country specific: BR example “password” → “senha”
- ▶ Daniel Miessler SecLists
  - ▶ Usernames ([link](#))
  - ▶ Passwords ([link](#))
  - ▶ Default Credentials ([link](#))
- ▶ IoT Default Passwords ([link](#)) ➡

# Insecure

## Insecure Cameras - Is your camera secure ?

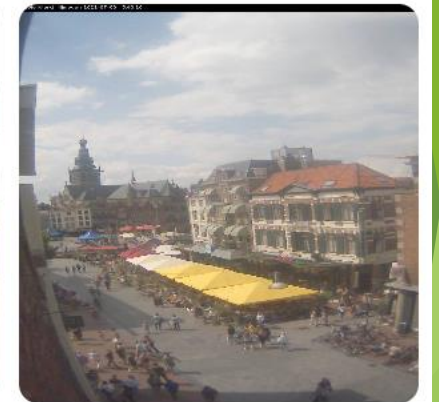
- Browser edit ([link](#))
  - Portugal ([link](#))



Live camera in Lisbon, Portugal



Live camera in Lisbon, Portugal



Live camera in Amsterdam, Netherlands



Live camera in Kiefersfelden, Germany



Live camera in PRAGUE, Czech Republic

# Databreach

# Databreach

## Is not a thing of the past

- ▶ Troy Hunt
  - ▶ HaveIBeenPwned ([link](#))
  - ▶ Pwned websites ([link](#))
- ▶ Ashley Madison Breach 2015 ([link](#))
  - ▶ When private data gets public
- ▶ Piracy - Subtitles
  - ▶ Don't think you can hide – **Illegal activities are tracked**
- ▶ Companies are leaking all your information
  - ▶ Compromised data: Dates of birth, Email addresses, Employers, Family structure, Genders, Income levels, Living costs, Marital statuses, Mothers maiden names, Names, Phone numbers, Physical addresses, Places of birth, Religions, Spouses names

# Databreach

## Company credentials ?

- ▶ Source
  - ▶ Publicly available list of credentials
  - ▶ More than 10k credentials just for Bosch
- ▶ Information gathered
  - ▶ Rule of email/login
    - ▶ (FirstName.LastName)@((Country).(company).com)
  - ▶ Rule of password complexity
  - ▶ List of users
    - ▶ Phishing campaigns
    - ▶ Brute force
    - ▶ Look for those users on Social Media
- ▶ Added Problem
  - ▶ Credentials reuse

Email/Login	Password
data/m/i/c:mich	er@de.bosch.com:\$HEX[576569c3
data/m/i/c:mich	er@de.bosch.com:weißer
data/m/i/c:mich	zkus@de.bosch.com:shannon
data/m/i/c:mich	tke@bosch.com:lumpi007
data/m/i/c:mich	der@de.bosch.com:a6fc6b19
data/m/i/c:mich	z4@de.bosch.com:jaguar
data/m/i/c:mich	@us.bosch.com:ultra06
data/m/i/c:mich	@cz.bosch.com:micsis
data/m/i/c:mich	ll@uk.bosch.com:frances
data/m/i/c:mich	@bosch.com:petros69
data/m/i/c:mich	us.bosch.com:mike5920
data/m/i/c:mich	n@us.bosch.com:radar123
data/m/i/c:mich	om@us.bosch.com:2af415a2174b1
data/m/i/c:mich	om@us.bosch.com:hardrock
data/m/i/c:mich	rger@za.bosch.com:mike123
data/m/i/c:mich	cn.bosch.com:Mikomido
data/m/i/c:mich	@us.bosch.com:bulldog3120
data/m/i/c:mich	@de.bosch.com:maccaroni
data/m/i/c:mich	mann@de.bosch.com:\$HEX
data/m/i/c:mich	mann@de.bosch.com:asdfjklö
data/m/i/c:mich	mann@de.bosch.com:asdfjklr¶
data/m/i/c:mich	comcast.net:mojopapa
data/m/i/c:mich	comcast.net:mojopapa1
data/m/i/c:mich	s.bosch.com:bogey
data/m/i/c:mich	cz.bosch.com:koqueti
data/m/i/c:mich	cz.bosch.com:wunazaqu
data/m/i/c:mich	zak@pl.bosch.com:igi74mick77
data/m/i/c:mich	z.bosch.com:hyqokibu
data/m/i/c:mich	@fr.bosch.com:CHOISNE
data/m/i/c:mich	@be.bosch.com:elsclaes
data/m/i/c:mich	de.bosch.com:janlasse79
data/m/i/c:mich	nl.bosch.com:Killer1
data/m/i/c:mich	ey@us.bosch.com:leander65
data/m/i/c:mich	r.bosch.com:ro67vsh5
data/m/i/c:mich	nte@it.bosch.com:michele
data/m/i/c:mich	lli@us.bosch.com:radica4
data/m/i/c:mich	de@br.bosch.com:m1s2g3a4
data/m/i/c:mich	hi@br.bosch.com:Talita
data/m/i/c:mich	@br.bosch.com:Orquideas1



# Databreach

## Portuguese domain examples (2018)

- ▶ uminho.pt - Universidade do Minho
  - ▶ adv.oa.pt - Ordem dos Advogados
  - ▶ pj.pt - Policia Judiciária
  - ▶ mail.exercito.pt - Exército
  - ▶ cm-braga.pt - Câmara Municipal de Braga
  - ▶ cm-guimaraes.pt - Câmara Municipal de Guimarães
  - ▶ psd.pt - Partido Social Democrata
  - ▶ ps.pt - Partido Socialista
  - ▶ fcporto.pt - Futebol Clube do Porto
  - ▶ min.justiça - Ministério da Justiça
- 
- ▶ Were these the sources for criminal “hacker” Rui Pinto ?

Free to Share

# License

- ▶ Feel free to use/modify/share
- ▶ Teach someone
- ▶ Improve awareness