FEDERPRIVACY

PRIVACY DAY FORUM 2023

Protezione dei dati personali inclusiva e sviluppo sostenibile della società digitale

CNR Area della Ricerca di Pisa, 25 maggio 2023

Consiglio Nazionale delle Ricerche
Area Territoriale di Ricerca di Pisa

Il lato oscuro dell’Internet of Things

Domenico Laforenza
Ricercatore Emerito Associato
Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa

Scena tratta da:

«Accadde in una casa intelligente....»

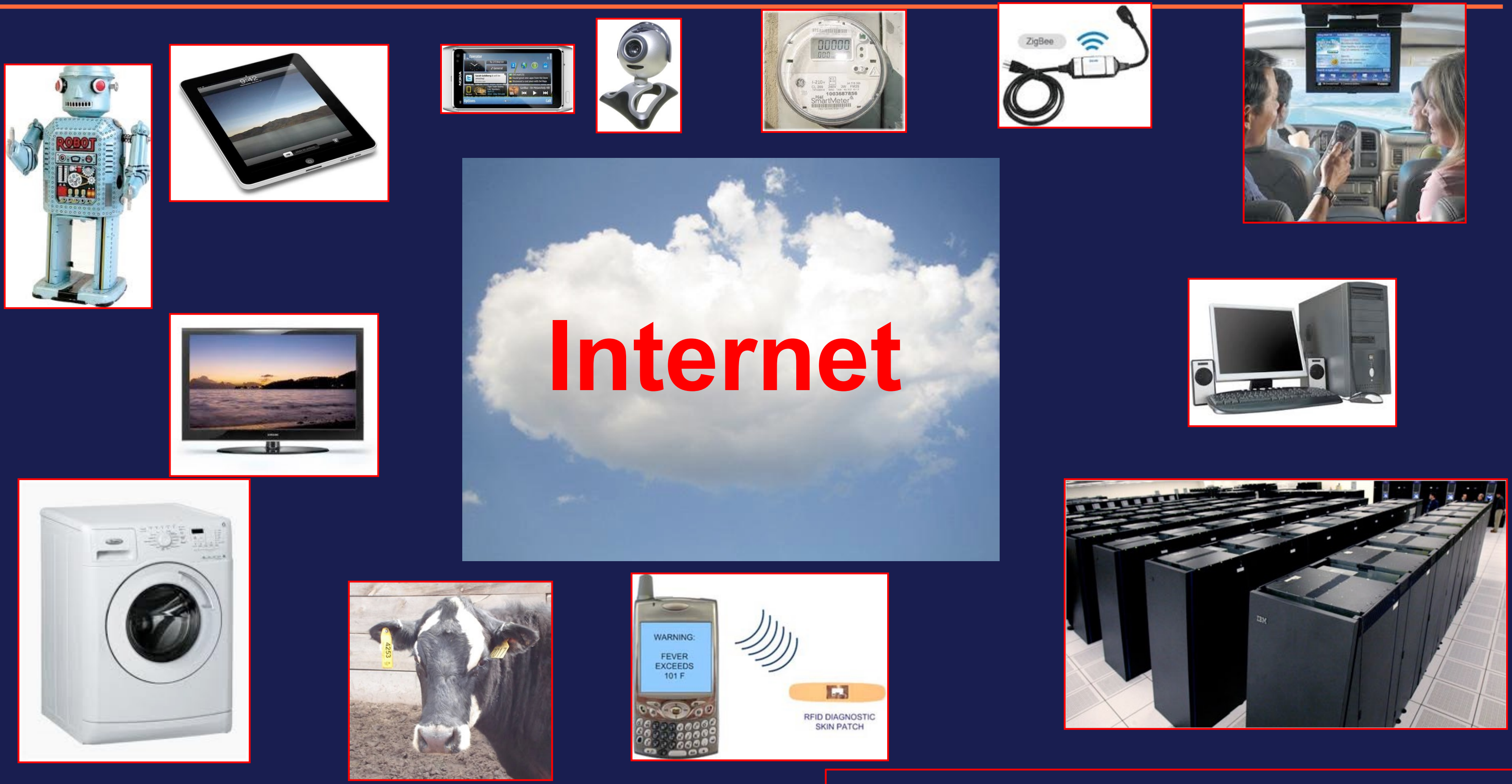
Lavatrice
Smart TV
Webcam

ssss...ma lo sai che la settimana scorsa i padroni sono andati in vacanza?

Ah, ecco perchè non li “vedevo” più.... Immagino che te l’abbia detto quella spiona della webcam?

Ma perchè danno sempre la colpa a me? Io l’ho saputo dallo smartphone che l’ha appreso da Facebook!

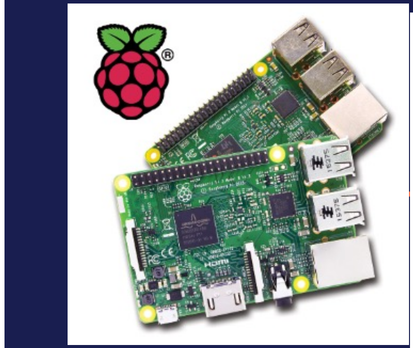
INTERNET

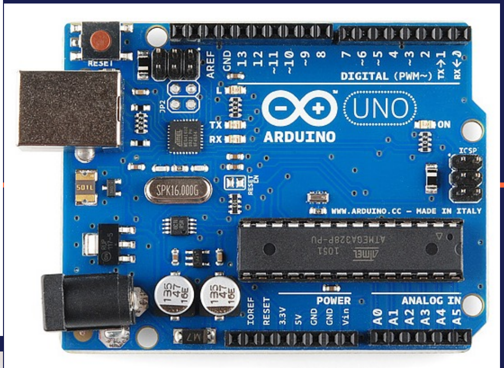


2a00:1620:c0:60:aa20:66ff:fe27:c47f

“Una rete a dimensione mondiale di “oggetti” interconnessi, indirizzabili univocamente mediante protocolli standard di comunicazione

TCP/IP



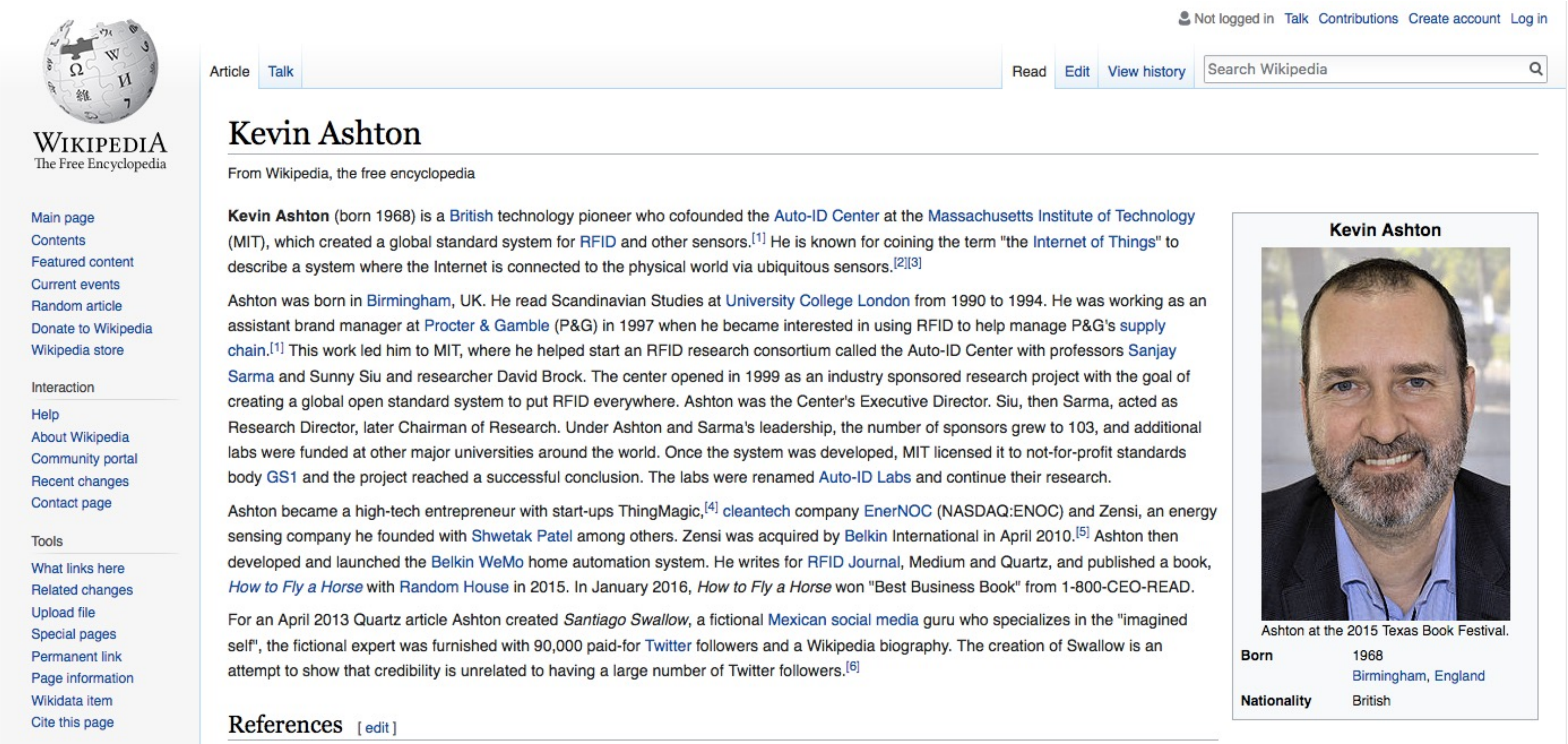


74/135 **Withings Stell HR** L'orologio analogico che monitora il battito cardiaco (foto: Milo Sciaky)

Le «cose»

Dispositivi connessi $(\approx 30\ G\ nel\ 2030)$

- termostati
- lampadine intelligenti
- prese elettriche intelligenti
- sistemi di intrattenimento (stereo, TV,..)
- assistenti personali
- telecamere di sicurezza e rilevatori di movimento
- rilevatori di fumo
- campanelli video e serrature intelligenti
- elettrodomestici (frigorifero, aspirapolvere, ecc.)
- giocattoli e localizzatori per bambini
- webcam per controllare bambini o animali domestici
- mangiatoie intelligenti per animali domestici
- ……..



Kevin Ashton

From Wikipedia, the free encyclopedia

Kevin Ashton (born 1968) is a British technology pioneer who cofounded the Auto-ID Center at the Massachusetts Institute of Technology (MIT), which created a global standard system for RFID and other sensors.[1] He is known for coining the term "the Internet of Things" to describe a system where the Internet is connected to the physical world via ubiquitous sensors.[2][3]

Ashton was born in Birmingham, UK. He read Scandinavian Studies at University College London from 1990 to 1994. He was working as an assistant brand manager at Procter & Gamble (P&G) in 1997 when he became interested in using RFID to help manage P&G's supply chain.[1] This work led him to MIT, where he helped start an RFID research consortium called the Auto-ID Center with professors Sanjay Sarma and Sunny Siu and researcher David Brock. The center opened in 1999 as an industry sponsored research project with the goal of creating a global open standard system to put RFID everywhere. Ashton was the Center's Executive Director. Siu, then Sarma, acted as Research Director, later Chairman of Research. Under Ashton and Sarma's leadership, the number of sponsors grew to 103, and additional labs were funded at other major universities around the world. Once the system was developed, MIT licensed it to not-for-profit standards body GS1 and the project reached a successful conclusion. The labs were renamed Auto-ID Labs and continue their research.

Ashton became a high-tech entrepreneur with start-ups ThingMagic,[4] cleantech company EnerNOC (NASDAQ:ENOC) and Zensi, an energy sensing company he founded with Shwetak Patel among others. Zensi was acquired by Belkin International in April 2010.[5] Ashton then developed and launched the Belkin WeMo home automation system. He writes for RFID Journal, Medium and Quartz, and published a book, *How to Fly a Horse* with Random House in 2015. In January 2016, *How to Fly a Horse* won "Best Business Book" from 1-800-CEO-READ.

For an April 2013 Quartz article Ashton created *Santiago Swallow*, a fictional Mexican social media guru who specializes in the "imagined self", the fictional expert was furnished with 90,000 paid-for Twitter followers and a Wikipedia biography. The creation of Swallow is an attempt to show that credibility is unrelated to having a large number of Twitter followers.[6]

Kevin Ashton	
Ashton at the 2015 Texas Book Festival.	
Born	1968 Birmingham, England
Nationality	British

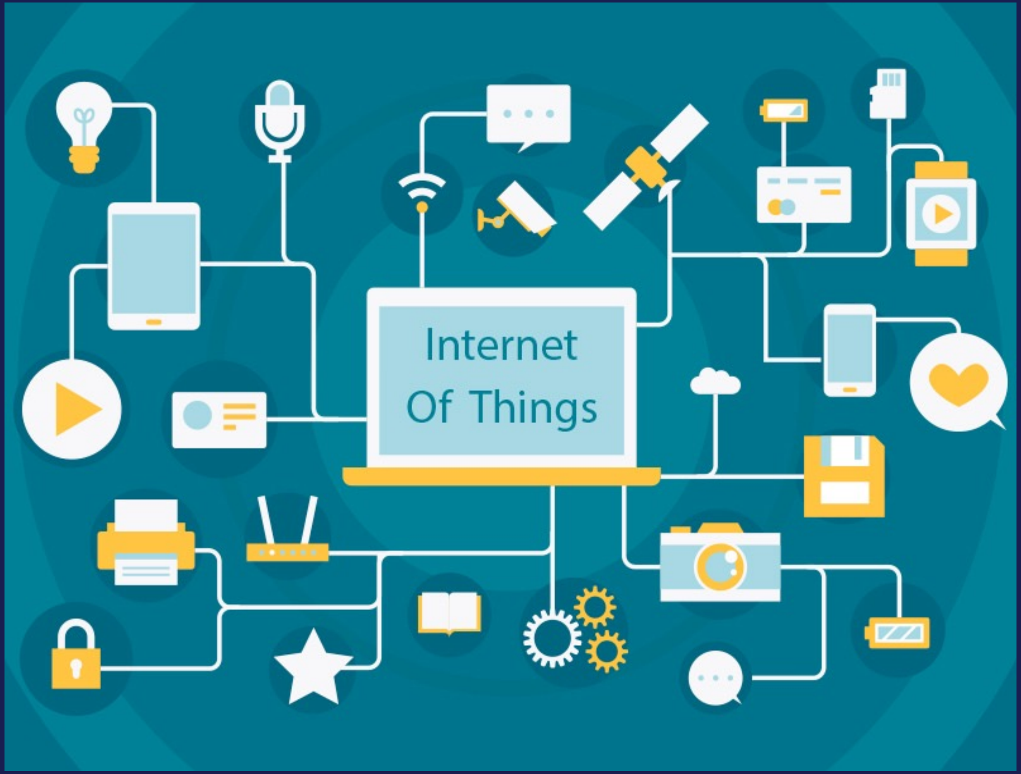
References [edit]

Internet of Things, coniata nel 1999 dal ricercatore britannico **Kevin Ashton** per indicare la possibilità di collegare a Internet qualunque «oggetto» o «dispositivo dotato di sensori»

Internet of Things (IoT)

(Le quattro componenti)

- Percezione
- Calcolo
- Comunicazione
- Attuazione



Casa intelligente (Smart Home)

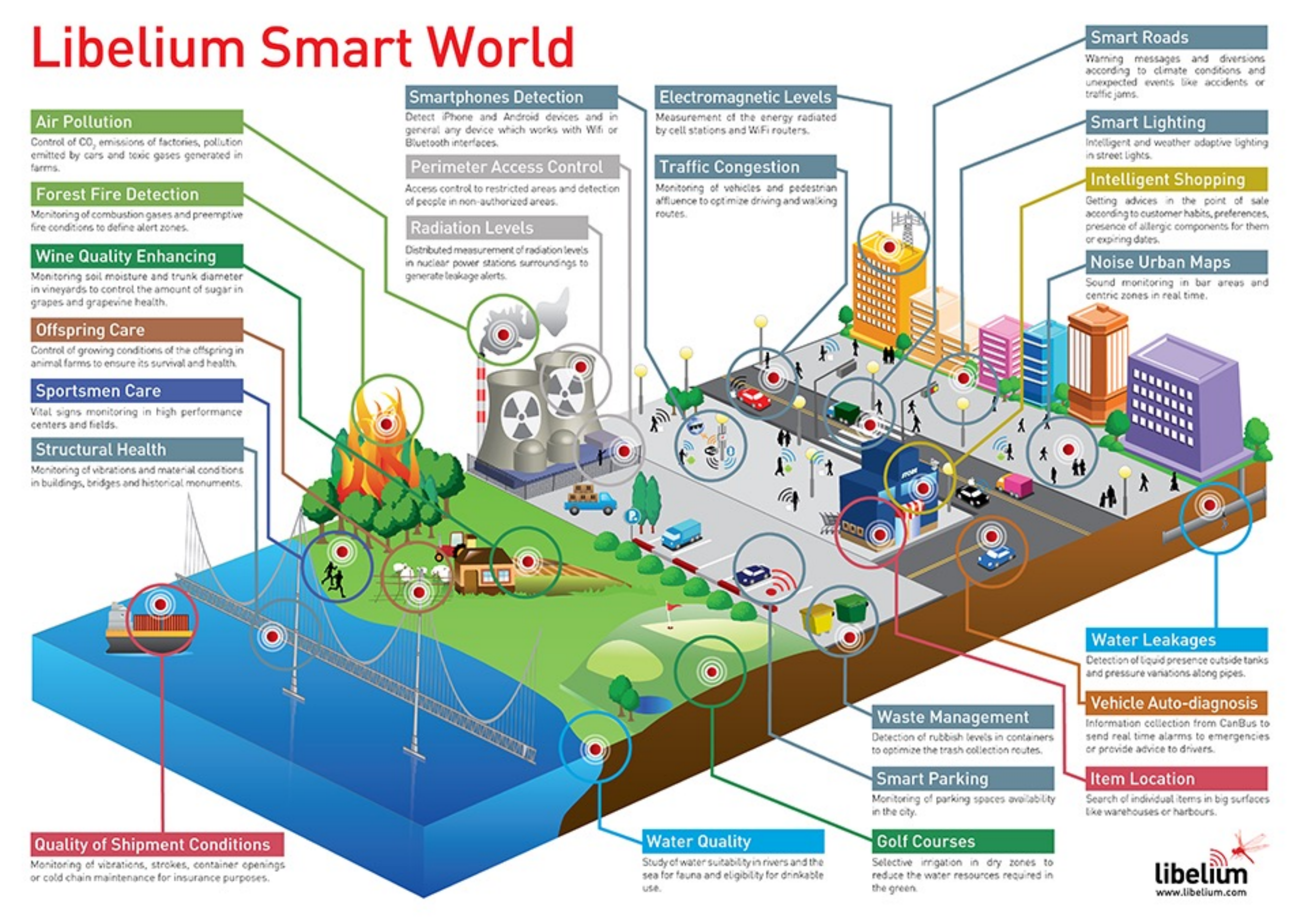
Gestione in automatico e/o da remoto degli impianti e degli oggetti connessi dell'abitazione

- Obiettivi:
- ridurre i consumi energetici
- migliorare il comfort
- sicurezza dell'abitazione e delle persone al suo interno

https://pixabay.com/it/photos/smart-home-casa-tecnologia-3574545/

Città intelligente (Smart City)

Monitoraggio e gestione degli elementi di una città e per migliorarne vivibilità, sostenibilità e competitività



Libelium Smart World

Air Pollution
Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

Forest Fire Detection
Monitoring of combustion gases and preemptive fire conditions to define alert zones.

Wine Quality Enhancing
Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.

Offspring Care
Control of growing conditions of the offspring in animal farms to ensure its survival and health.

Sportsmen Care
Vital signs monitoring in high performance centers and fields.

Structural Health
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.

Smartphones Detection
Detect iPhone and Android devices and in general any device which works with Wifi or Bluetooth interfaces.

Perimeter Access Control
Access control to restricted areas and detection of people in non-authorized areas.

Radiation Levels
Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.

Electromagnetic Levels
Measurement of the energy radiated by cell stations and WiFi routers.

Traffic Congestion
Monitoring of vehicles and pedestrian affluence to optimize driving and walking routes.

Smart Roads
Warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Smart Lighting
Intelligent and weather adaptive lighting in street lights.

Intelligent Shopping
Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.

Noise Urban Maps
Sound monitoring in bar areas and centric zones in real time.

Water Leakages
Detection of liquid presence outside tanks and pressure variations along pipes.

Vehicle Auto-diagnosis
Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.

Item Location
Search of individual items in big surfaces like warehouses or harbours.

Waste Management
Detection of rubbish levels in containers to optimize the trash collection routes.

Smart Parking
Monitoring of parking spaces availability in the city.

Golf Courses
Selective irrigation in dry zones to reduce the water resources required in the green.

Water Quality
Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.

Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

libelium
www.libelium.com

Esempi:

- mezzi per il trasporto pubblico
- illuminazione pubblica
- parcheggi
- smaltimento rifiuti
- inclusione e partecipazione sociale

https://www.libelium.com/libeliumworld/top-50-iot-sensor-applications-ranking/

Auto intelligente (Smart Car)

Auto connesse: comunicare informazioni in tempo reale al consumatore, interazione tra veicoli e con l'infrastruttura circostante: guida più sicura, prevenzione di incidenti

https://www.lagenziadiviaggi.it/auto-intelligenti-inaugurata-la-sezione-digital-di-aniasa/

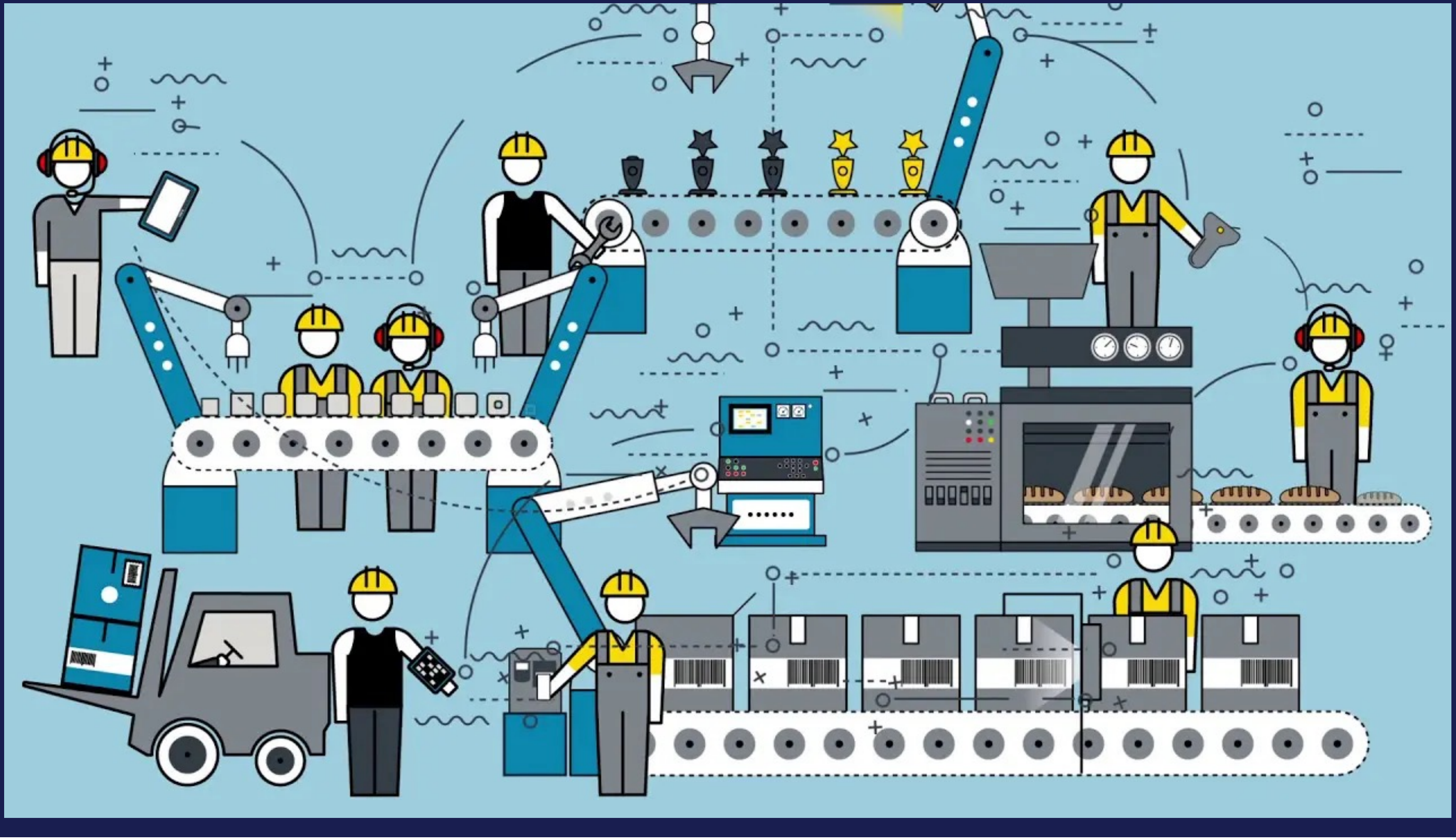
Agricoltura intelligente (Smart Agricolture)

Monitoraggio di parametri micro-climatici a supporto dell’agricoltura: migliorare la qualità dei prodotti, ridurre le risorse utilizzate e l’impatto ambientale

https://www.agendadigitale.eu/industry-4-0/smart-agricolture-che-cosa-serve-allitalia-il-quadro/

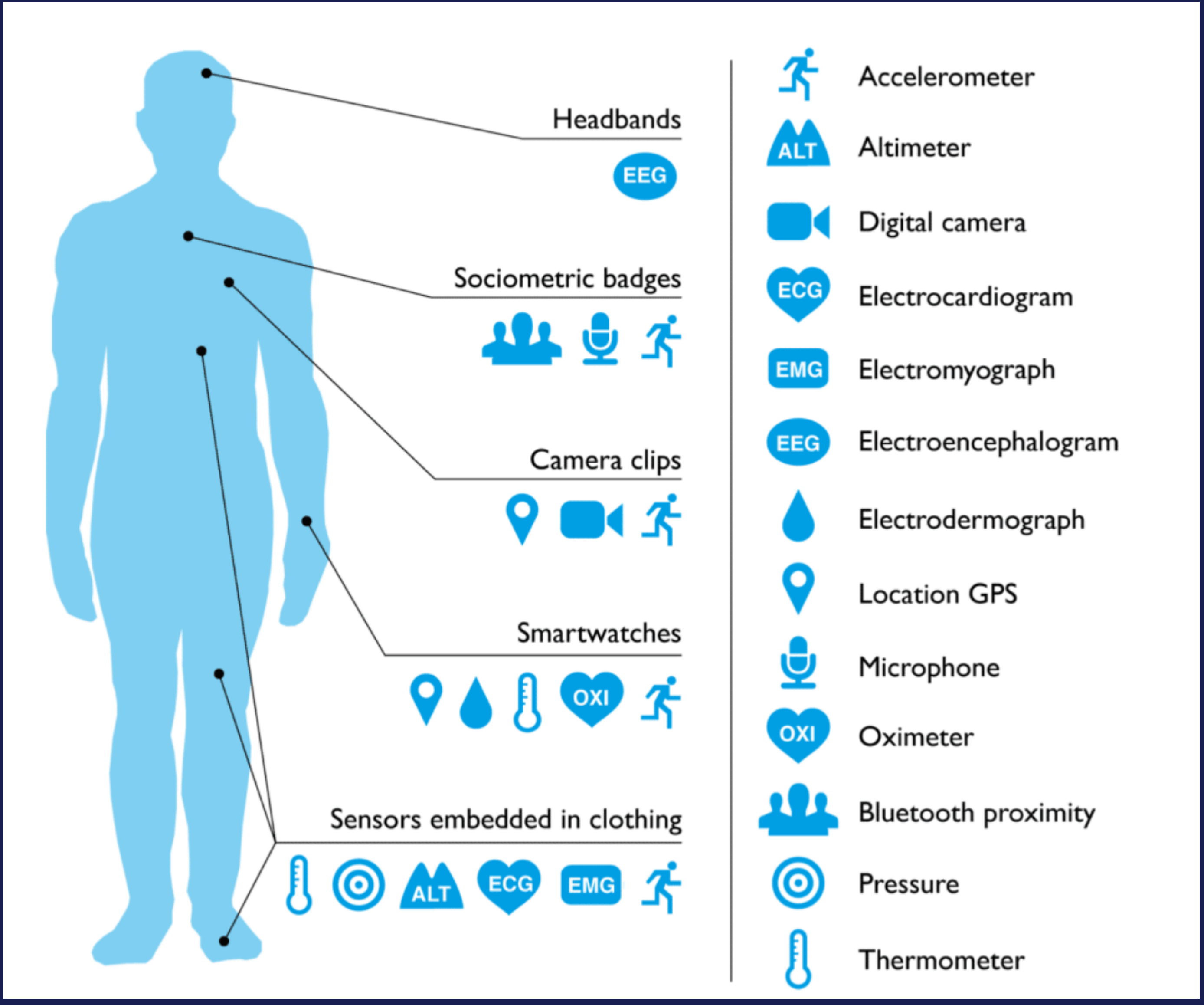
Industrial IoT (IoT per l'Industria 4.0)

Adozione di sistemi «cyber-fisici»: connessione dei macchinari, degli operatori e dei prodotti per abilitare nuove logiche di gestione della produzione



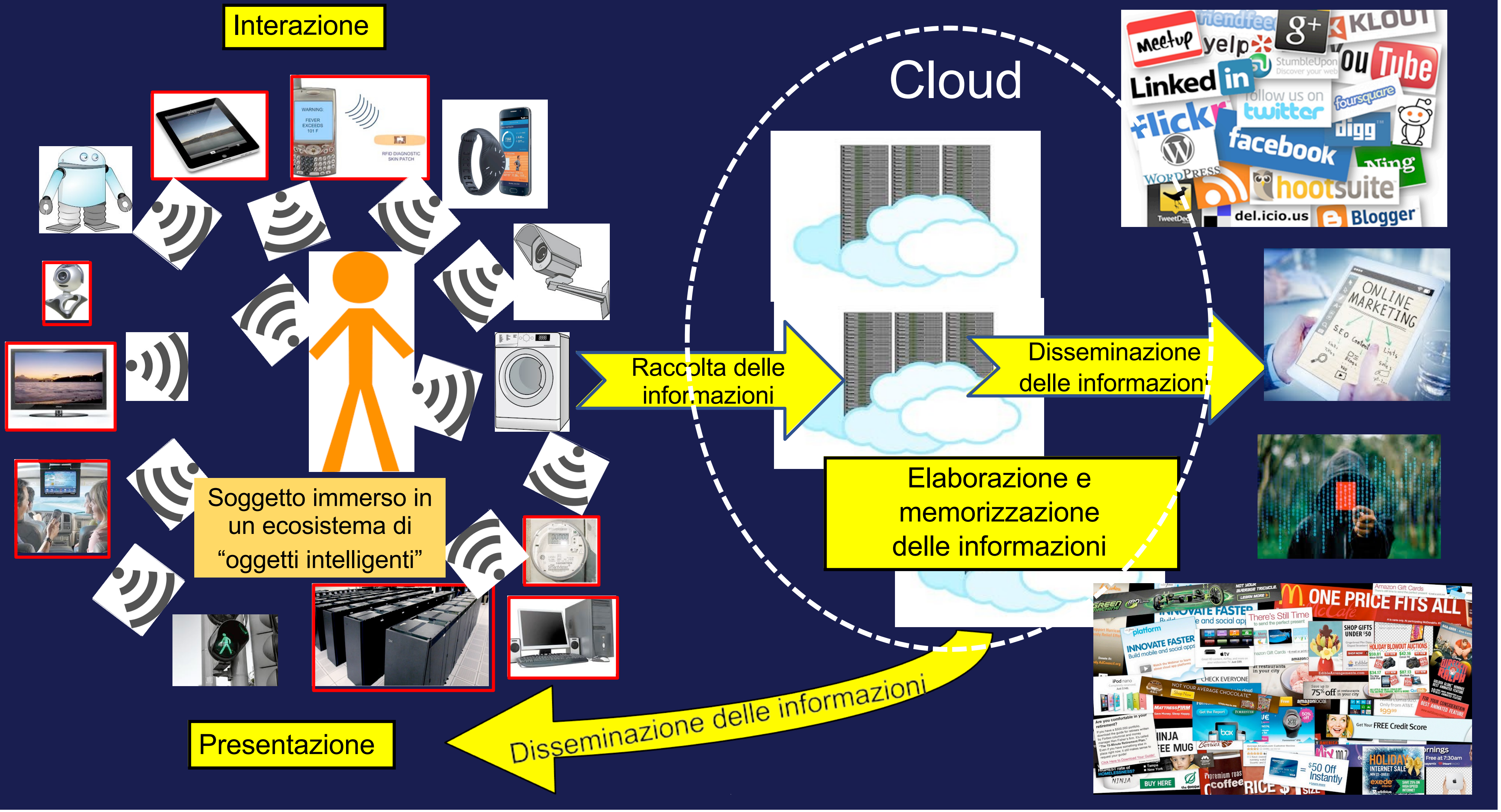
https://www.agendadigitale.eu/infrastrutture/industrial-iot-come-saa-nel-breve-termine/

Dispositivi IoT in Sanità



https://www.iotworlds.com/intelligent-iot-devices-for-health-and-well-being-an-ever-changing-evolution/zione

Modello di interazione tra un soggetto e l’ecosistema IoT circostante



Interazione

Cloud

Raccolta delle informazioni

Disseminazione delle informazioni

Elaborazione e memorizzazione delle informazioni

Soggetto immerso in un ecosistema di “oggetti intelligenti”

Presentazione

Disseminazione delle informazioni

Potenziali punti di attacco alla privacy

Come proteggere la nostra sicurezza/privacy dall'invasione dei nuovi «popoli nomadi»?

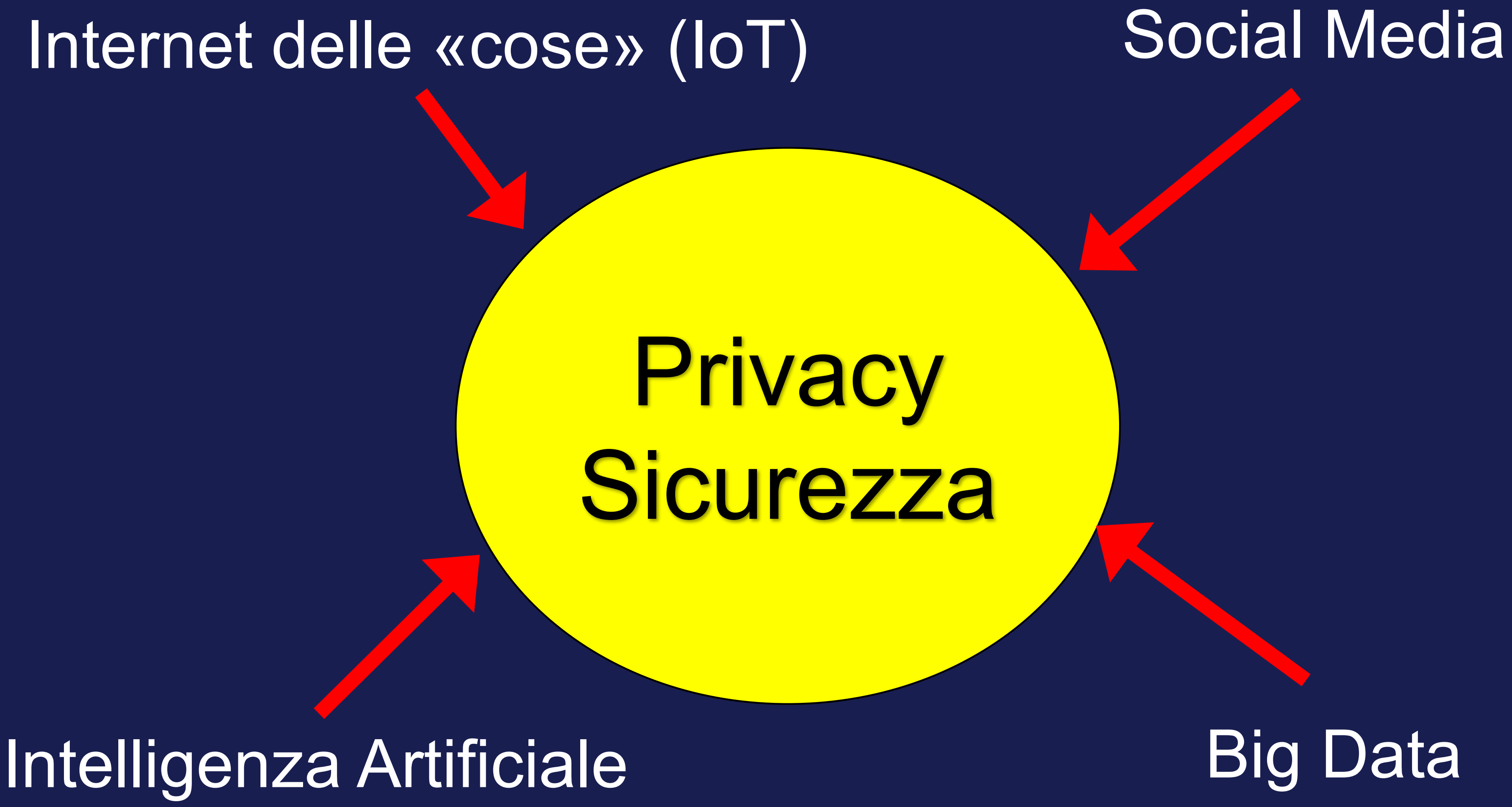
La Valle della sicurezza e della privacy

La superfice di attacco si espande a dismisura….

Privacy e Security

Due facce della stessa medaglia

Privacy e sicurezza delle persone sotto attacco…

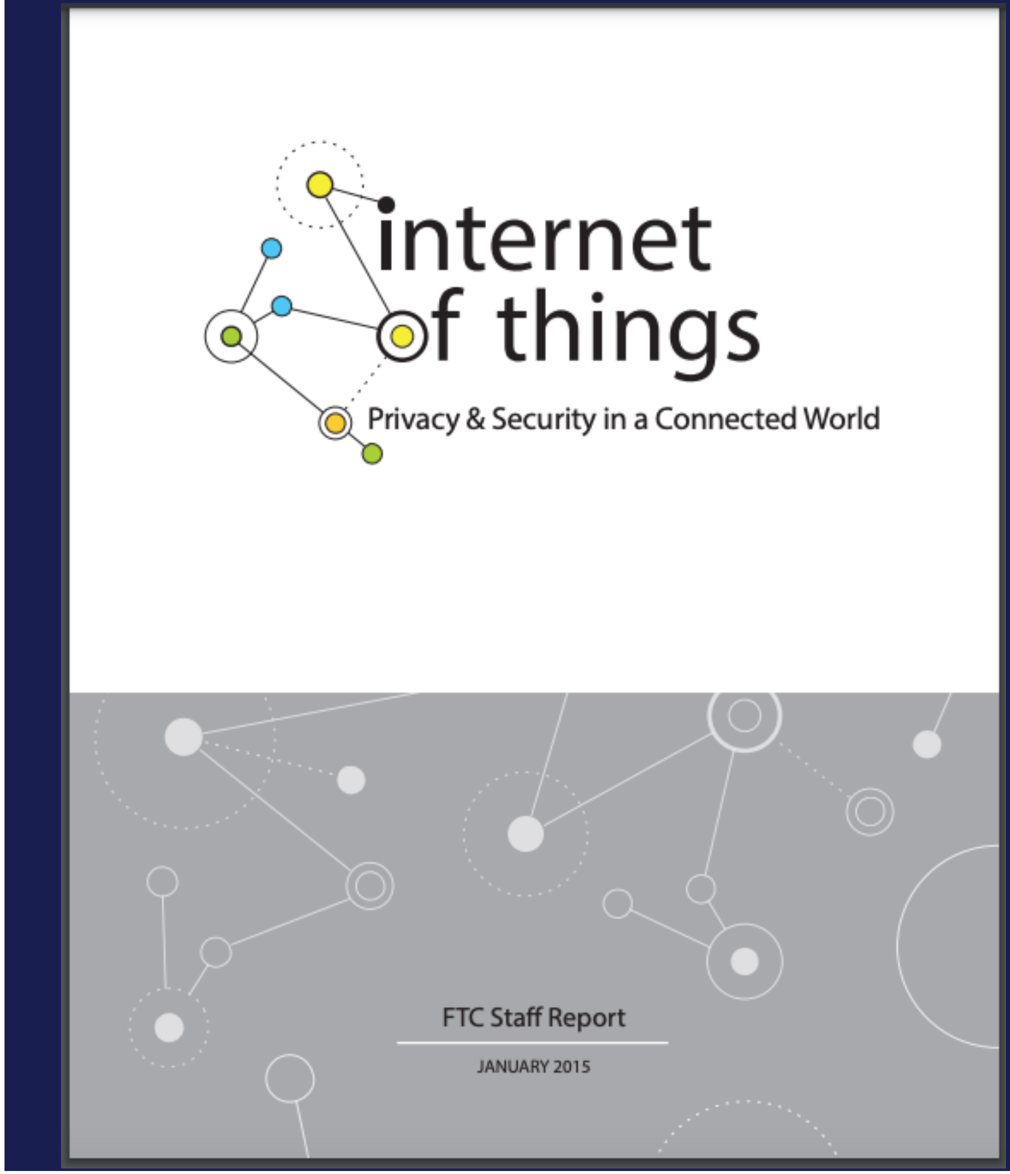


Privacy: Protezione “by Laws”

- Esempi:
  - General Data Protection Regulation (GDPR)
    - Regolamento 2016/679 UE (25 maggio 2018)
  - Fair Information Practice Principles (FIPPS)
  - Children’s Online Privacy Protection Act (COPPA)
  - ………

https://www.garanteprivacy.it/codice

Correva l'anno 2015……



internet of things

Privacy & Security in a Connected World

FTC Staff Report

JANUARY 2015

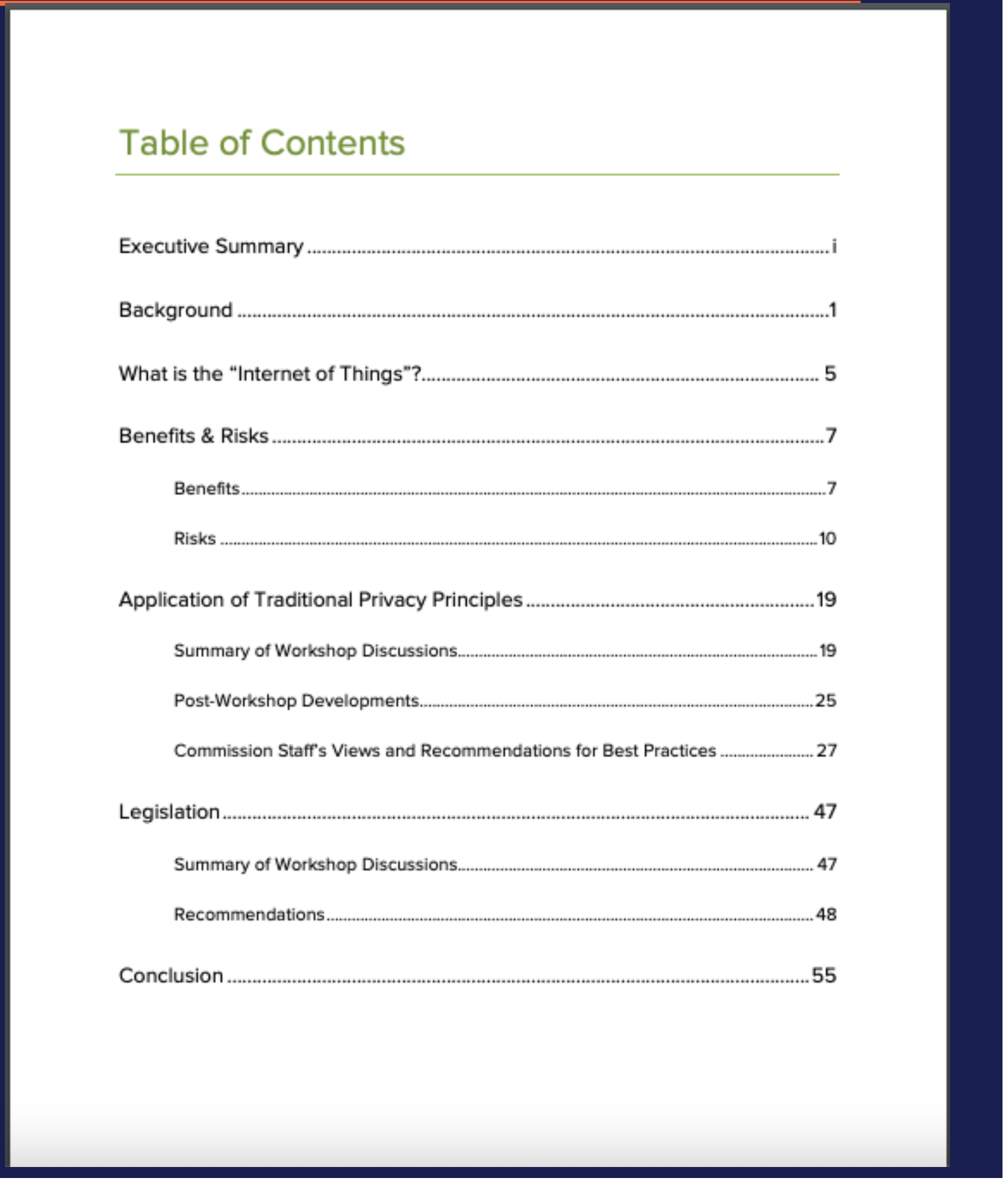
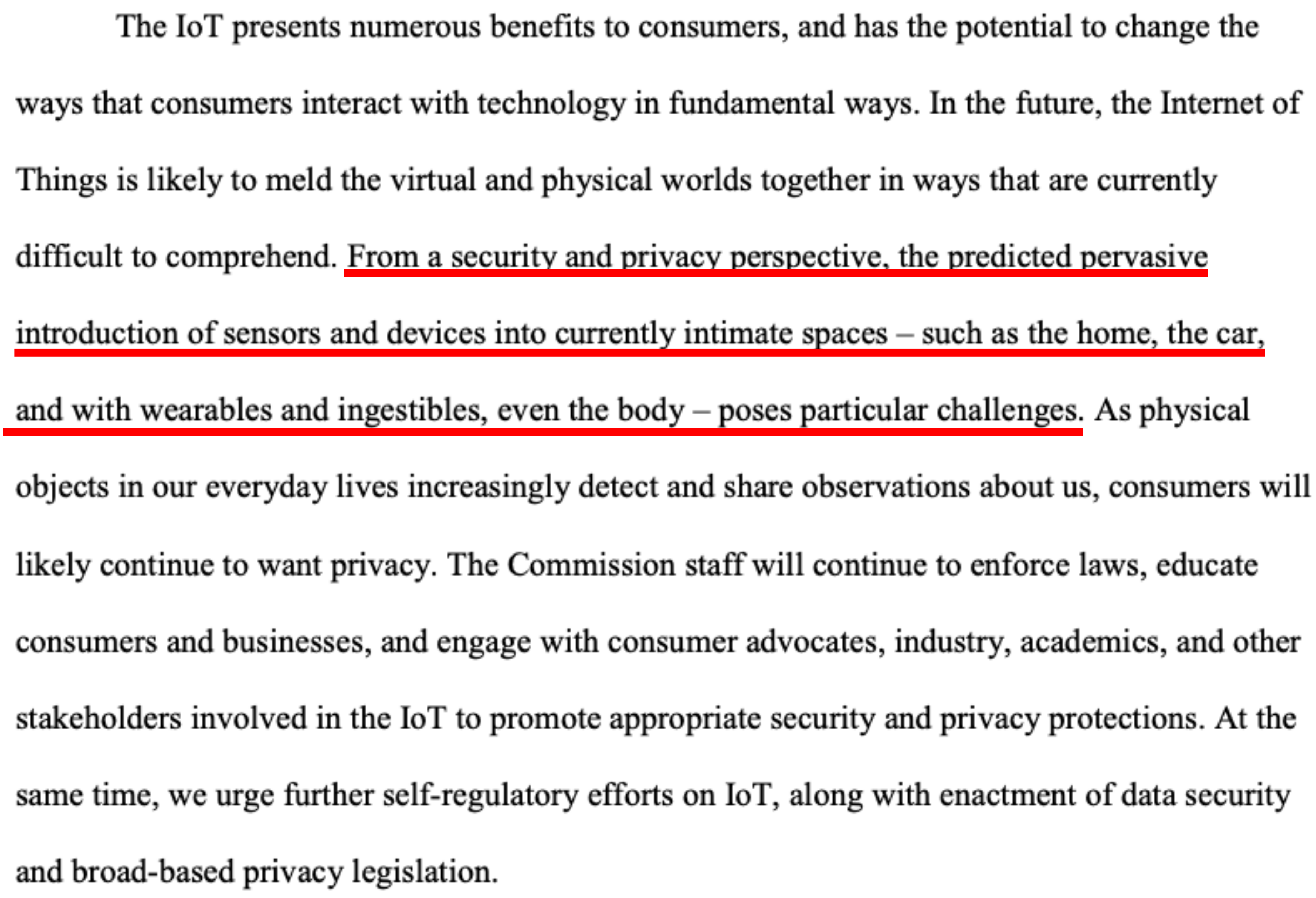


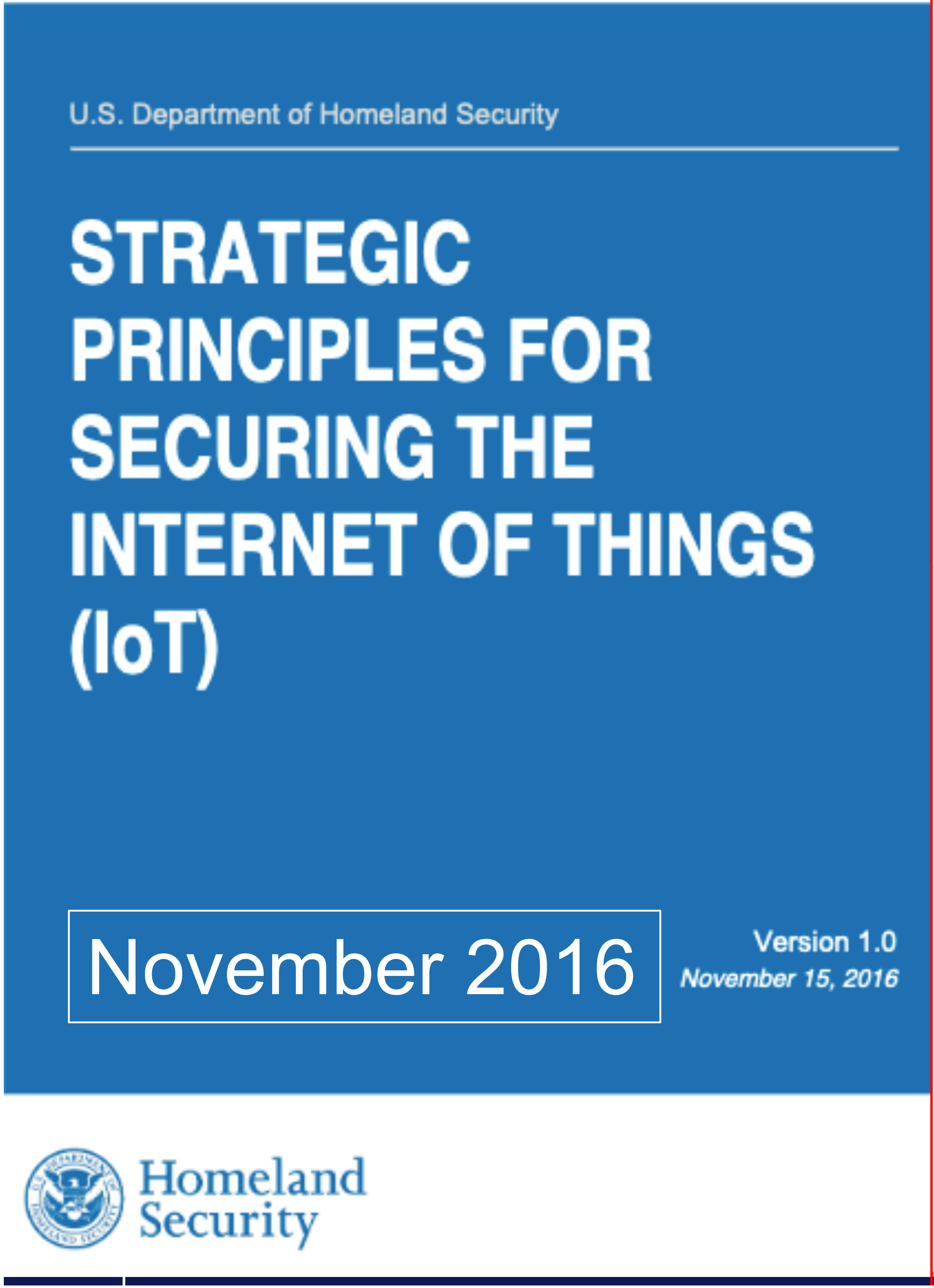
Table of Contents

https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy

Conclusion



The IoT presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car, and with wearables and ingestibles, even the body – poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation.



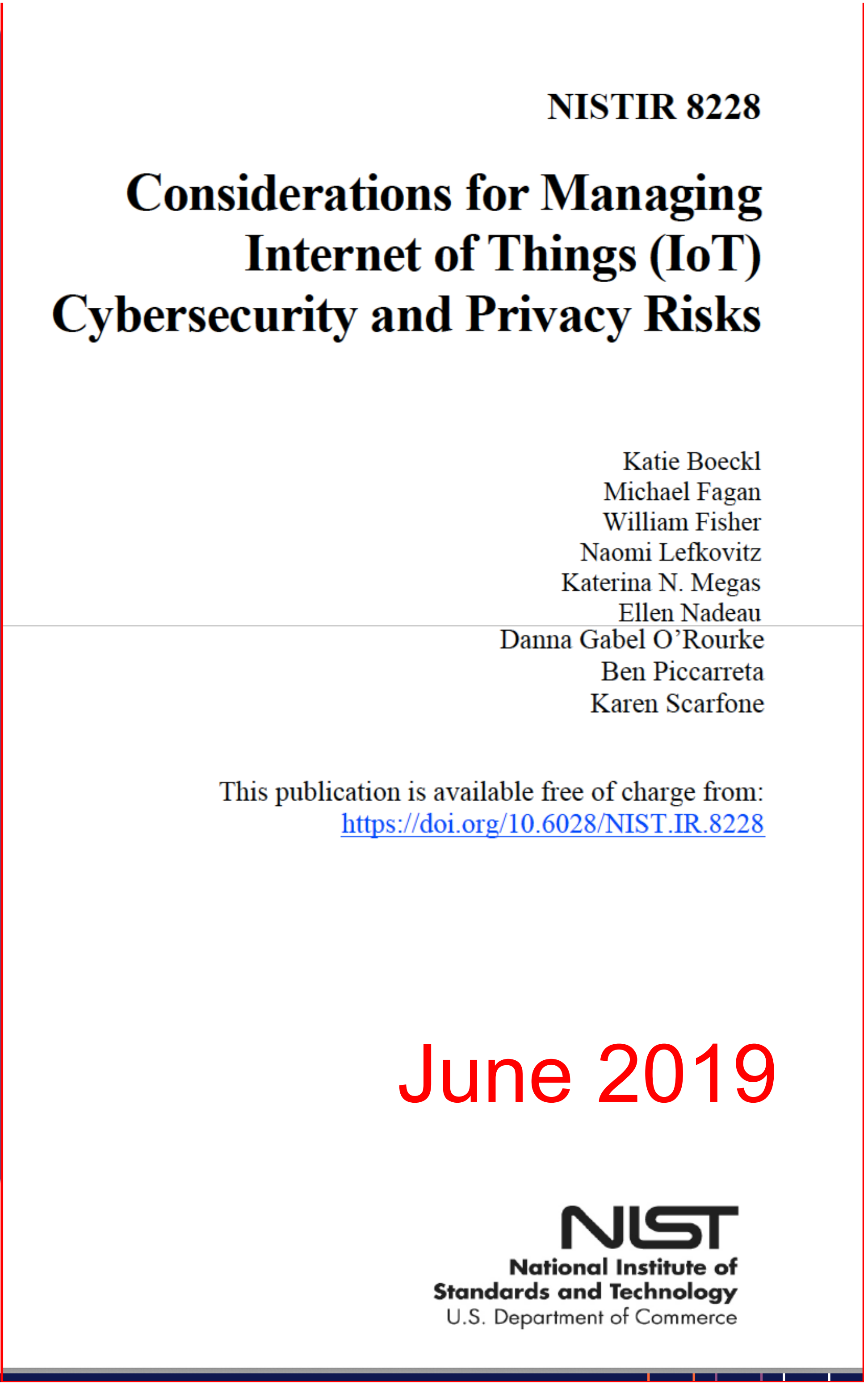
U.S. Department of Homeland Security

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

November 2016

Version 1.0
November 15, 2016

Homeland
Security



NISTIR 8228

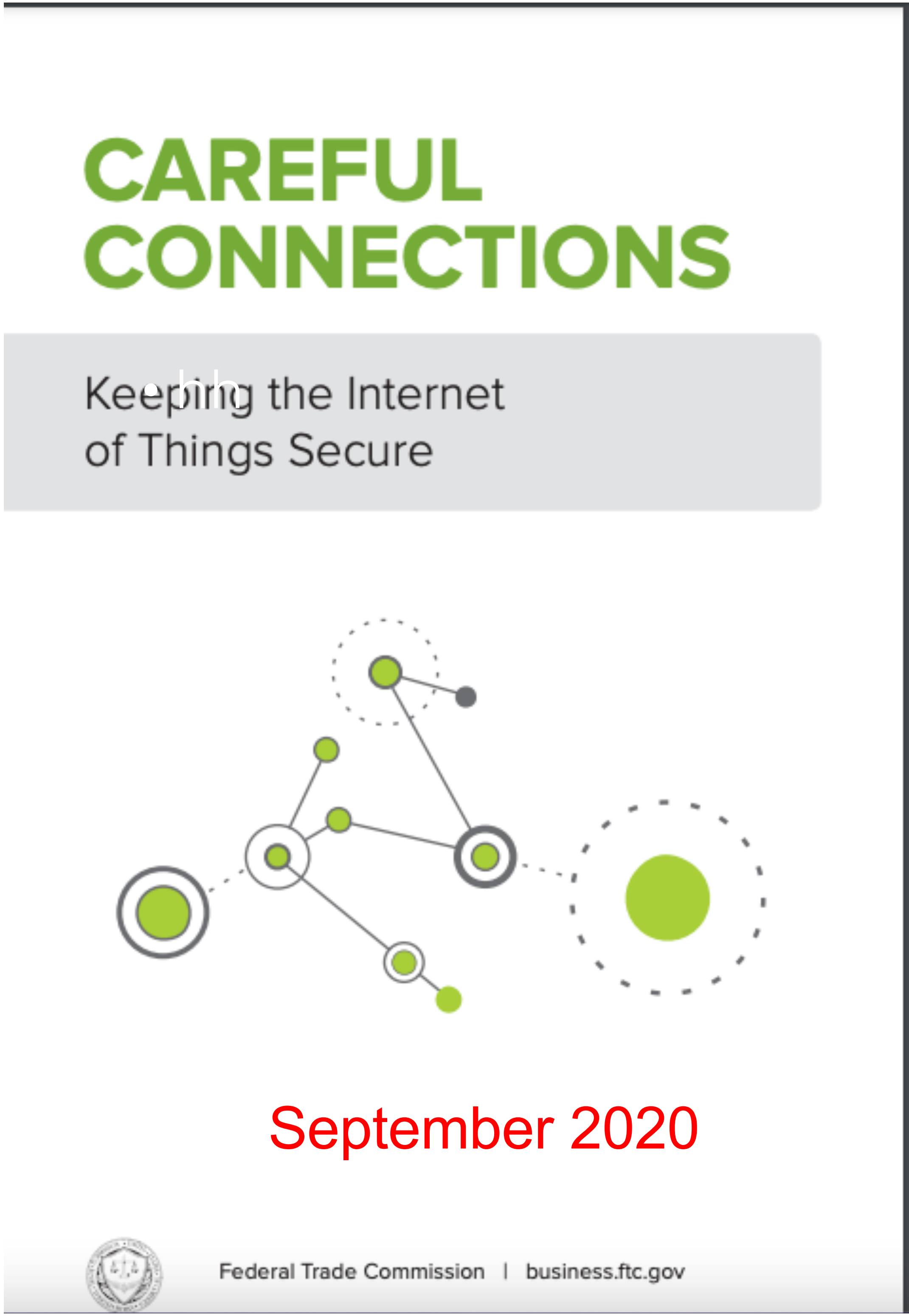
Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

Katie Boeckl
Michael Fagan
William Fisher
Naomi Lefkovitz
Katerina N. Megas
Ellen Nadeau
Danna Gabel O'Rourke
Ben Piccarreta
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8228

June 2019

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



CAREFUL CONNECTIONS

Keeping the Internet
of Things Secure

September 2020

Federal Trade Commission | business.ftc.gov

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SECURING THE INTERNET OF THINGS

Secure supply chain for IoT

NOVEMBER 2020

November 2020

https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/@@download/fullReport

ENISA Threat Landscape

15 Top Threats in 2020

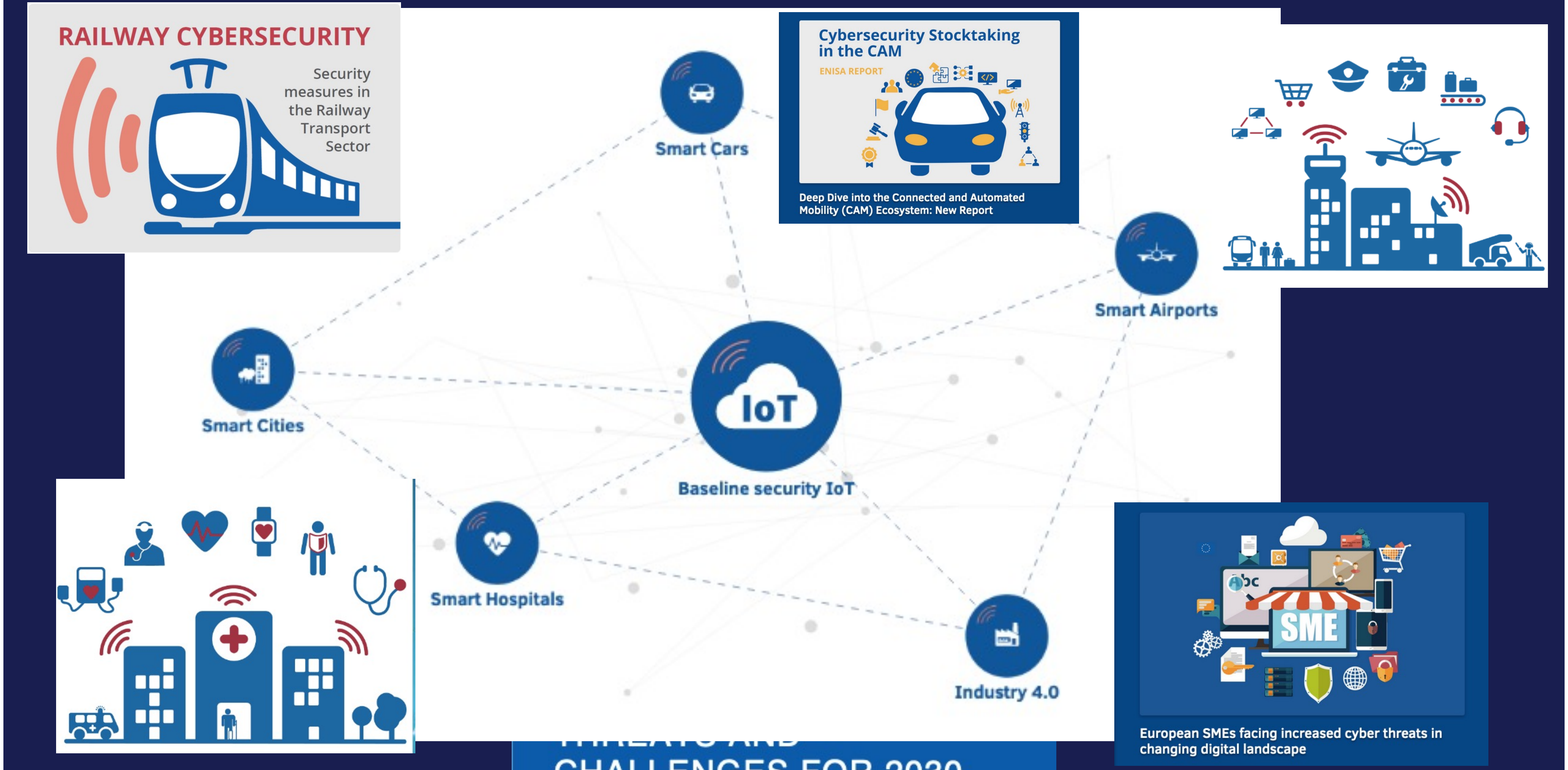
enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

www.enisa.europa.eu

For more information: https://www.enisa.europa.eu/topics/etl

IoT: Sicurezza e Privacy



RAILWAY CYBERSECURITY

Security measures in the Railway Transport Sector

Cybersecurity Stocktaking in the CAM

ENISA REPORT

Deep Dive into the Connected and Automated Mobility (CAM) Ecosystem: New Report

European SMEs facing increased cyber threats in changing digital landscape

CHALLENGES FOR 2030

MARCH 2023

https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

FOR CYBERSECURITY

ENISA THREAT LANDSCAPE 2022

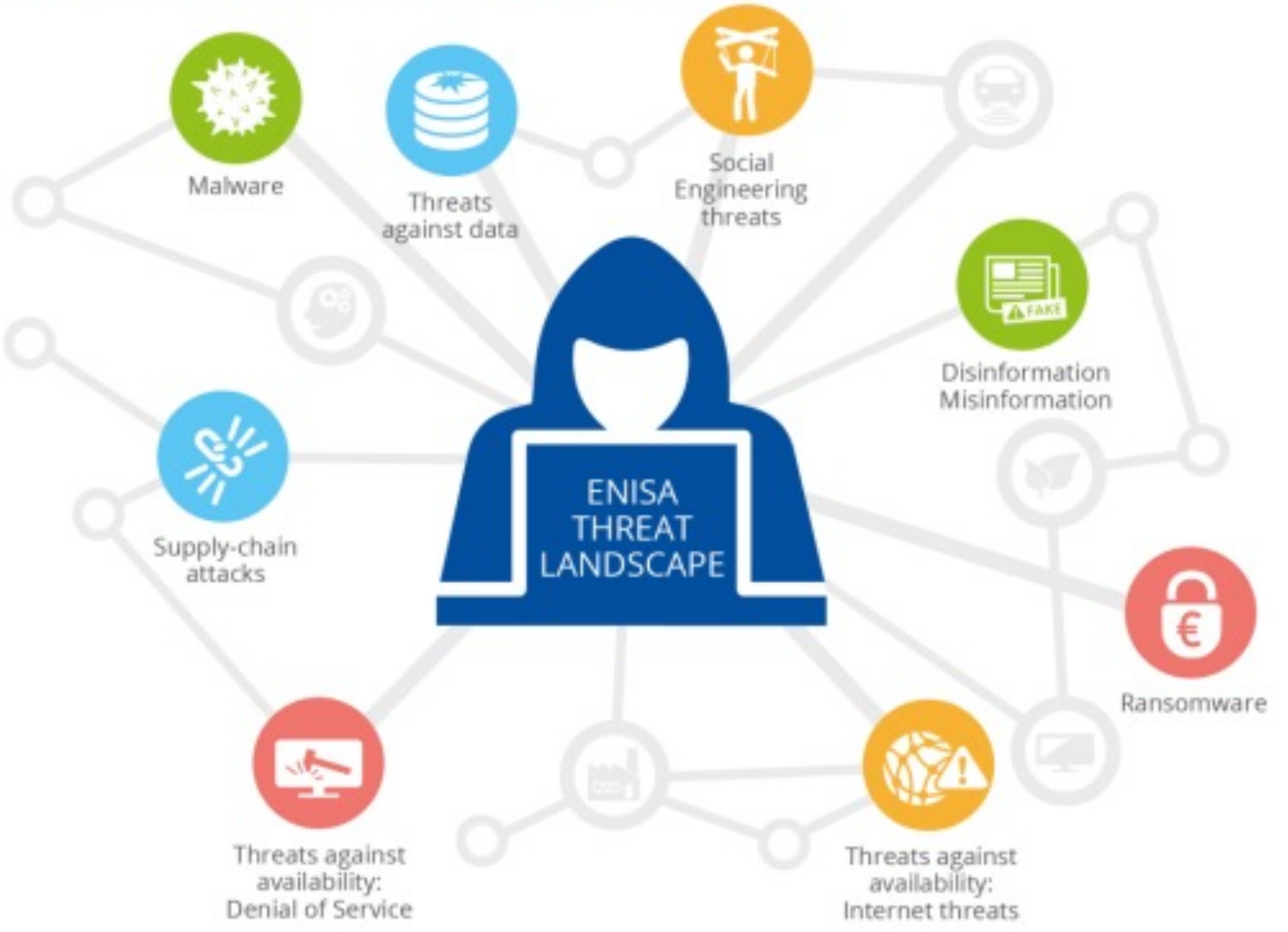
(July 2021 to July 2022)

OCTOBER 2022

Minacce

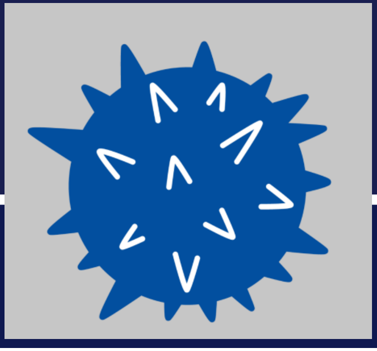
1. Ransomware
2. Malware
3. Social Engineering
4. Threats against data 5
5. Threats against availability: Denial of Service
6. Threats against availability: Internet threats
7. Disinformation – misinformation
8. Supply-chain attacks

Figure 1: ENISA Threat Landscape 2022 - Prime threats


Malware
Threats against data
Social Engineering threats
Disinformation Misinformation
ENISA THREAT LANDSCAPE
Supply-chain attacks
Ransomware
FAKE
Threats against availability: Denial of Service
Threats against availability: Internet threats

4.1.2 Malwa re targeting IoT almost doubles (pp. ......)

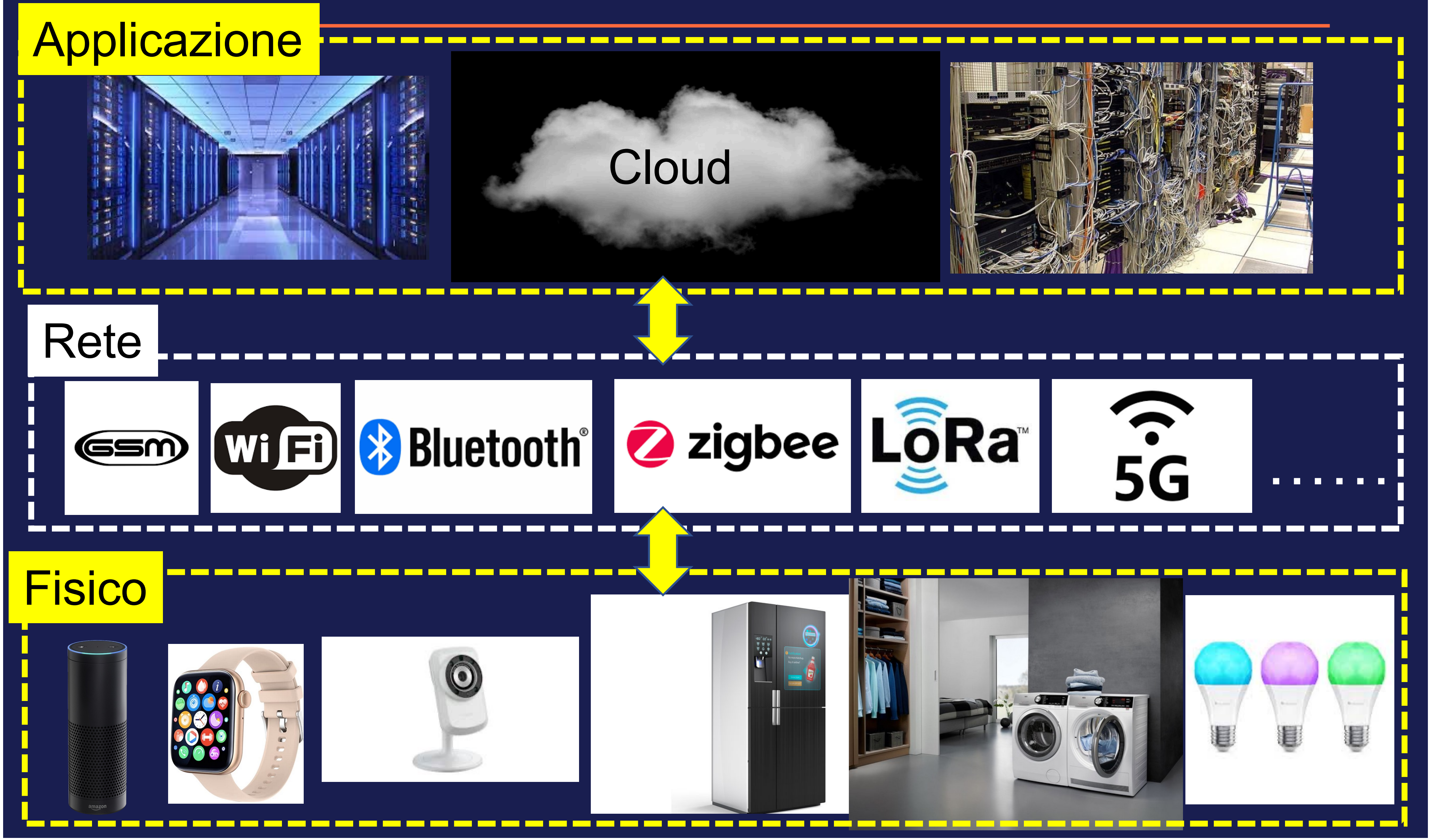
- IoT malware has increased over 2021. The change in the first half of 2022 shows the prevalence of IoT targeting malware almost doubling.
- In the first 6 months of 2022, the attack volume is already higher than had been recorded over the last 4 years.
- Research shows that in the first months of 2022, Mirai botnets were responsible for most attacks, quantified to more than 7 million attacks.
- Mozi, another large botnet, has grown slightly since Q3 2021 and was detected more than 5 million times



7.1.2 DDoS attacks are increasingly moving towards mobile networks and IoT

- (IoT) Devices are simple to corrupt, often coming with misconfigurations (e.g. weak passwords)
- At the same time, the increasing complexity of these mobile systems make users' shortage of security skills increasingly relevant
- DDoS attacks were often launched from compromised servers or consumer devices, such as IoT products and broadband routers

Architettura IoT



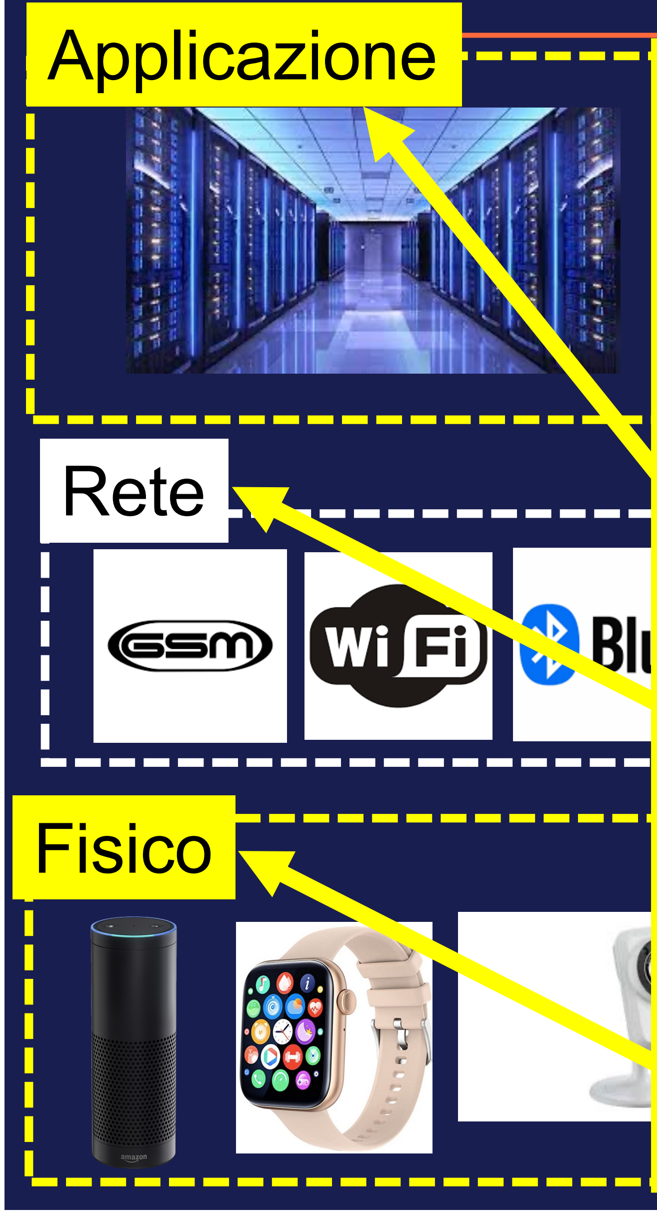
Applicazione

Cloud

Rete

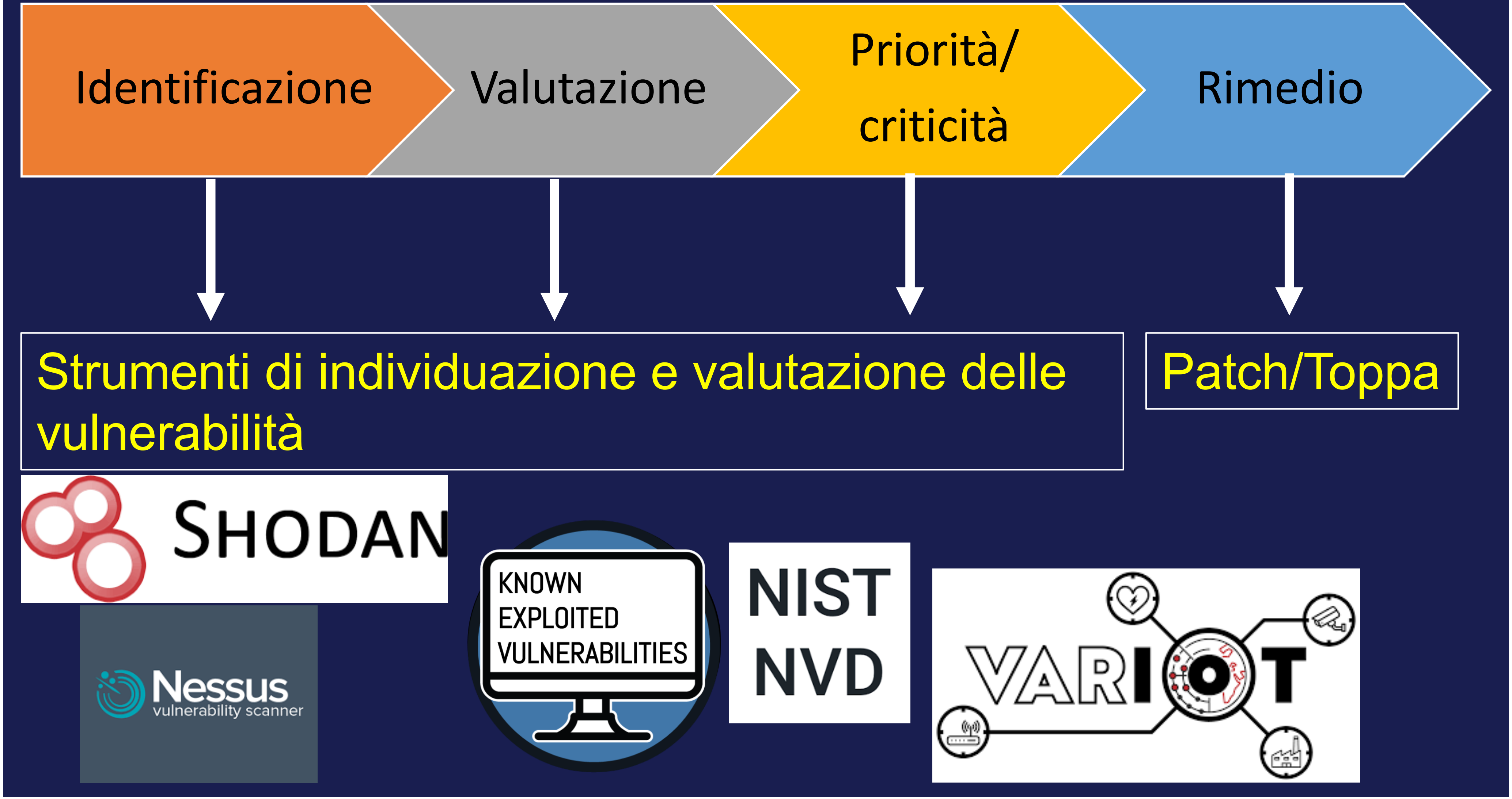
Fisico

Potenziali vulnerabilità



- Scarsa sicurezza fisica
- Autenticazione/autorizzazione debole
- Password deboli o settate dal costruttore e mai cambiate dall'utente
- Comunicazioni «in chiaro» (non crittografate)
- Firmware instabile
- Servizi di rete insicuri
- Software insicuro
- Porte aperte, anche se non necessarie
- Componenti insicure o obsolete
- ……….

Processo di gestione delle vulnerabilità



Identificazione

Valutazione

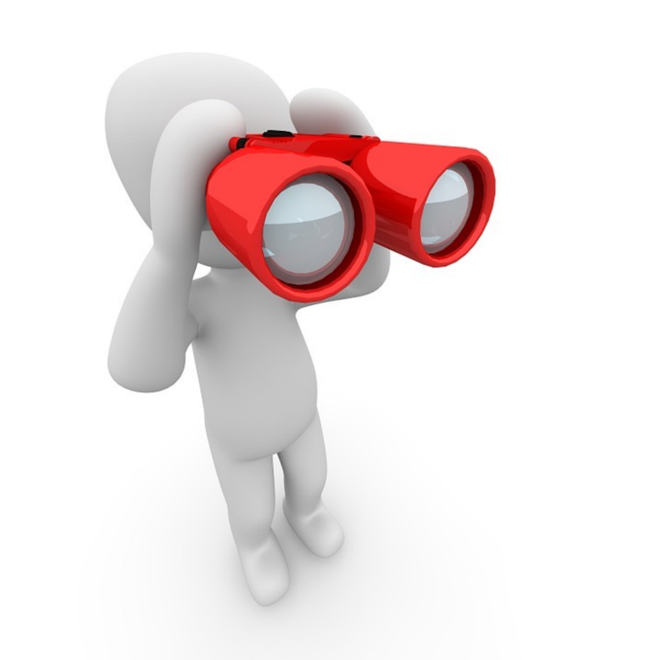
Priorità/ criticità

Rimedio

Strumenti di individuazione e valutazione delle vulnerabilità

Patch/Toppa

E’ possibile scoprire le «cose» collegate in Internet?

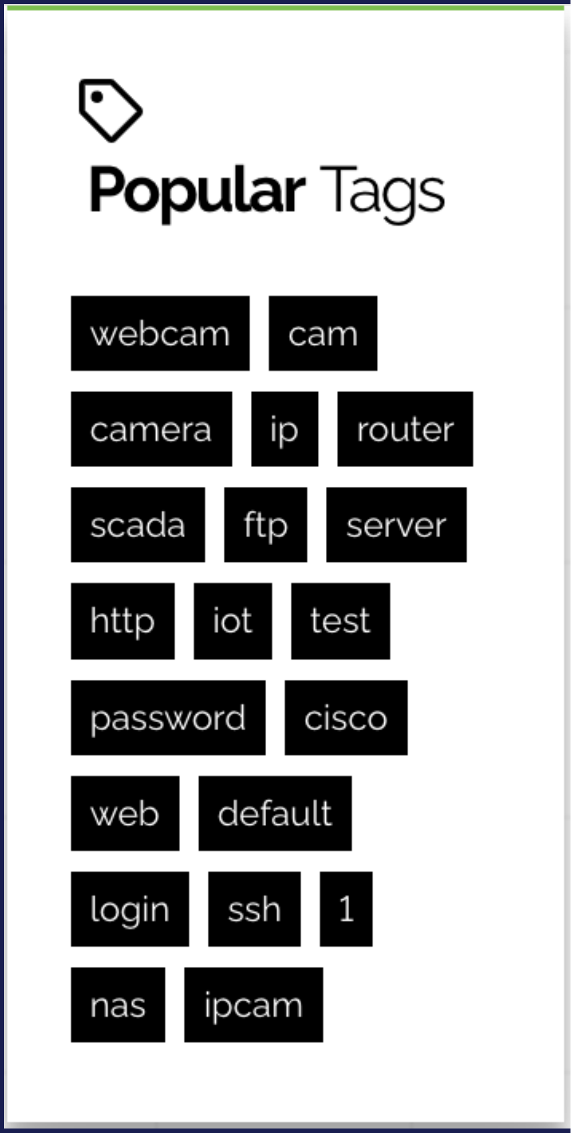


D. Laforenza, Internet of Things e Big Data, Corso DPO, FederPrivacy, 20 novembre 2019

Cos'è Shodan?

SHODAN

- è un motore di ricerca per estrarre informazioni sui dispositivi IoT connessi a Internet
- Classifica le informazioni critiche su vari dispositivi IoT trovati in rete:
  - ➢Telecamere (ad es. CCTV, webcam, baby monitor, …)
  - ➢Router e dispositivi di comunicazione
  - ➢Industrial control systems (ICS)
  - ➢SCADA (Supervisory Control and Data Acquisition)
  - ➢PLC (Programmable Logic Controller)
  - ➢DCS (Distributed Control System)
  - ➢………

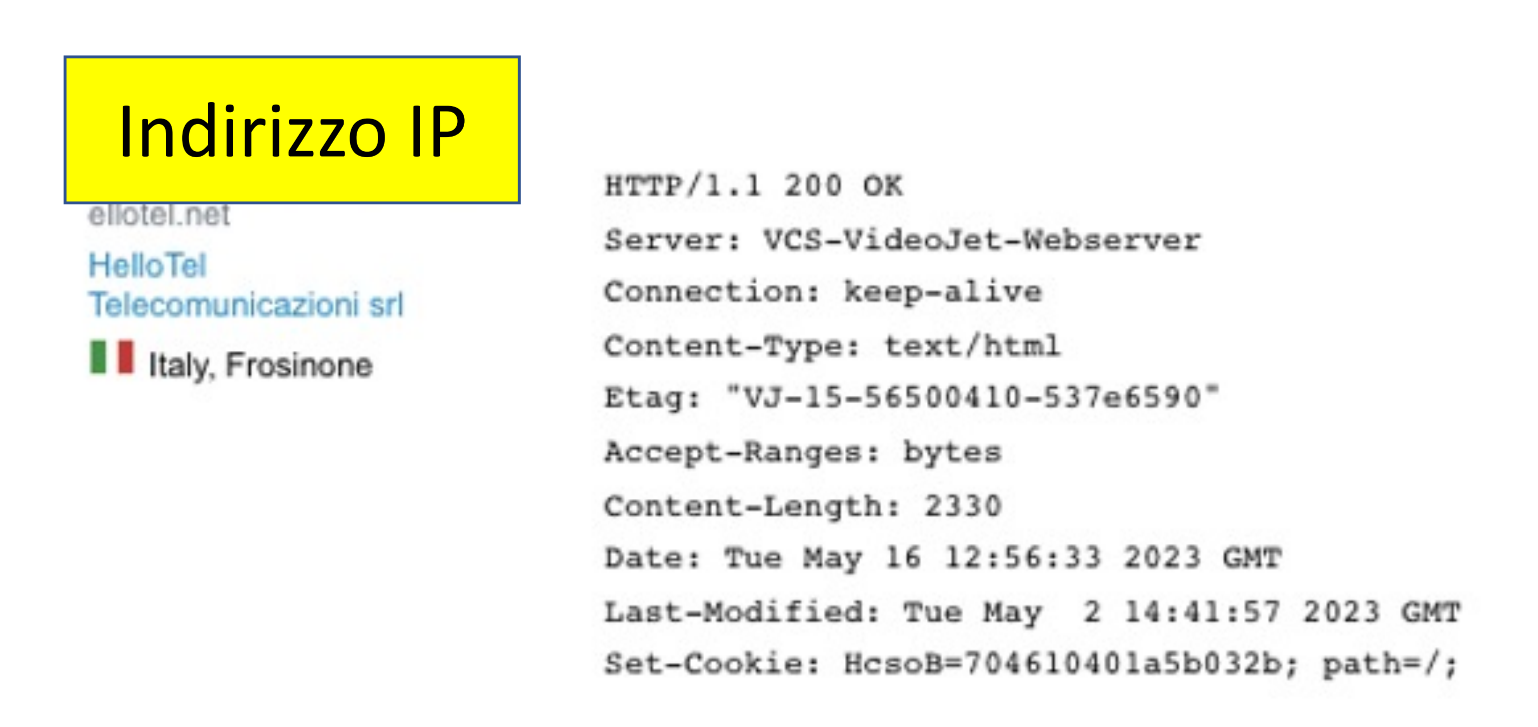


Popular Tags

webcam cam
camera ip router
scada ftp server
http iot test
password cisco
web default
login ssh 1
nas ipcam

Come funziona Shodan?

- Esegue la scansione di Internet usando gli indirizzi IP
  - ➢Indicizza tutte le informazioni ricevute da questi IP
  - ➢L'unità di base dei dati raccolti da Shodan è il banner
    - ▪ informazioni testuali che descrivono un servizio su un dispositivo
    - ▪ Il contenuto del banner varia notevolmente a seconda del tipo di servizio



Indirizzo IP

ellotel.net

HelloTel Telecomunicazioni srl

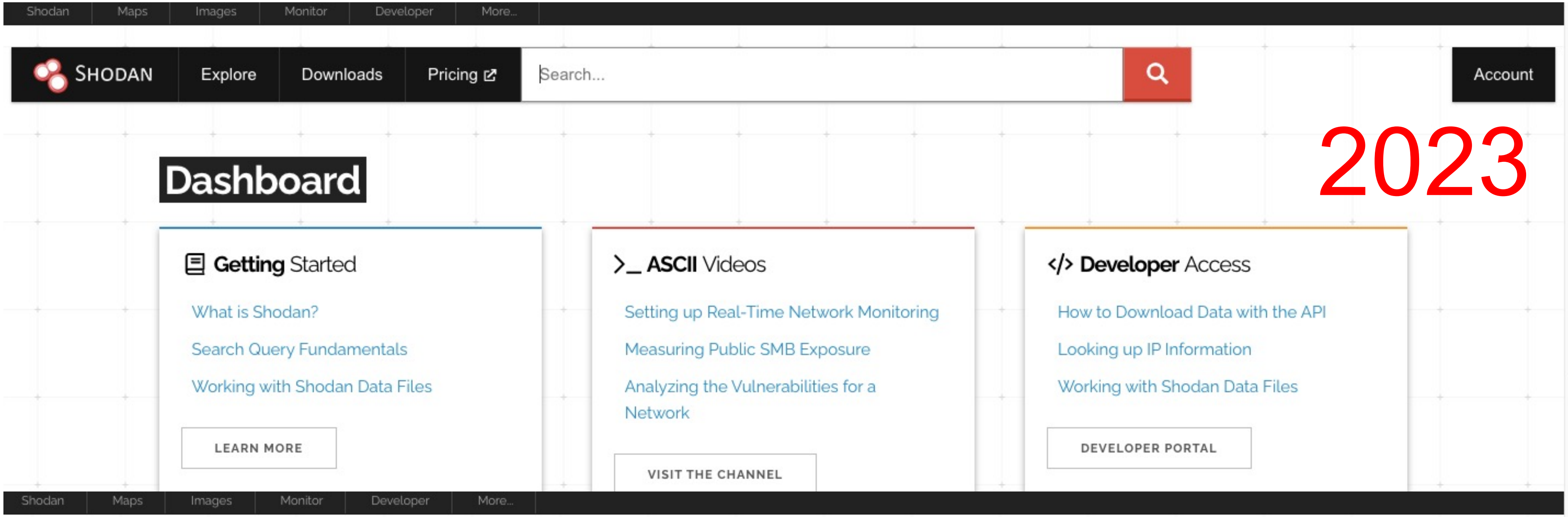
Italy, Frosinone

```
HTTP/1.1 200 OK
Server: VCS-VideoJet-Webserver
Connection: keep-alive
Content-Type: text/html
Etag: "VJ-15-56500410-537e6590"
Accept-Ranges: bytes
Content-Length: 2330
Date: Tue May 16 12:56:33 2023 GMT
Last-Modified: Tue May  2 14:41:57 2023 GMT
Set-Cookie: HcsoB=70461040la5b032b; path=/;
```

Nota: non tutti gli indirizzi IP restituiranno informazioni rilevanti

Come funziona Shodan?

- Oltre al banner vengono recuperate informazioni sui metadati dei dispositivi che includono:
  - ➢Nome dispositivo
  - ➢Indirizzo IP
  - ➢Posizione: paese, città o qualsiasi altro identificatore geografico in cui si trova il dispositivo
  - ➢Organizzazione di appartenenza
  - ➢Porte
  - ➢Login e password predefiniti
  - ➢Servizi e software in esecuzione sul dispositivo
  - ➢Marca e modello tecnologie web adottate
  - ➢……..



Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | Search... | Account

2023

Dashboard

Getting Started

- What is Shodan?
- Search Query Fundamentals
- Working with Shodan Data Files

LEARN MORE

>_ ASCII Videos

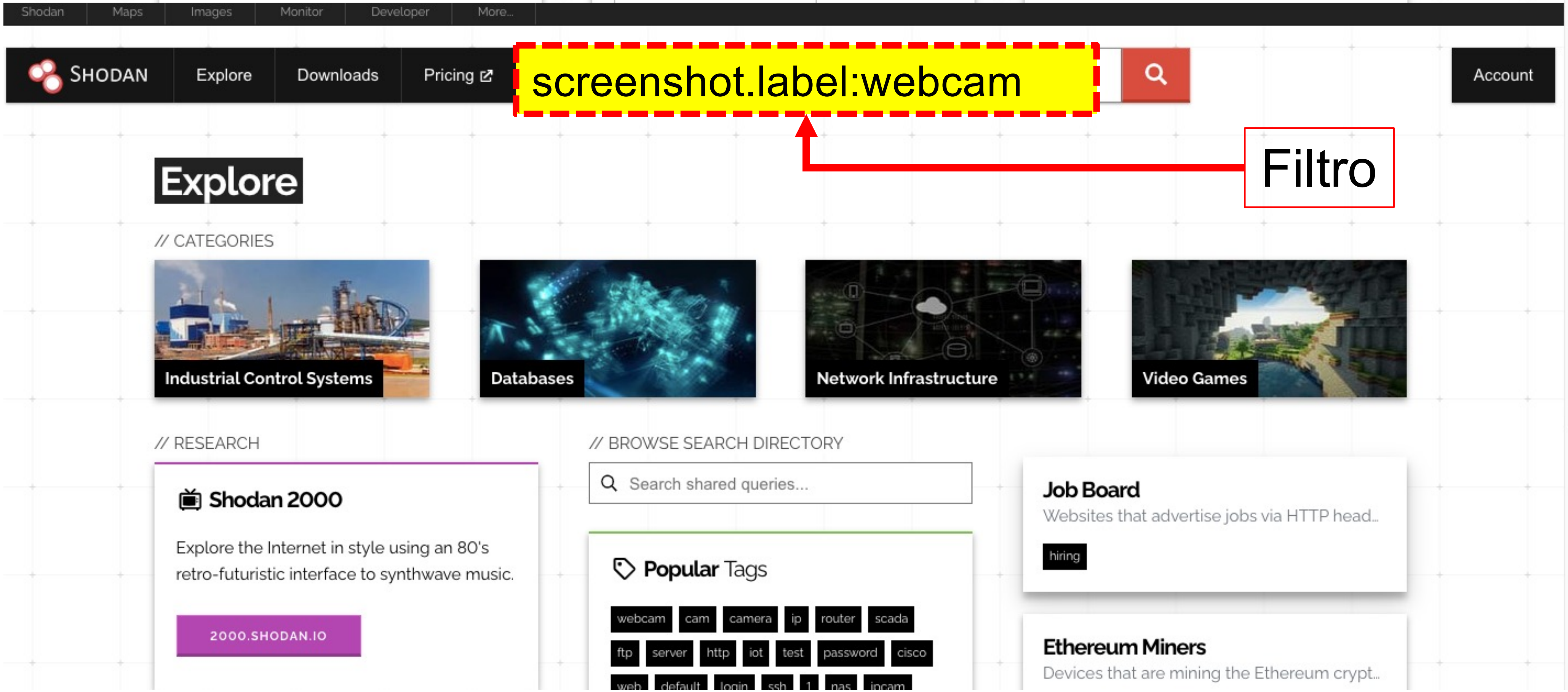
- Setting up Real-Time Network Monitoring
- Measuring Public SMB Exposure
- Analyzing the Vulnerabilities for a Network

VISIT THE CHANNEL

</> Developer Access

- How to Download Data with the API
- Looking up IP Information
- Working with Shodan Data Files

DEVELOPER PORTAL



Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | screenshot.label:webcam | Account

Filtro

Explore

// CATEGORIES

// RESEARCH

Shodan 2000

Explore the Internet in style using an 80's retro-futuristic interface to synthwave music.

2000.SHODAN.IO

// BROWSE SEARCH DIRECTORY

Search shared queries...

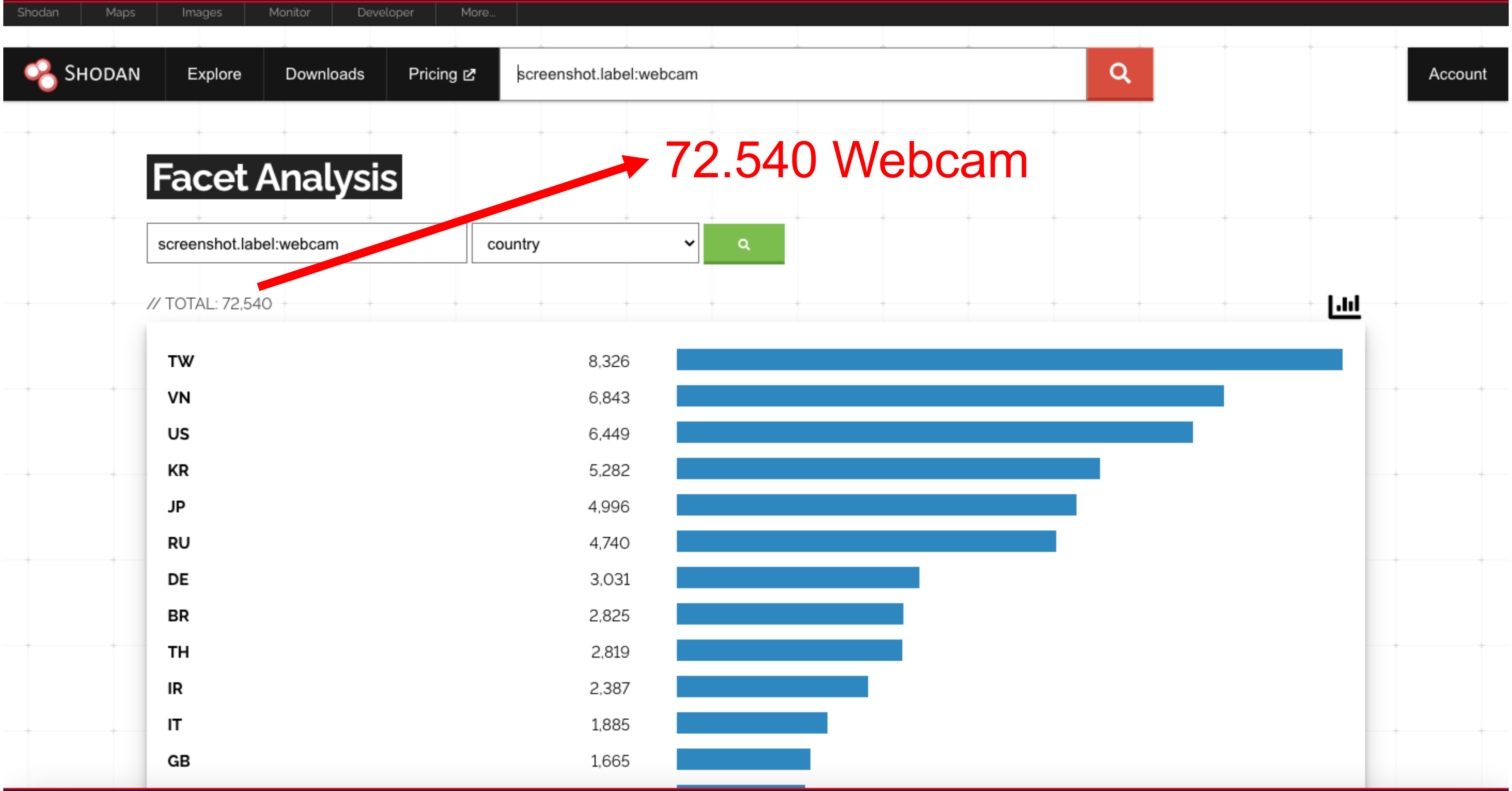
Popular Tags

webcam cam camera ip router scada
ftp server http iot test password cisco
web default login ssh 1 nas ipcam

Job Board
Websites that advertise jobs via HTTP head...
hiring

Ethereum Miners
Devices that are mining the Ethereum crypt...

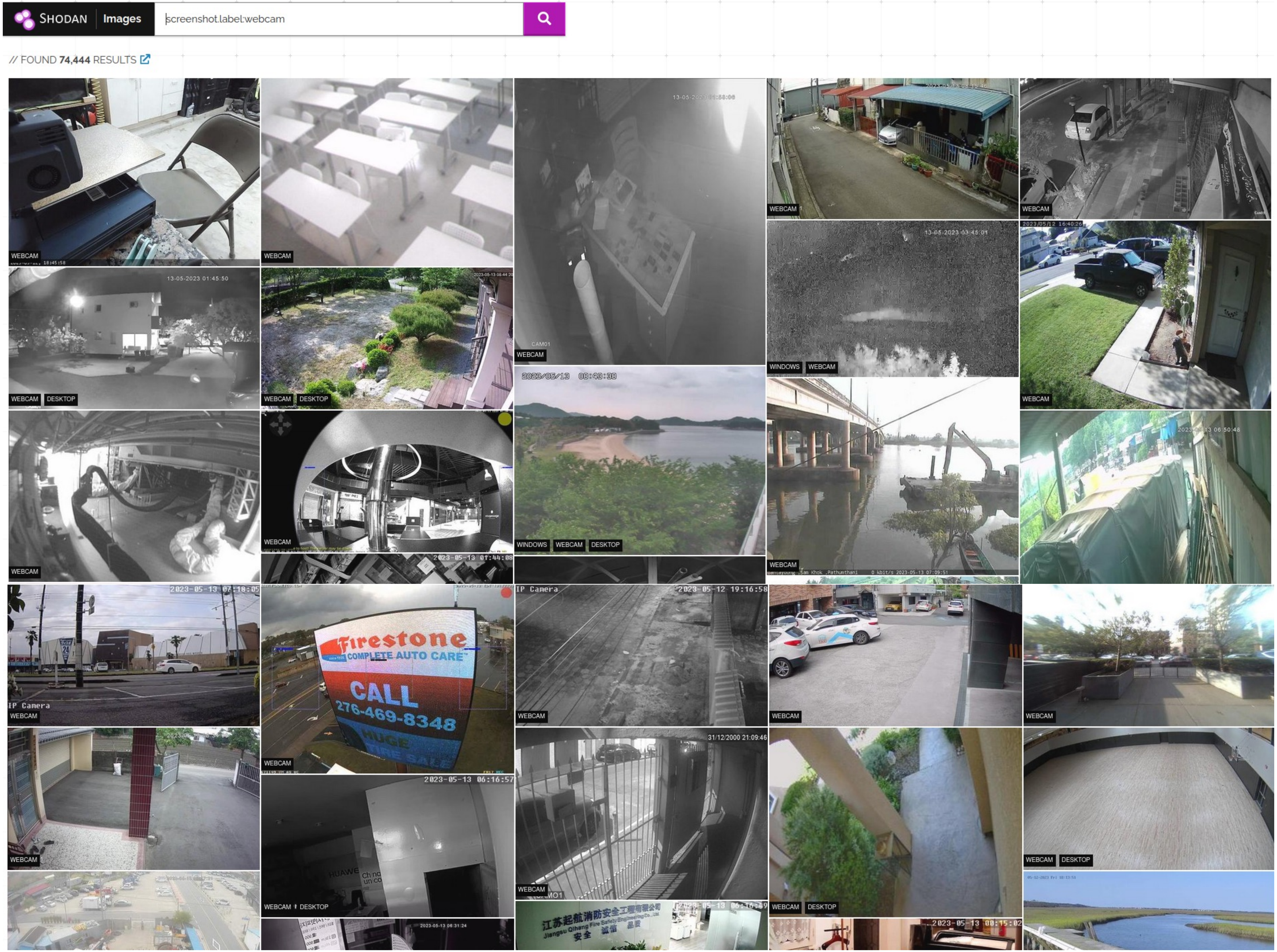
Filtro: screenshot.label:webcam



72.540 Webcam

// TOTAL: 72,540

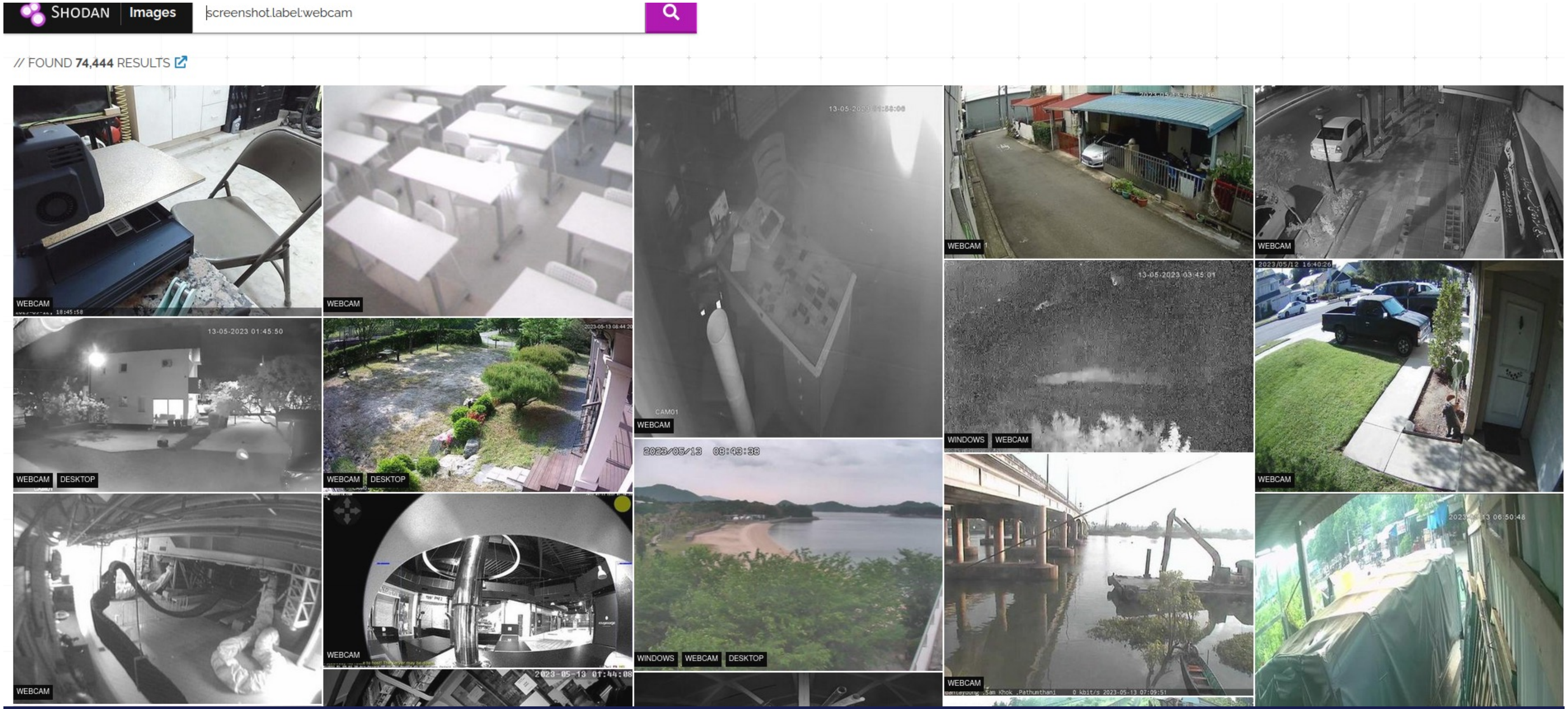
TW	8,326
VN	6,843
US	6,449
KR	5,282
JP	4,996
RU	4,740
DE	3,031
BR	2,825
TH	2,819
IR	2,387
IT	1,885
GB	1,665



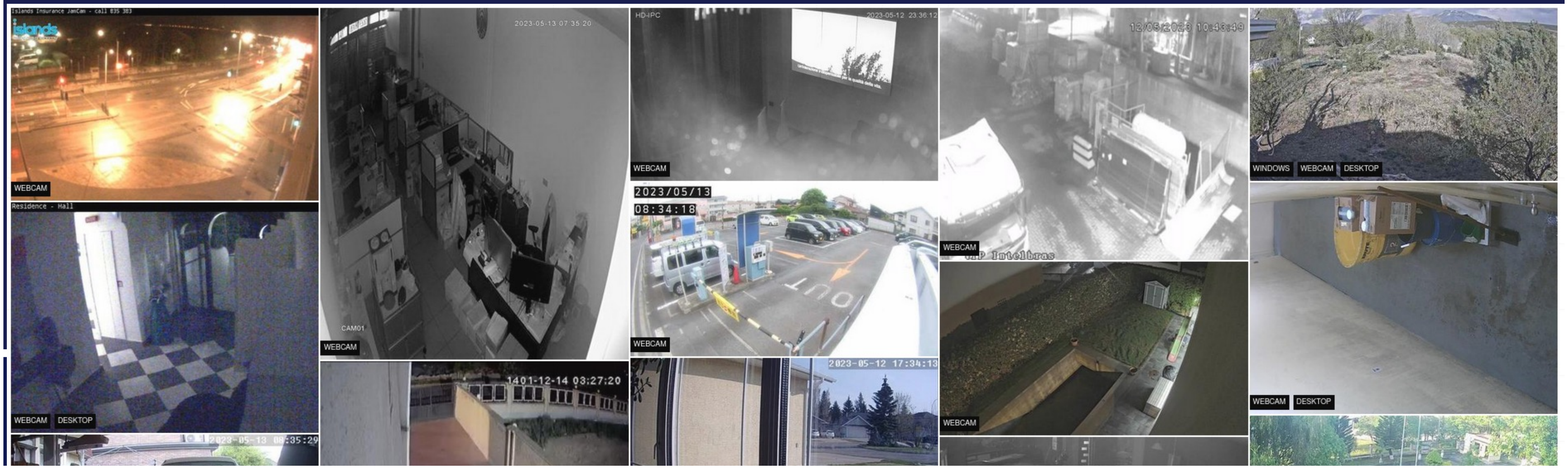
SHODAN Images

screenshot.label:webcam

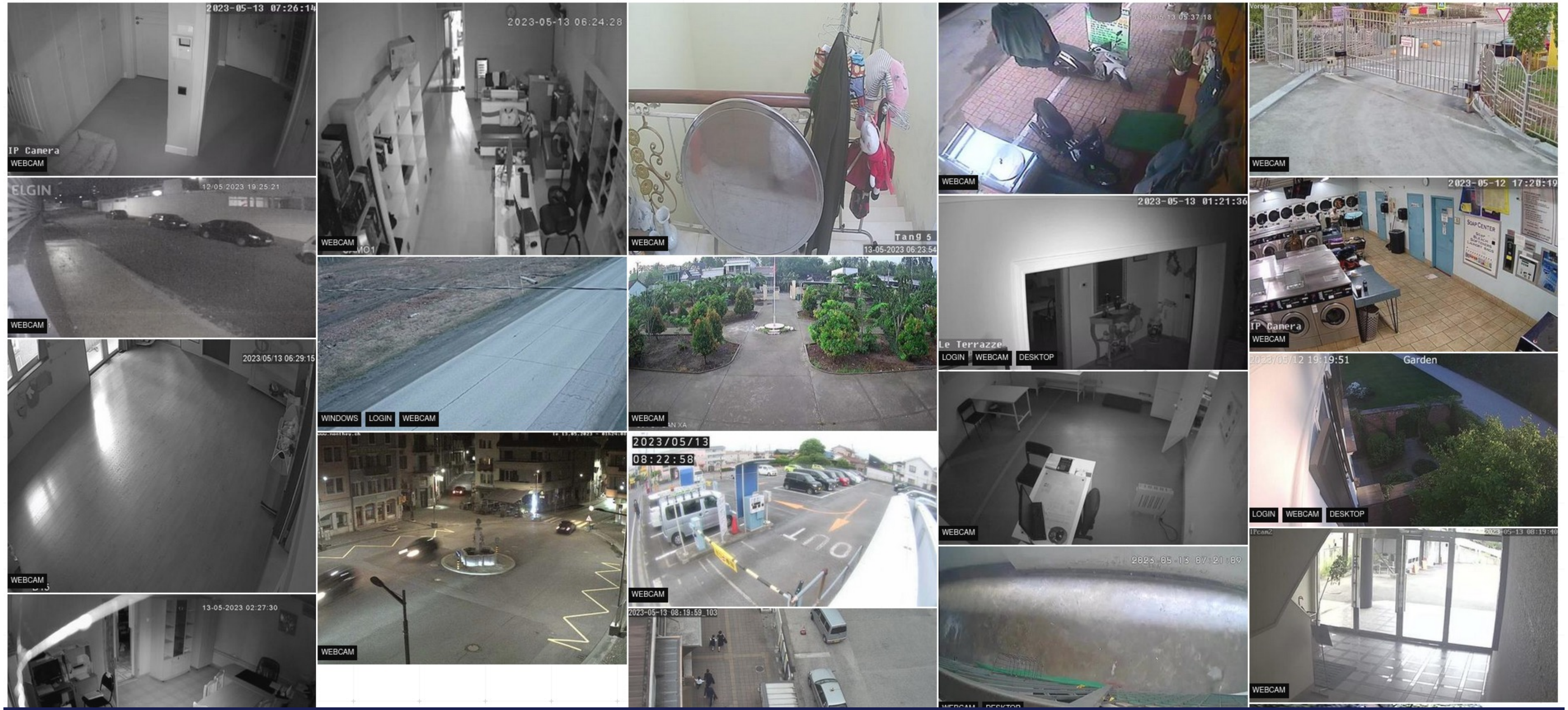
// FOUND **74,444** RESULTS



SHODAN
Images
screenshot.label:webcam
// FOUND 74,444 RESULTS
WEBCAM
WEBCAM
13-05-2023 01:45:50
WEBCAM
DESKTOP
2023-05-13 08:44:20
WEBCAM
DESKTOP
WEBCAM
WEBCAM
2023-05-13 01:44:08
CAM01
WEBCAM
2023/05/13 08:43:38
WINDOWS
WEBCAM
DESKTOP
WEBCAM
13-05-2023 03:45:01
WINDOWS
WEBCAM
WEBCAM
WEBCAM
2023/05/12 16:40:26
WEBCAM
WEBCAM

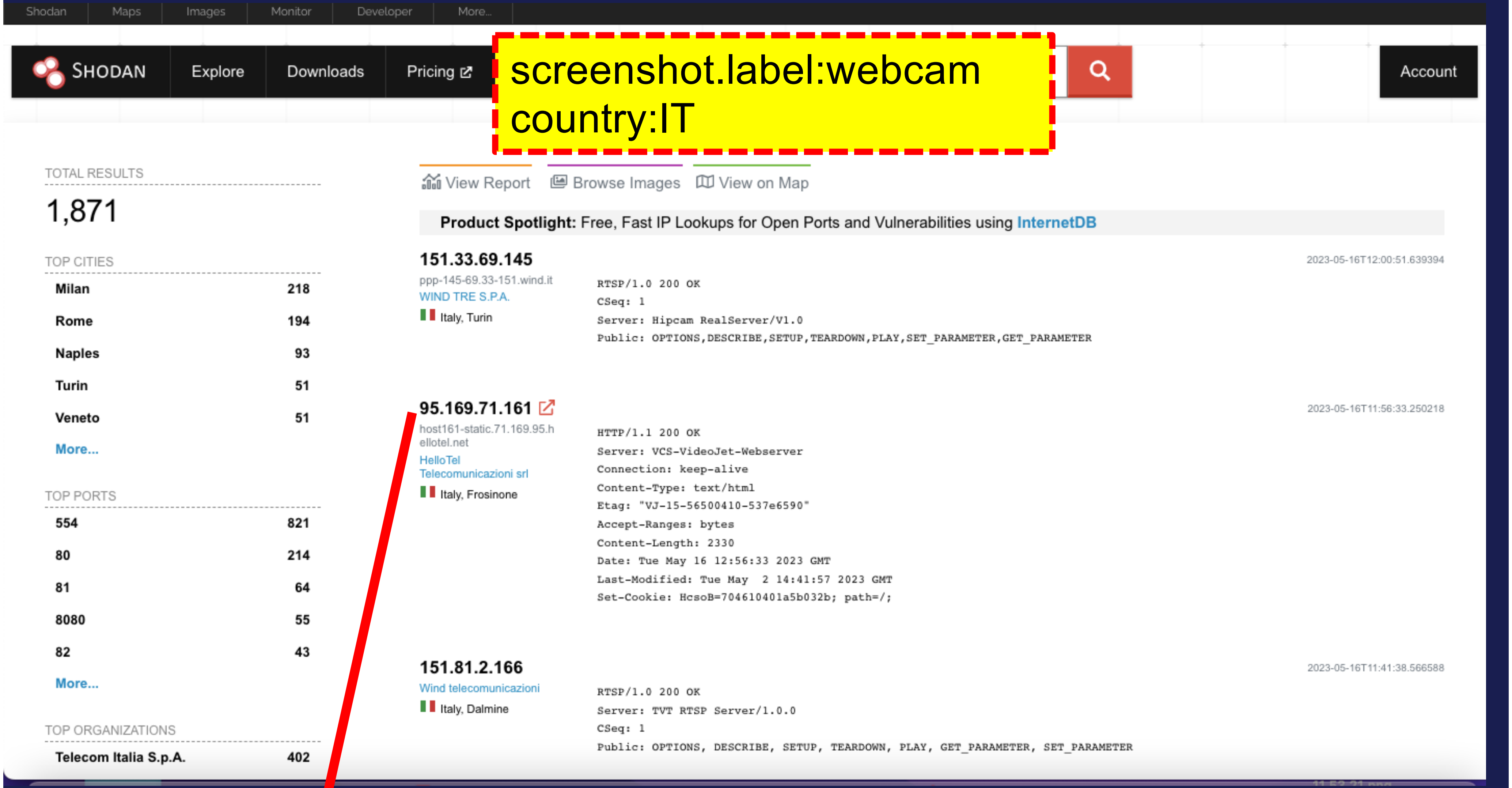


Islands Insurance JamCam - call 835 383
islands
WEBCAM
Residence - Hall
WEBCAM
DESKTOP
2023-05-13 08:35:29
2023-05-13 07:35:20
CAM01
WEBCAM
1401-12-14 03:27:20
HD-IPC
2023-05-12 23:36:12
WEBCAM
2023/05/13
08:34:18
OUT
WEBCAM
2023-05-12 17:34:13
12/05/2023 10:43:49
WEBCAM
Intelbras
WEBCAM
WINDOWS
WEBCAM
DESKTOP
WEBCAM
DESKTOP



AVVERTENZA: non è detto che le webcam «aperte» costituiscano un problema di privacy

- i legittimi utilizzatori, per molteplici interessi personali, potrebbero avere intenzionalmente fatto in modo che le webcam siano accessibili da chiunque/dovunque



screenshot.label:webcam country:IT

TOTAL RESULTS

1,871

TOP CITIES

Milan	218
Rome	194
Naples	93
Turin	51
Veneto	51
More...	

TOP PORTS

554	821
80	214
81	64
8080	55
82	43
More...	

TOP ORGANIZATIONS

Telecom Italia S.p.A.	402

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

151.33.69.145
ppp-145-69.33-151.wind.it
WIND TRE S.P.A.
Italy, Turin

2023-05-16T12:00:51.639394

```
RTSP/1.0 200 OK
CSeq: 1
Server: Hipcam RealServer/V1.0
Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
```

95.169.71.161
host161-static.71.169.95.hellotel.net
HelloTel Telecomunicazioni srl
Italy, Frosinone

2023-05-16T11:56:33.250218

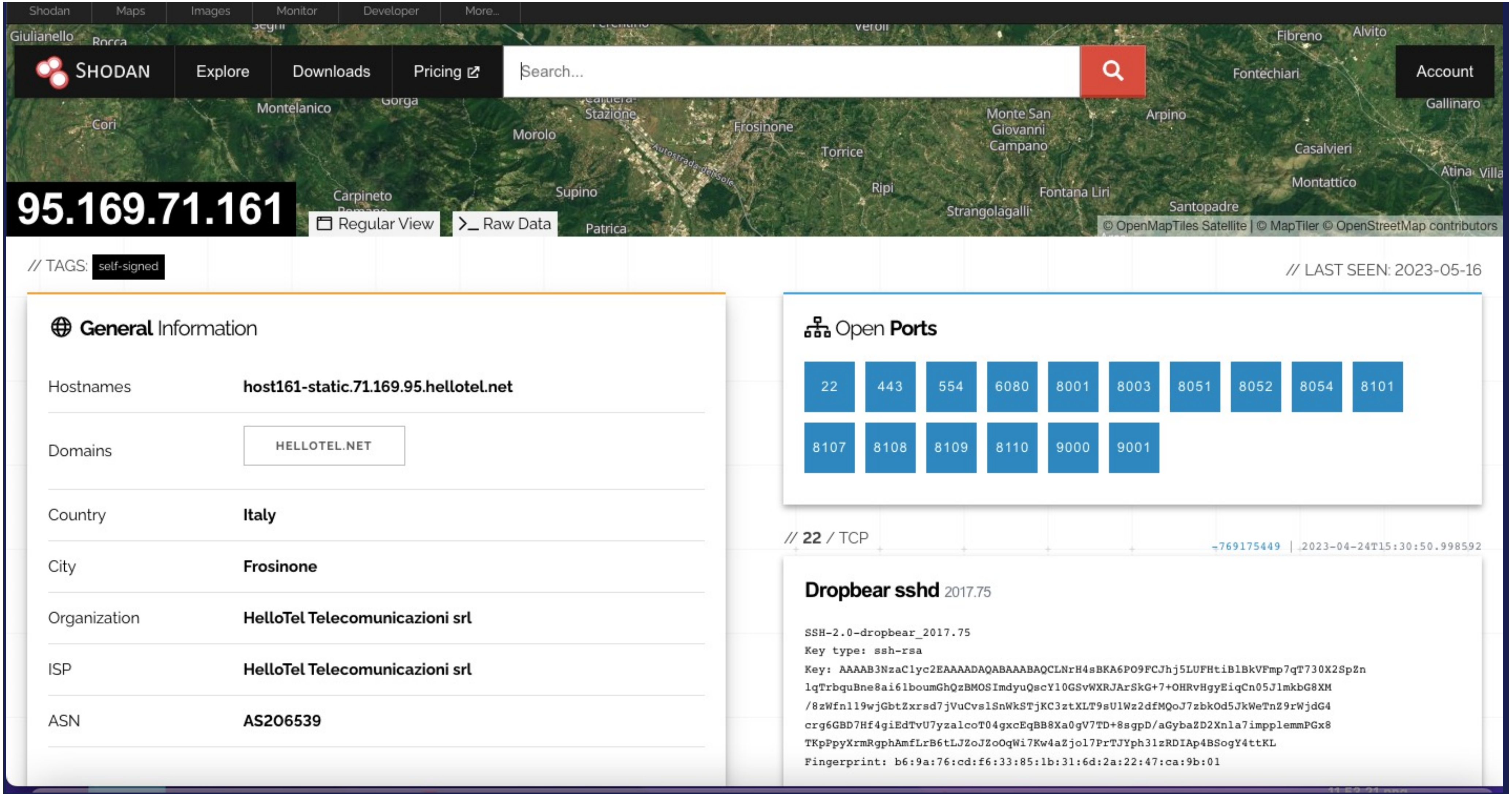
```
HTTP/1.1 200 OK
Server: VCS-VideoJet-Webserver
Connection: keep-alive
Content-Type: text/html
Etag: "VJ-15-56500410-537e6590"
Accept-Ranges: bytes
Content-Length: 2330
Date: Tue May 16 12:56:33 2023 GMT
Last-Modified: Tue May  2 14:41:57 2023 GMT
Set-Cookie: HcsoB=704610401a5b032b; path=/;
```

151.81.2.166
Wind telecomunicazioni
Italy, Dalmine

2023-05-16T11:41:38.566588

```
RTSP/1.0 200 OK
Server: TVT RTSP Server/1.0.0
CSeq: 1
Public: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, GET_PARAMETER, SET_PARAMETER
```

Cliccandoci sopra



95.169.71.161

// TAGS: self-signed

// LAST SEEN: 2023-05-16

General Information

Hostnames	**host161-static.71.169.95.hellotel.net**
Domains	HELLOTEL.NET
Country	**Italy**
City	**Frosinone**
Organization	**HelloTel Telecomunicazioni srl**
ISP	**HelloTel Telecomunicazioni srl**
ASN	**AS206539**

Open Ports

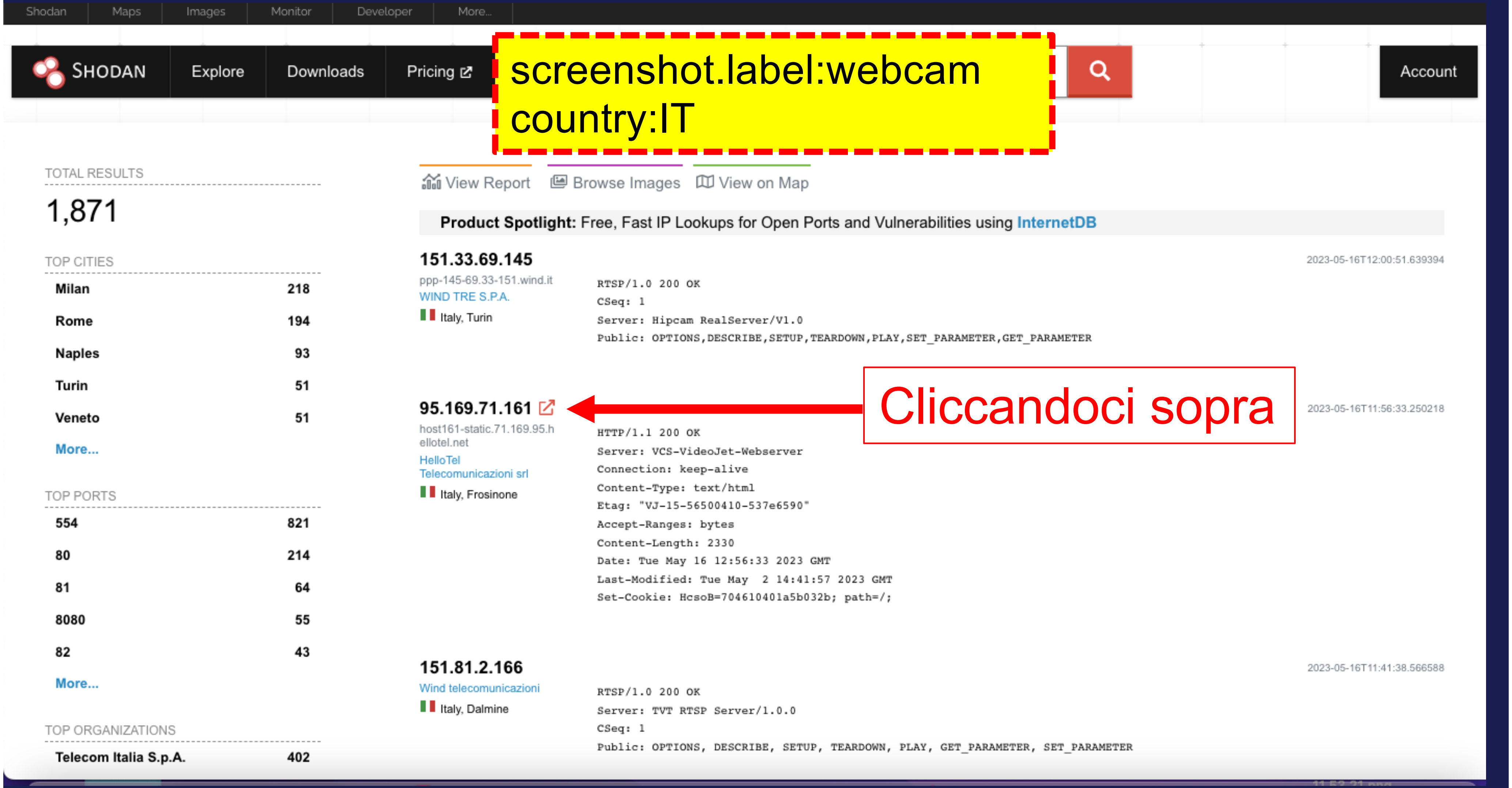
22	443	554	6080	8001	8003	8051	8052	8054	8101
8107	8108	8109	8110	9000	9001				

// **22** / TCP

-769175449 | 2023-04-24T15:30:50.998592

Dropbear sshd 2017.75

```
SSH-2.0-dropbear_2017.75
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCLNrH4sBKA6PO9FCJhj5LUFHtiBlBkVFmp7qT730X2SpZn
lqTrbquBne8ai6lboumGhQzBMOSImdyuQscYl0GSvWXRJArSkG+7+OHRvHgyEiqCn05JlmkbG8XM
/8zWfnl19wjGbtZxrsd7jVuCvslSnWkSTjKC3ztXLT9sUlWz2dfMQoJ7zbkOd5JkWeTnZ9rWjdG4
crg6GBD7Hf4giEdTvU7yzalcoT04gxcEqBB8Xa0gV7TD+8sgpD/aGybaZD2Xnla7impplemmPGx8
TKpPpyXrmRgphAmfLrB6tLJZoJZoOqWi7Kw4aZjol7PrTJYph3lzRDIAp4BSogY4ttKL
Fingerprint: b6:9a:76:cd:f6:33:85:1b:31:6d:2a:22:47:ca:9b:01
```



screenshot.label:webcam country:IT

Cliccandoci sopra

TOTAL RESULTS

1,871

TOP CITIES

Milan	218
Rome	194
Naples	93
Turin	51
Veneto	51
More...	

TOP PORTS

554	821
80	214
81	64
8080	55
82	43
More...	

TOP ORGANIZATIONS

Telecom Italia S.p.A.	402

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

151.33.69.145
ppp-145-69.33-151.wind.it
WIND TRE S.P.A.
Italy, Turin

2023-05-16T12:00:51.639394

```
RTSP/1.0 200 OK
CSeq: 1
Server: Hipcam RealServer/V1.0
Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
```

95.169.71.161
host161-static.71.169.95.hellotel.net
HelloTel Telecomunicazioni srl
Italy, Frosinone

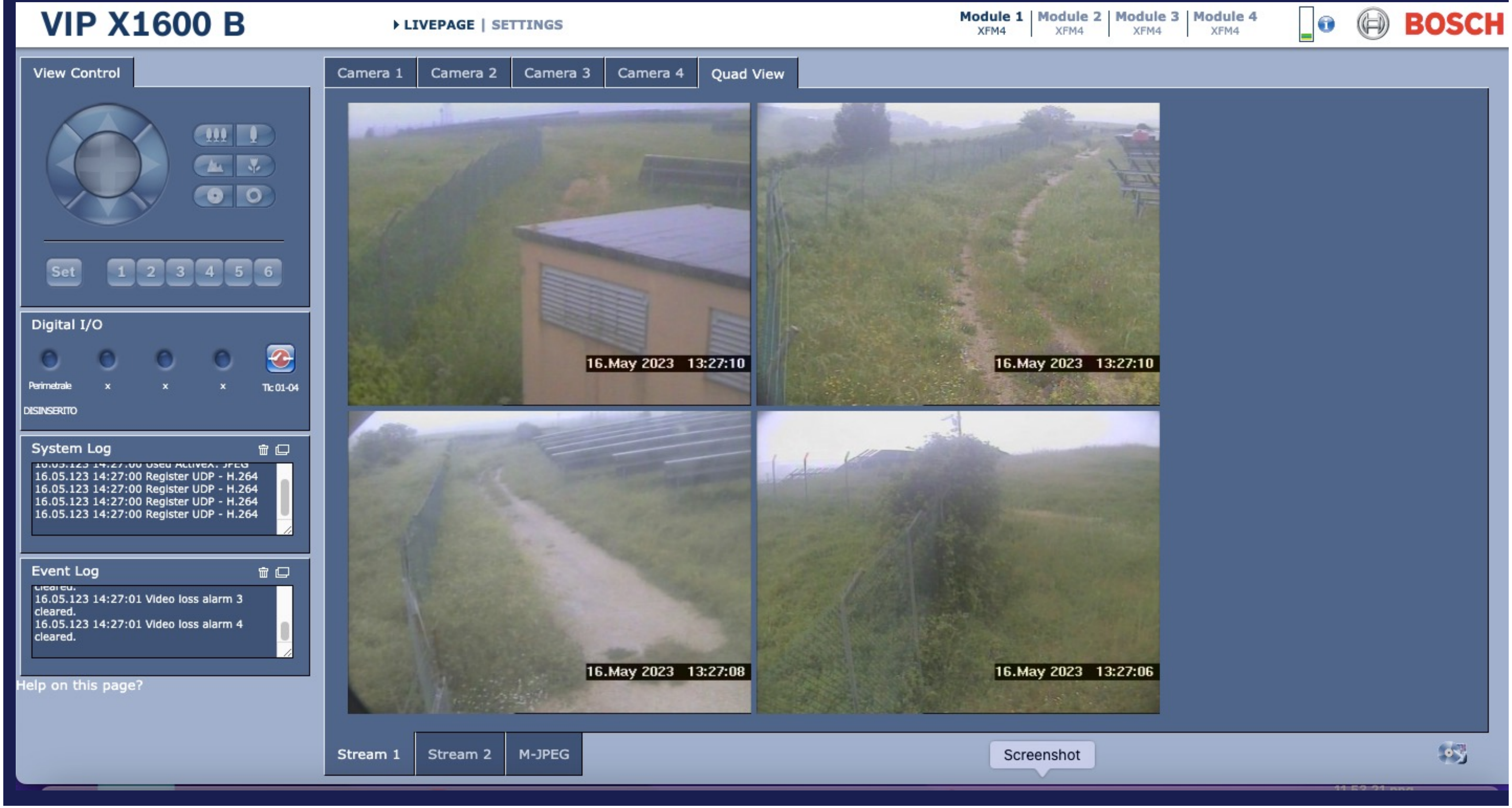
2023-05-16T11:56:33.250218

```
HTTP/1.1 200 OK
Server: VCS-VideoJet-Webserver
Connection: keep-alive
Content-Type: text/html
Etag: "VJ-15-56500410-537e6590"
Accept-Ranges: bytes
Content-Length: 2330
Date: Tue May 16 12:56:33 2023 GMT
Last-Modified: Tue May  2 14:41:57 2023 GMT
Set-Cookie: HcsoB=704610401a5b032b; path=/;
```

151.81.2.166
Wind telecomunicazioni
Italy, Dalmine

2023-05-16T11:41:38.566588

```
RTSP/1.0 200 OK
Server: TVT RTSP Server/1.0.0
CSeq: 1
Public: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, GET_PARAMETER, SET_PARAMETER
```



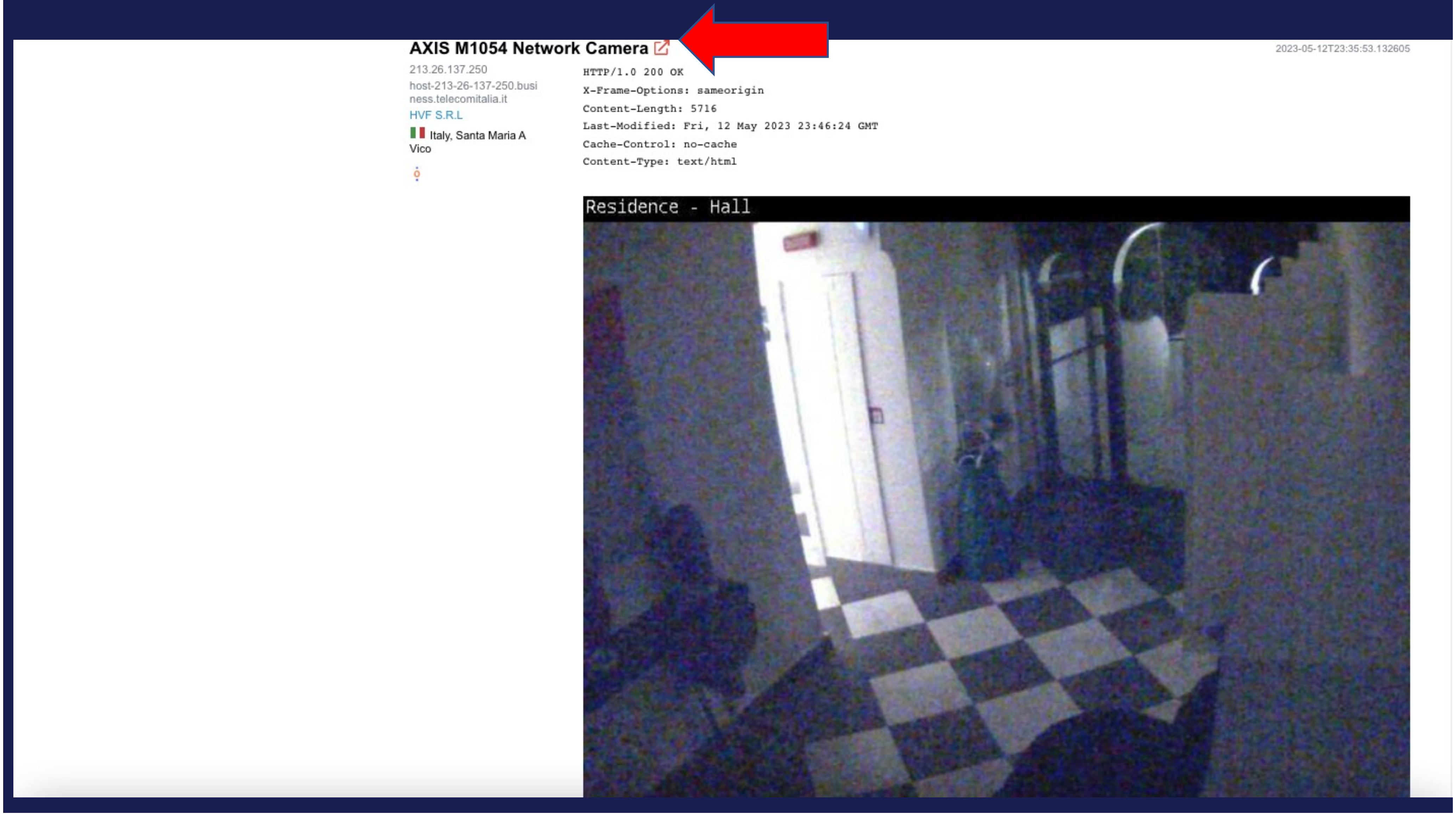
System Log

```
16.05.123 14:27:00 Used ActiveX: JPEG
16.05.123 14:27:00 Register UDP - H.264
16.05.123 14:27:00 Register UDP - H.264
16.05.123 14:27:00 Register UDP - H.264
16.05.123 14:27:00 Register UDP - H.264
```

Event Log

```
cleared.
16.05.123 14:27:01 Video loss alarm 3
cleared.
16.05.123 14:27:01 Video loss alarm 4
cleared.
```

Italy, Santa Maria a Vico



AXIS M1054 Network Camera

2023-05-12T23:35:53.132605

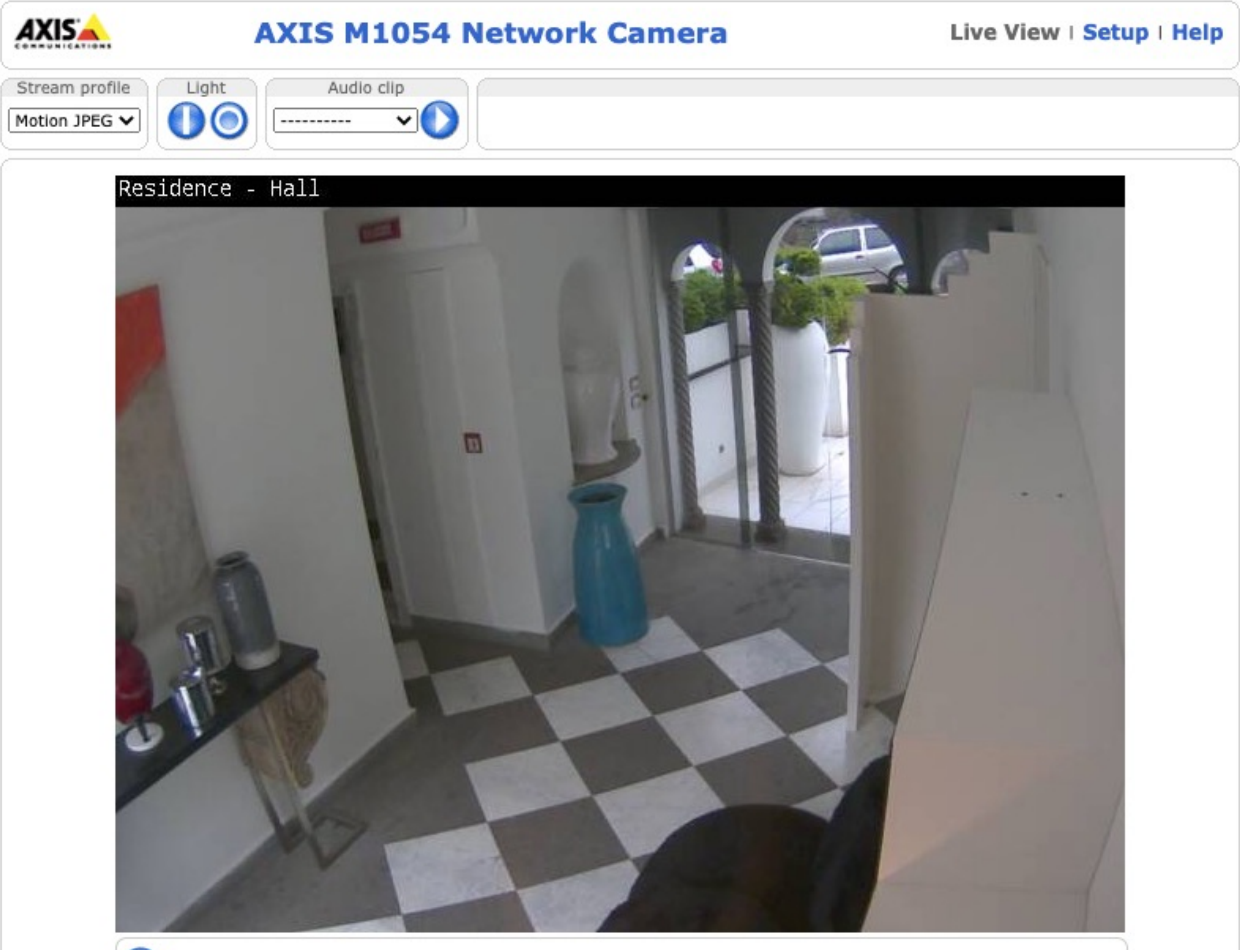
213.26.137.250

host-213-26-137-250.business.telecomitalia.it

HVF S.R.L

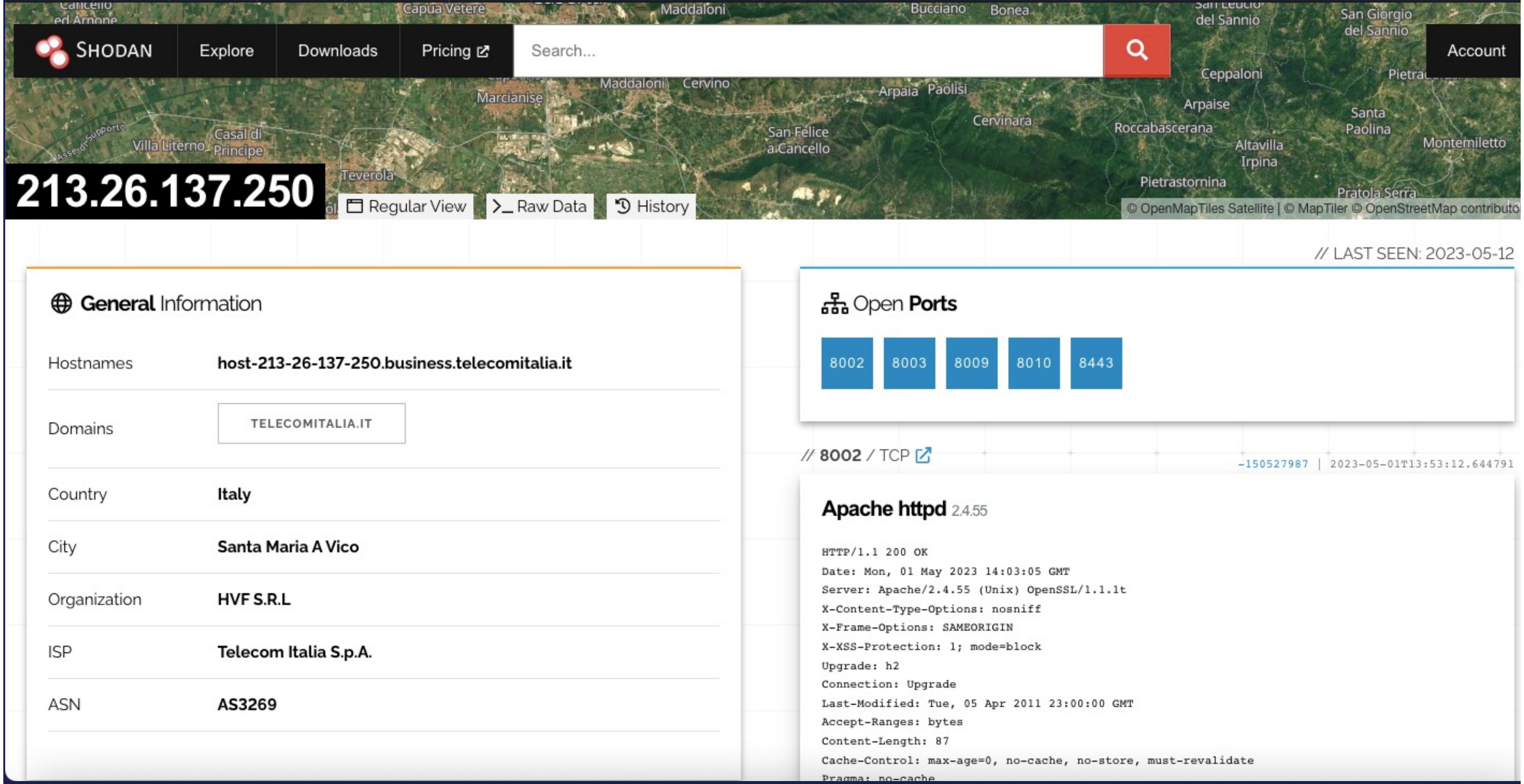
Italy, Santa Maria A Vico

```
HTTP/1.0 200 OK
X-Frame-Options: sameorigin
Content-Length: 5716
Last-Modified: Fri, 12 May 2023 23:46:24 GMT
Cache-Control: no-cache
Content-Type: text/html
```



AXIS M1054 Network Camera

Italy, Santa Maria a Vico



213.26.137.250

// LAST SEEN: 2023-05-12

General Information

Hostnames	host-213-26-137-250.business.telecomitalia.it
Domains	TELECOMITALIA.IT
Country	Italy
City	Santa Maria A Vico
Organization	HVF S.R.L
ISP	Telecom Italia S.p.A.
ASN	AS3269

Open Ports

8002 8003 8009 8010 8443

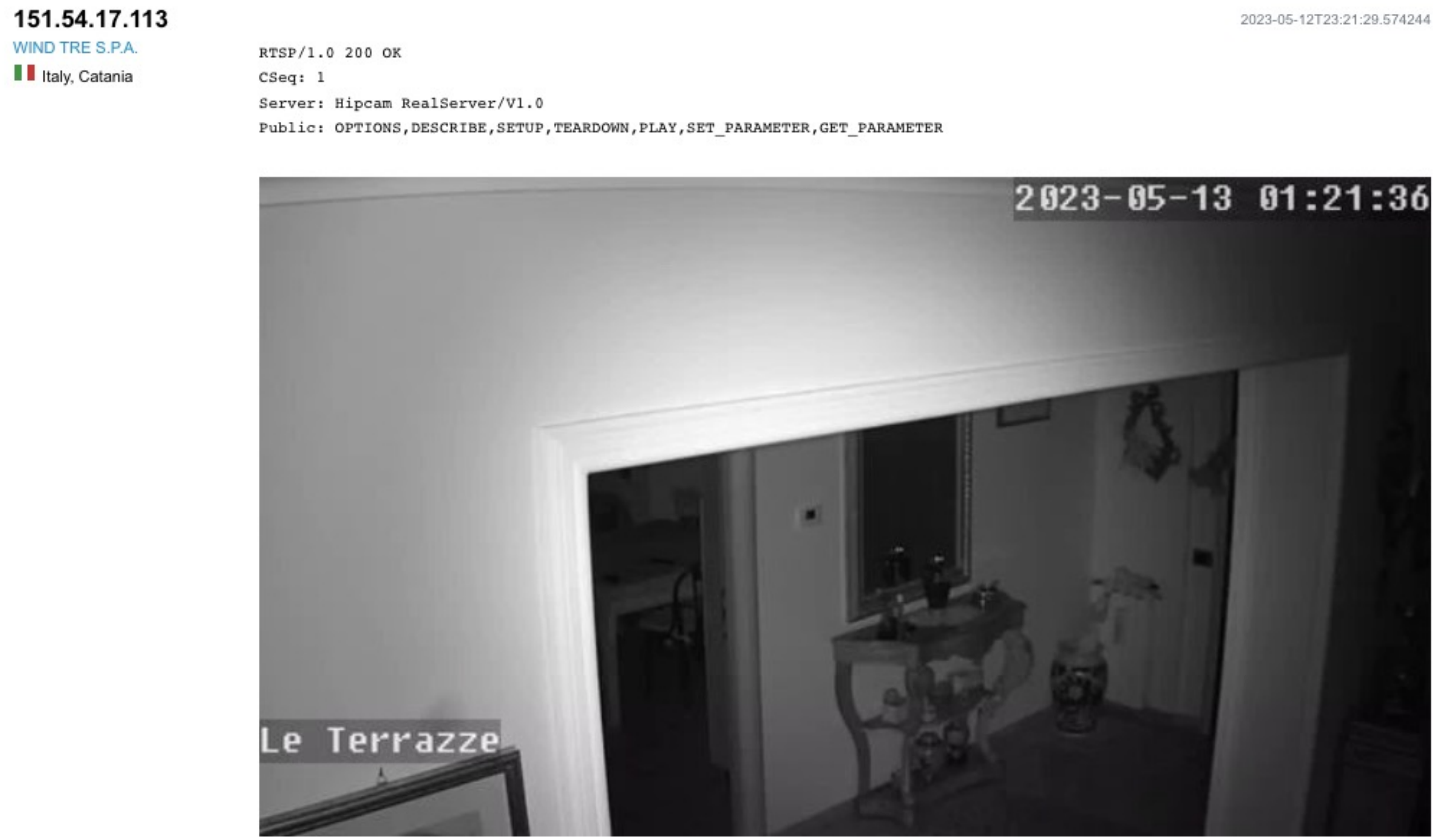
// 8002 / TCP

-150527987 | 2023-05-01T13:53:12.644791

Apache httpd 2.4.55

```
HTTP/1.1 200 OK
Date: Mon, 01 May 2023 14:03:05 GMT
Server: Apache/2.4.55 (Unix) OpenSSL/1.1.1t
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Upgrade: h2
Connection: Upgrade
Last-Modified: Tue, 05 Apr 2011 23:00:00 GMT
Accept-Ranges: bytes
Content-Length: 87
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Pragma: no-cache
```

Italy, Catania



151.54.17.113

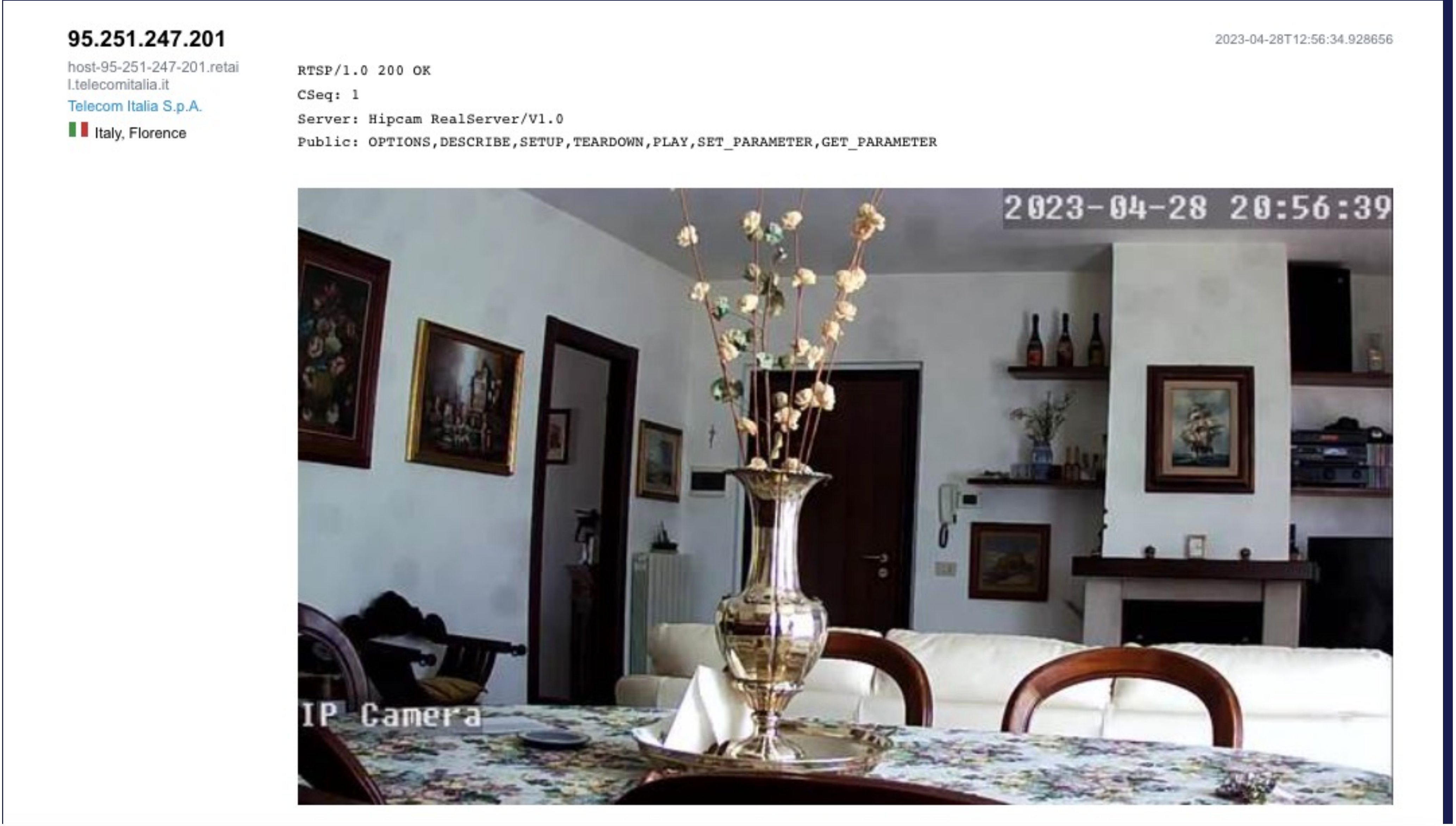
WIND TRE S.P.A.

Italy, Catania

2023-05-12T23:21:29.574244

```
RTSP/1.0 200 OK
CSeq: 1
Server: Hipcam RealServer/V1.0
Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
```

Italy, Florence



95.251.247.201

host-95-251-247-201.retail.telecomitalia.it

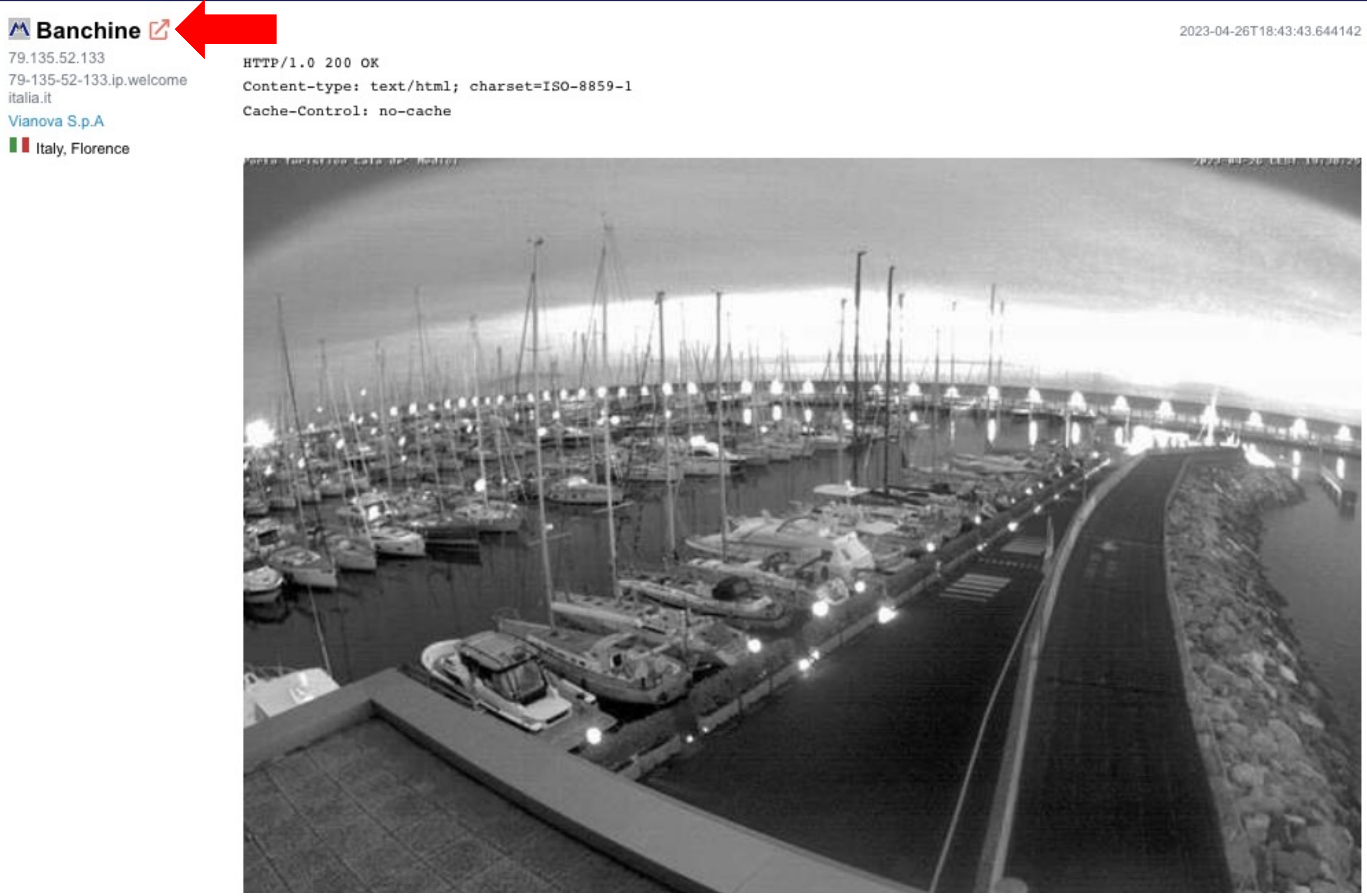
Telecom Italia S.p.A.

Italy, Florence

2023-04-28T12:56:34.928656

```
RTSP/1.0 200 OK
CSeq: 1
Server: Hipcam RealServer/V1.0
Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
```

Italy, Florence (Castiglioncello, Porto turistico Cala de' Medici)



Banchine

79.135.52.133

79-135-52-133.ip.welcomeitalia.it

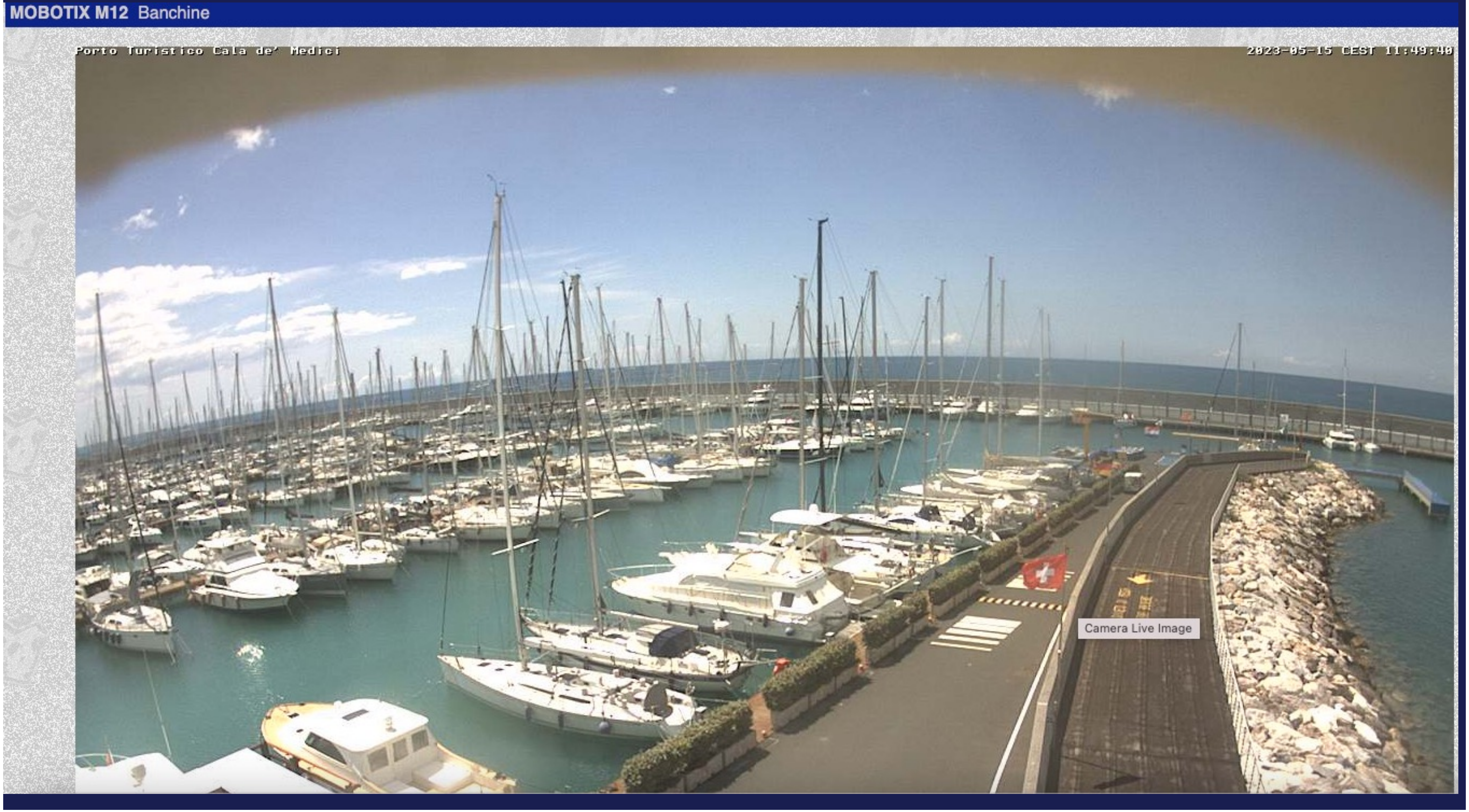
Vianova S.p.A

Italy, Florence

2023-04-26T18:43:43.644142

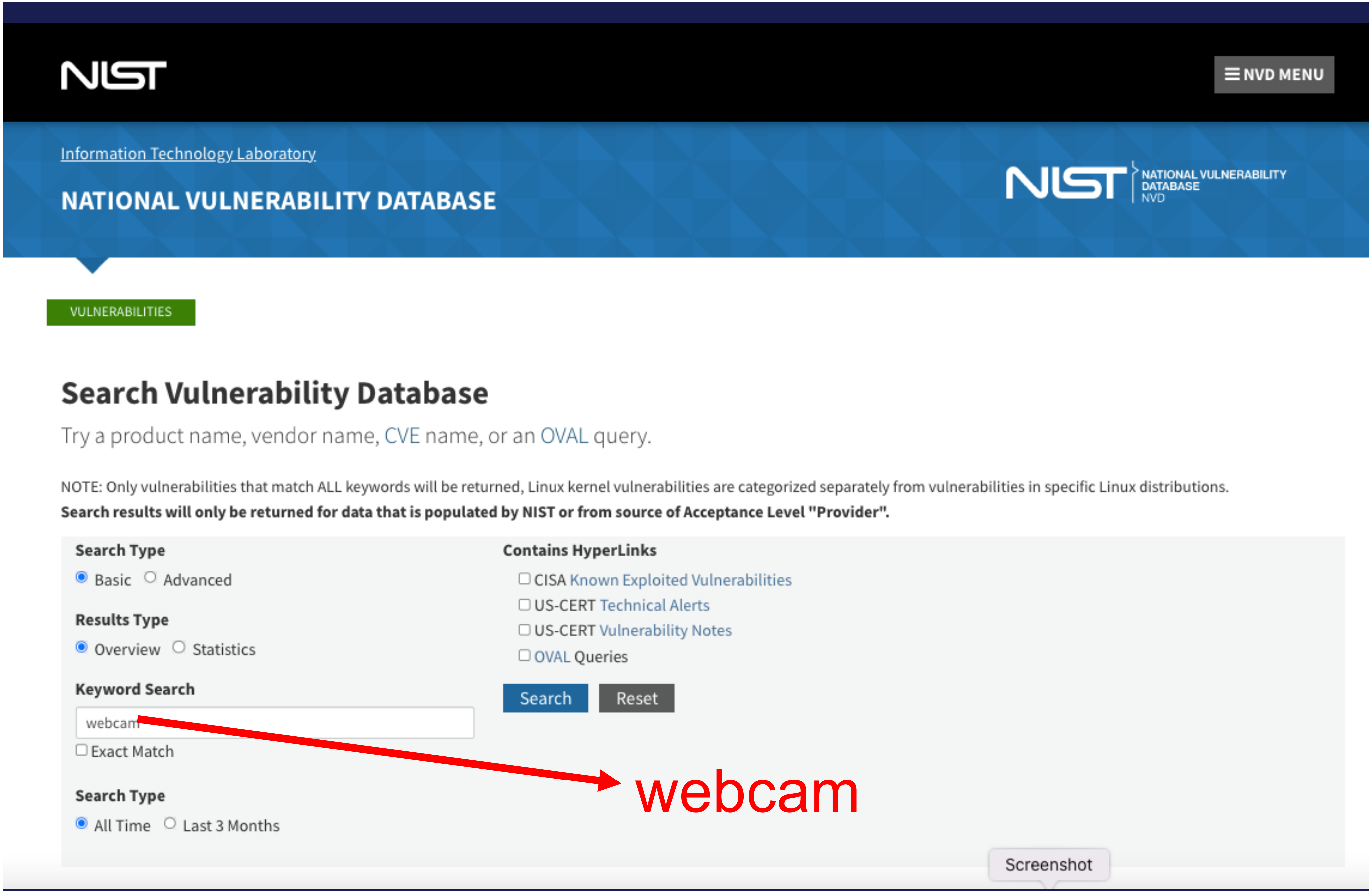
```
HTTP/1.0 200 OK
Content-type: text/html; charset=ISO-8859-1
Cache-Control: no-cache
```

Italy, Florence (Castiglioncello, Porto turistico Cala de' Medici)



Common Vulnerabilities and Exposures (CVE)

- NIST NVD (National Vulnerability Database)
  - https://nvd.nist.gov/vuln/search
- CISA
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- FIRST
  - https://www.first.org/epss/ and here
  - https://www.first.org/epss/data_stats



NIST
≡ NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.

Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type

● Basic ○ Advanced

Results Type

● Overview ○ Statistics

Keyword Search

webcam

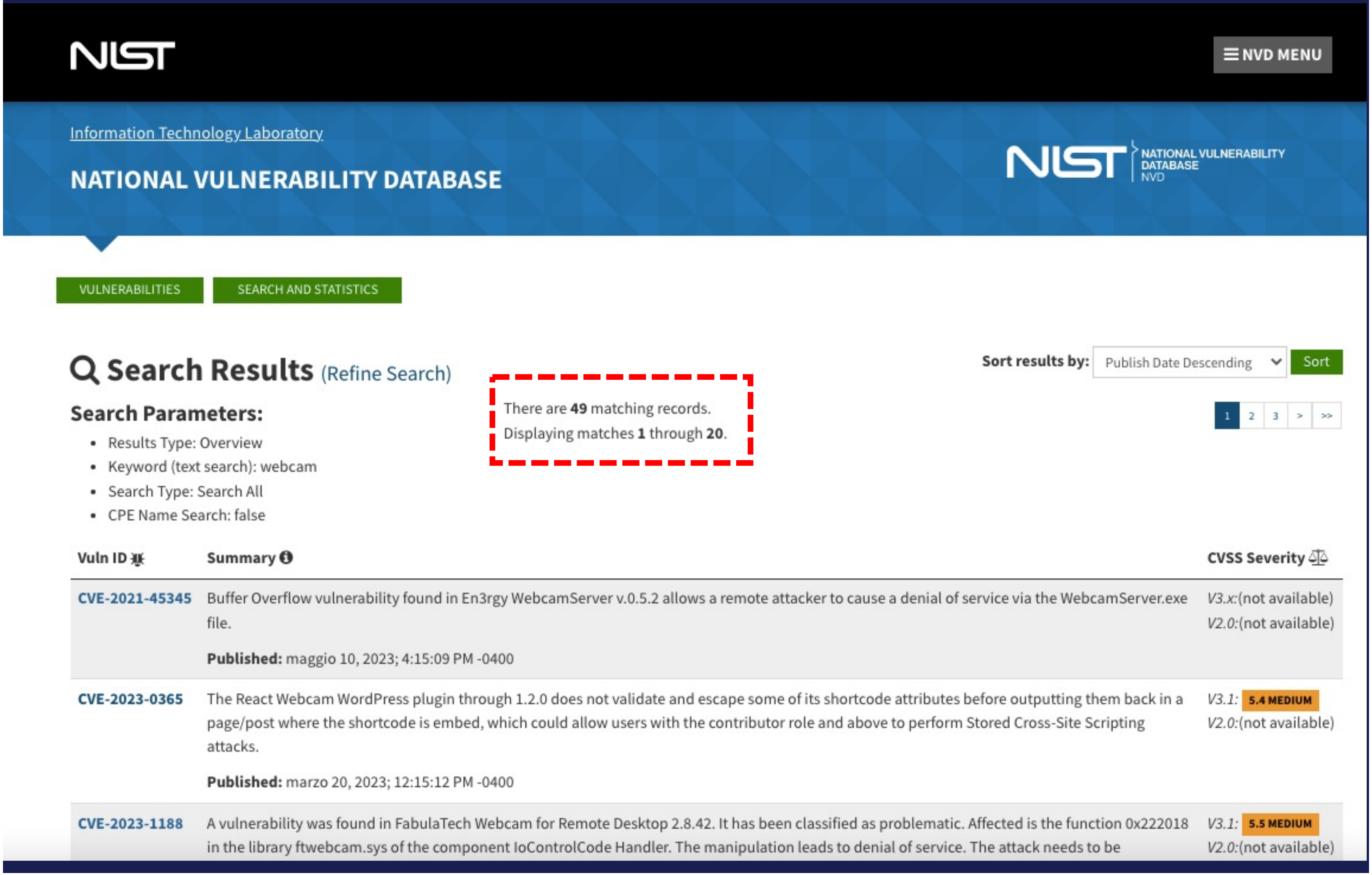
□ Exact Match

Search Type

● All Time ○ Last 3 Months

Contains HyperLinks

□ CISA Known Exploited Vulnerabilities
□ US-CERT Technical Alerts
□ US-CERT Vulnerability Notes
□ OVAL Queries



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

Search Results (Refine Search)

Sort results by: Publish Date Descending

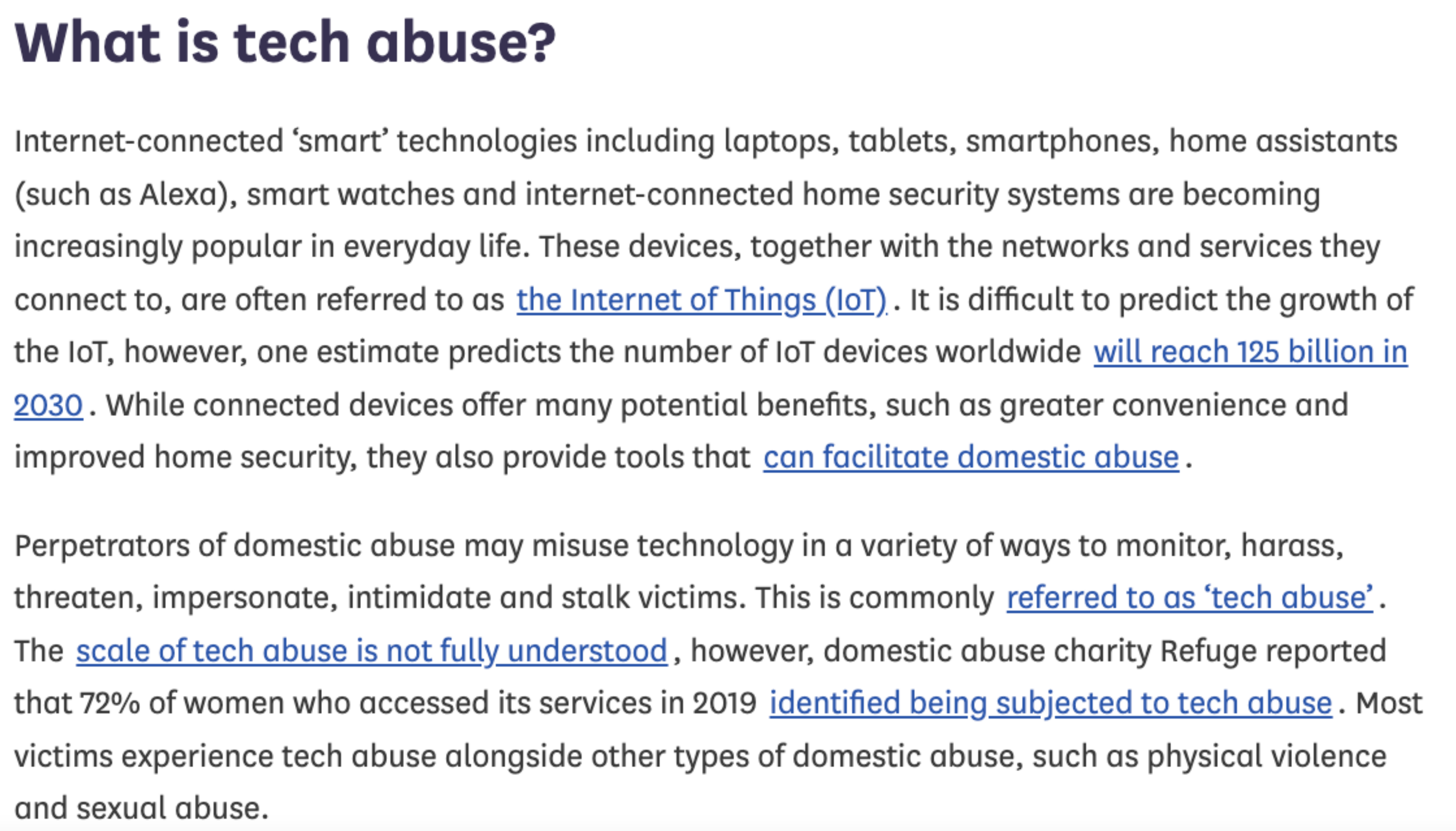
There are **49** matching records.
Displaying matches **1** through **20**.

Search Parameters:

- Results Type: Overview
- Keyword (text search): webcam
- Search Type: Search All
- CPE Name Search: false

Vuln ID	Summary	CVSS Severity
CVE-2021-45345	Buffer Overflow vulnerability found in En3rgy WebcamServer v.0.5.2 allows a remote attacker to cause a denial of service via the WebcamServer.exe file. **Published:** maggio 10, 2023; 4:15:09 PM -0400	*V3.x:*(not available) *V2.0:*(not available)
CVE-2023-0365	The React Webcam WordPress plugin through 1.2.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **Published:** marzo 20, 2023; 12:15:12 PM -0400	*V3.1:* **5.4 MEDIUM** *V2.0:*(not available)
CVE-2023-1188	A vulnerability was found in FabulaTech Webcam for Remote Desktop 2.8.42. It has been classified as problematic. Affected is the function 0x222018 in the library ftwebcam.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be	*V3.1:* **5.5 MEDIUM** *V2.0:*(not available)

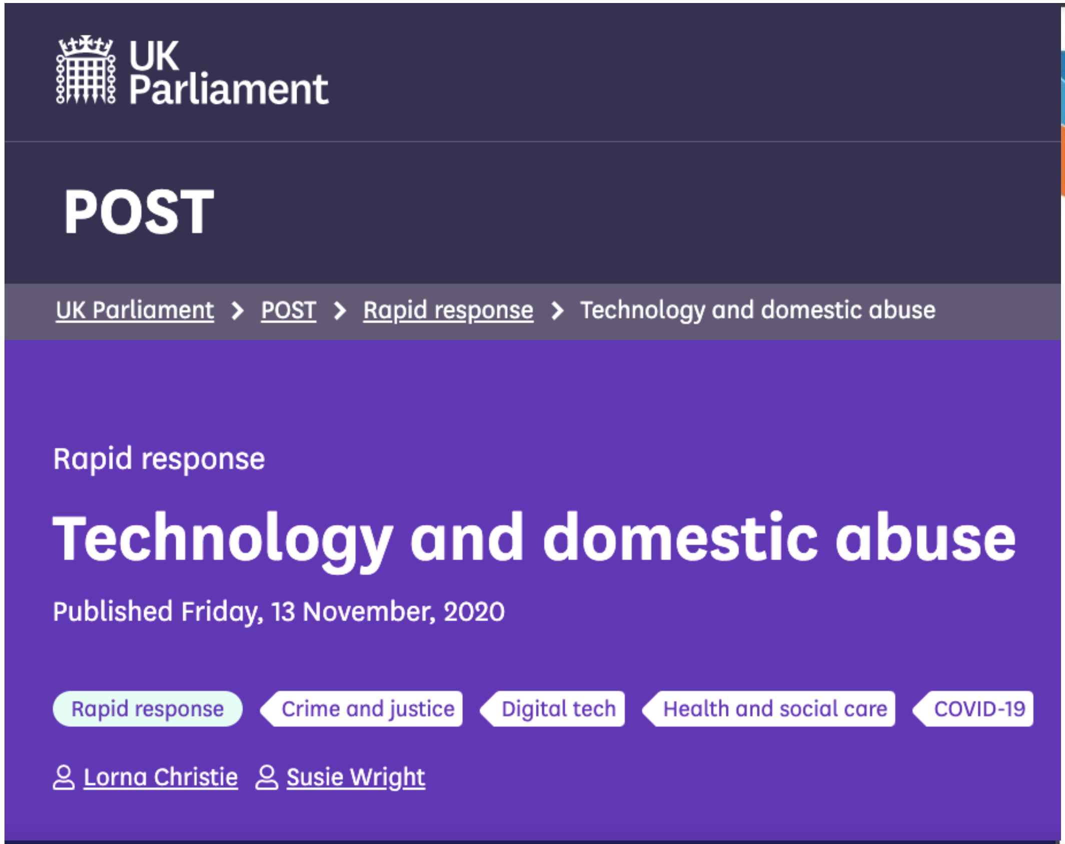
Una nuova forma di abuso.....



What is tech abuse?

Internet-connected 'smart' technologies including laptops, tablets, smartphones, home assistants (such as Alexa), smart watches and internet-connected home security systems are becoming increasingly popular in everyday life. These devices, together with the networks and services they connect to, are often referred to as the Internet of Things (IoT). It is difficult to predict the growth of the IoT, however, one estimate predicts the number of IoT devices worldwide will reach 125 billion in 2030. While connected devices offer many potential benefits, such as greater convenience and improved home security, they also provide tools that can facilitate domestic abuse.

Perpetrators of domestic abuse may misuse technology in a variety of ways to monitor, harass, threaten, impersonate, intimidate and stalk victims. This is commonly referred to as 'tech abuse'. The scale of tech abuse is not fully understood, however, domestic abuse charity Refuge reported that 72% of women who accessed its services in 2019 identified being subjected to tech abuse. Most victims experience tech abuse alongside other types of domestic abuse, such as physical violence and sexual abuse.



UK Parliament

POST

UK Parliament > POST > Rapid response > Technology and domestic abuse

Rapid response

Technology and domestic abuse

Published Friday, 13 November, 2020

Rapid response | Crime and justice | Digital tech | Health and social care | COVID-19

Lorna Christie Susie Wright

UCL

TECH ABUSE

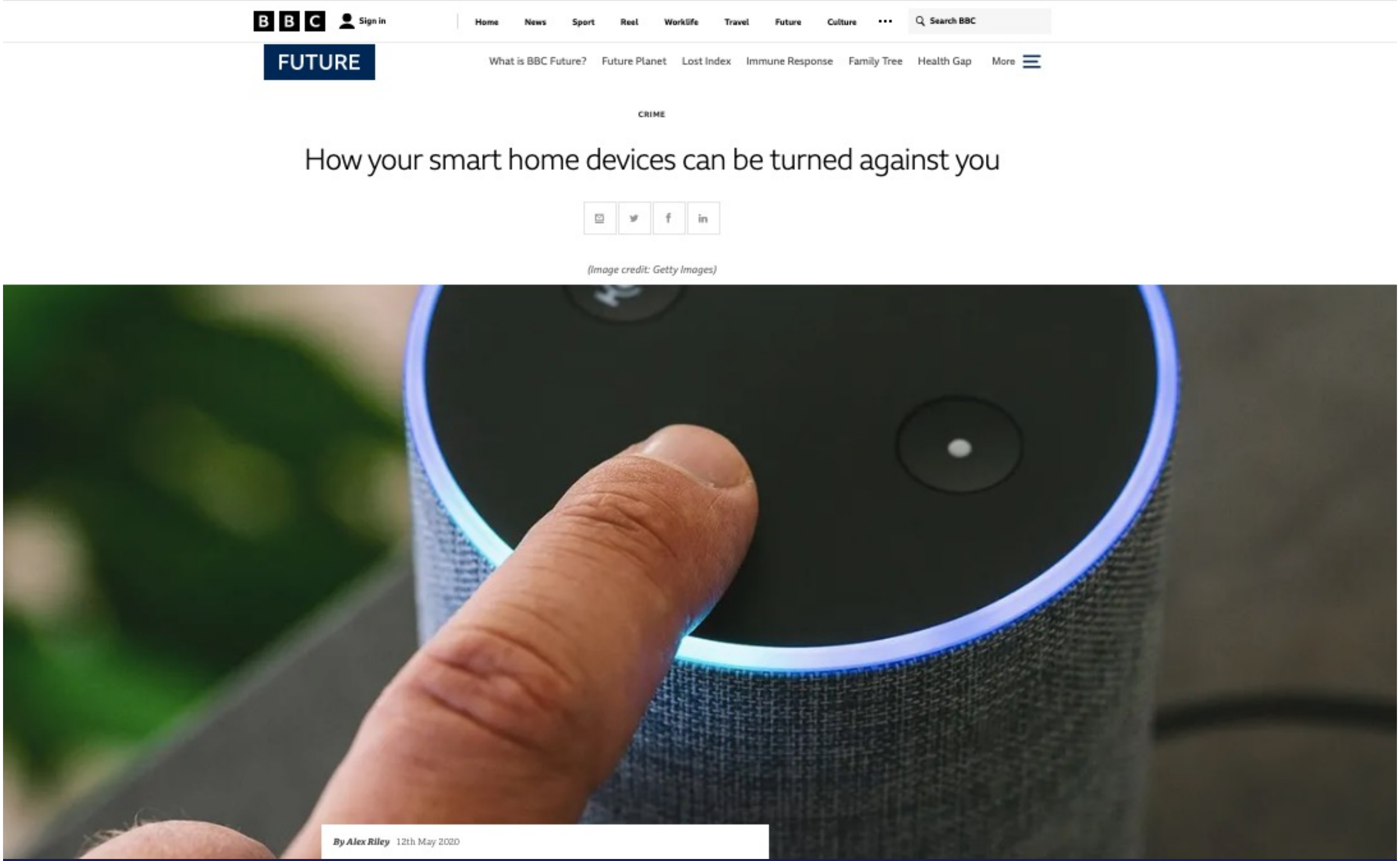
Gender and IoT Research Report

The rise of the Internet of Things and implications for technology-facilitated abuse

November 2018

Leonie Tanczer
Isabel Lopez Neira
Simon Parkin
Trupti Patel
George Danezis

https://post.parliament.uk/technology-and-domestic-abuse/



CRIME

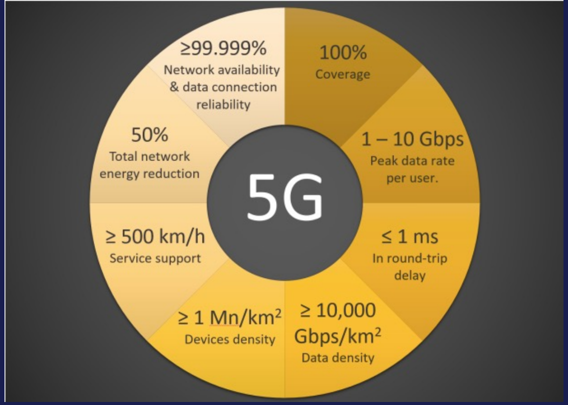
How your smart home devices can be turned against you

(Image credit: Getty Images)

By Alex Riley 12th May 2020

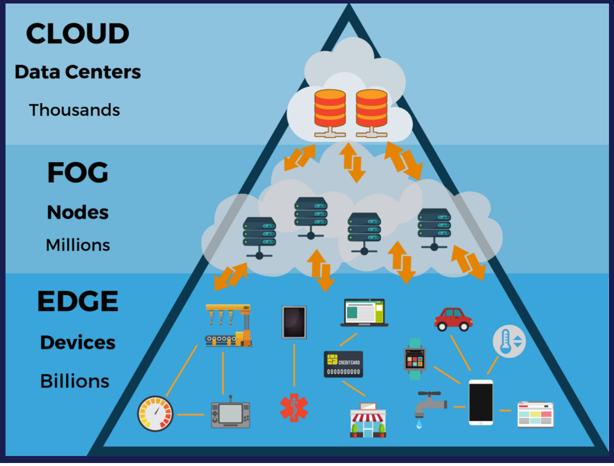
https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse

IoT: futuro e prospettive



- Rete 5G, 6G,..
  - ➢più velocità di comunicazione
  - ➢più dispositivi connessi
  - ➢maggiore affidabilità
- Intelligenza Artificiale
  - ➢auto-apprendimento
  - ➢autonomia dei sistemi IoT
  - ➢interazione in linguaggio naturale

- Edge Computing
  - ➢elaborazione locale dei dati
  - ➢beneficio in termini di privacy e sicurezza
  - ➢riduazione della latenza di comunicazione
  - ➢scalabilità e flessibilità



Siamo destinati ad essere supinamente monitorati, osservati, spiati, …., giudicati ?

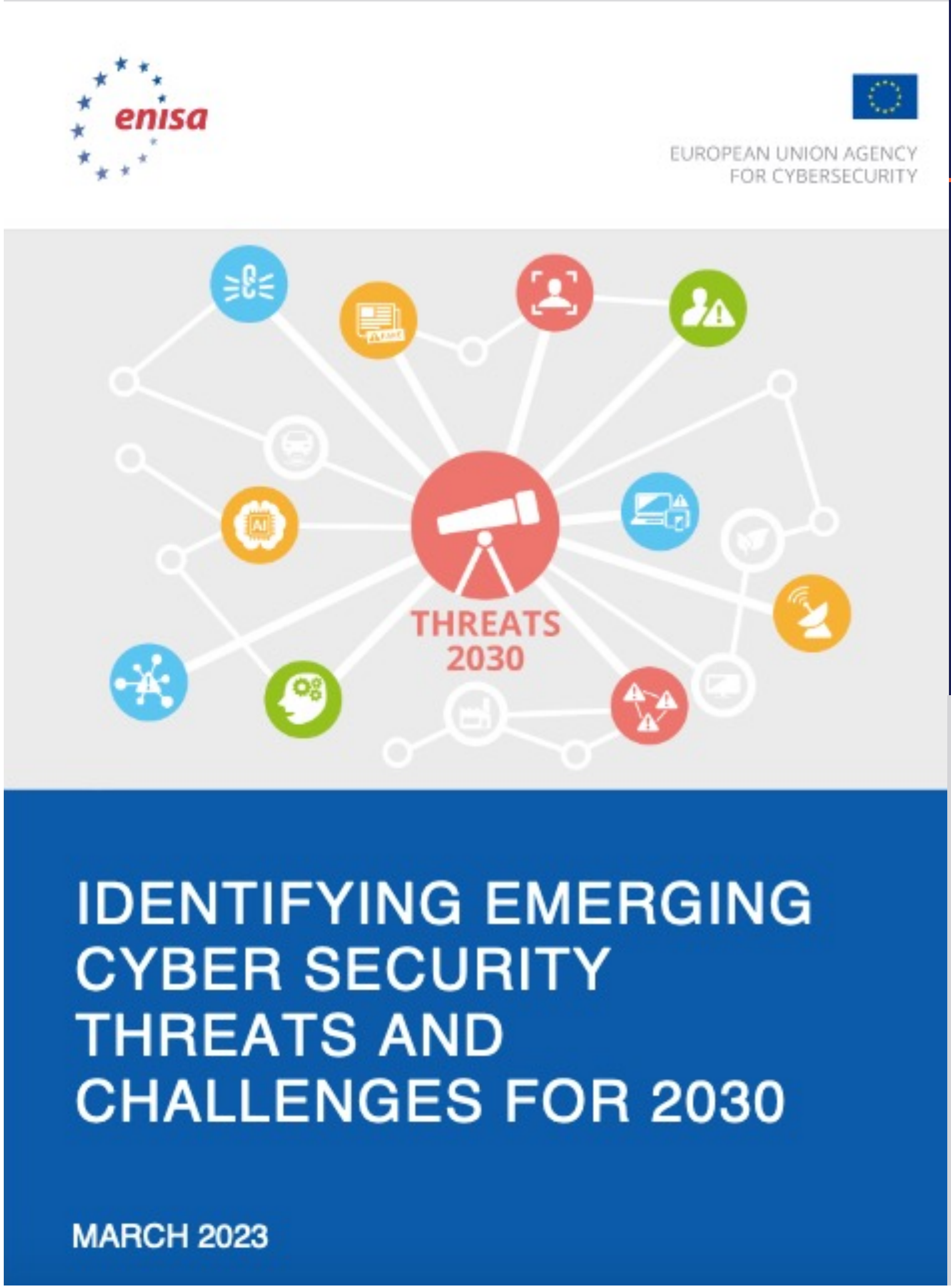
È possibile ridurre le nostre “tracce digitali” (la nostra ombra digitale)?

una distribuzione MARIO e VITTORIO CECCHI GORI e C.E.I.A.D.
MAURO BERARDI e ETTORE ROSBOCH presentano
MASSIMO TROISI
ROBERTO BENIGNI
Non ci resta che piangere
un film scritto e diretto da
MASSIMO TROISI ROBERTO BENIGNI
IRIS PEYNADO · AMANDA SANDRELLI · CARLO MONNI con la partecipazione di PAOLO BONACELLI
direttore della fotografia GIUSEPPE ROTUNNO musiche PINO DONAGGIO
edizioni musicali FREE LIFE COMPANY s.r.l. e CLISCA s.r.l. prodotto da MAURO BERARDI e ETTORE ROSBOCH

Sempre che siamo davvero interessati a farlo?

…. Nel 2019 concludevo il mio talk:

- Adozione e diffusione di tecnologie e applicazioni IoT in fortissima crescita
- Crescente numero di produttori e di prodotti IoT
- Estremamente complesso un controllo accurato della rispondenza tra quanto proposto sul mercato e le necessarie garanzie in termini di privacy e sicurezza che garantiscano i consumatori



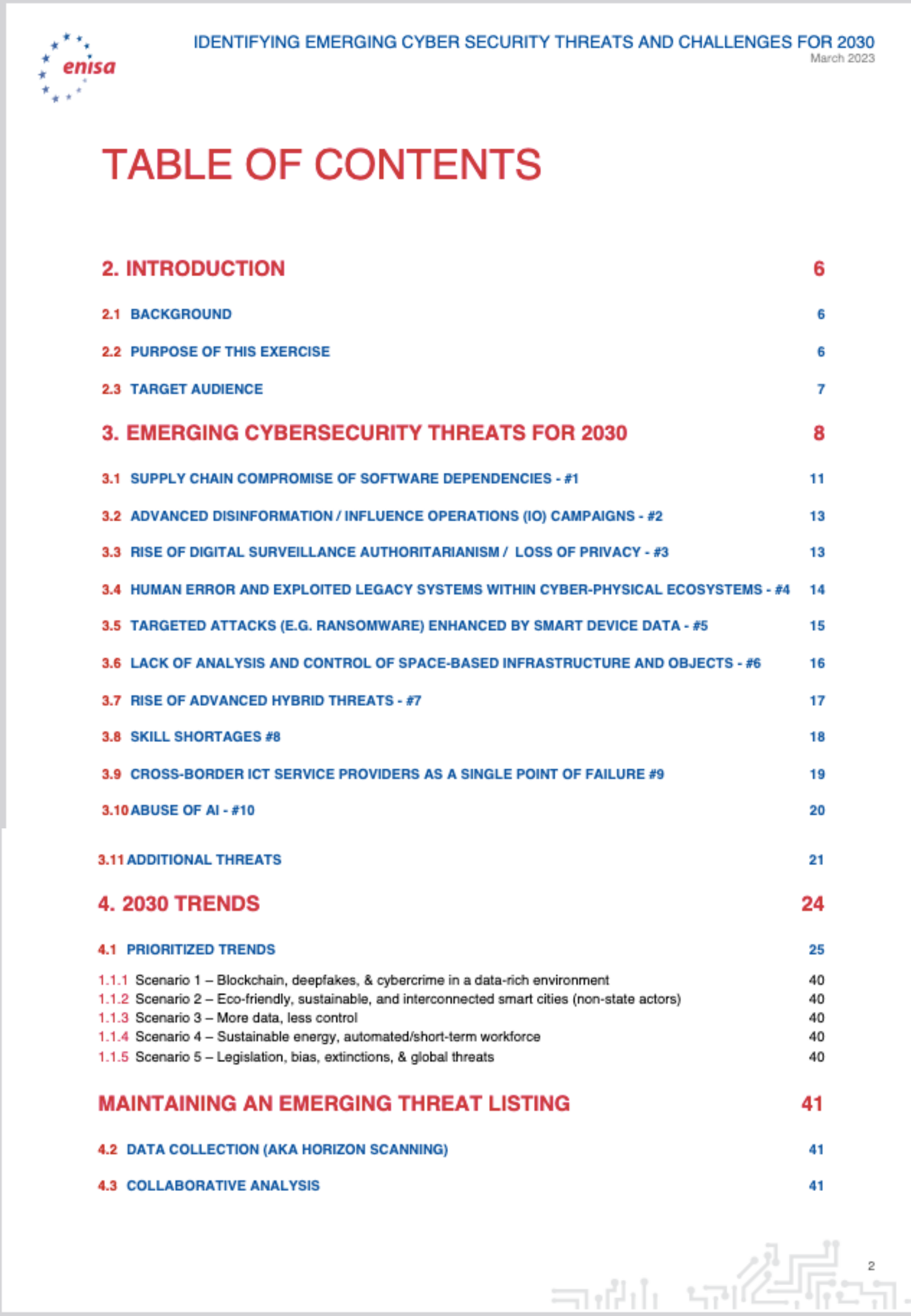
enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

THREATS
2030

IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030

MARCH 2023

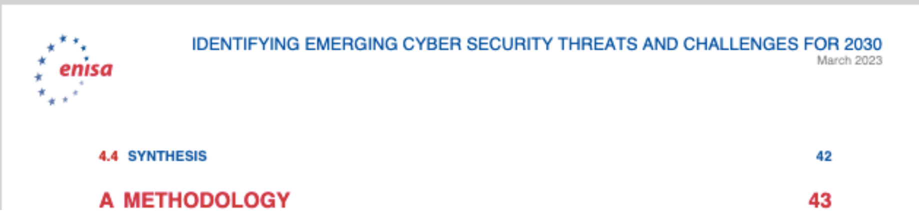


enisa

IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030
March 2023

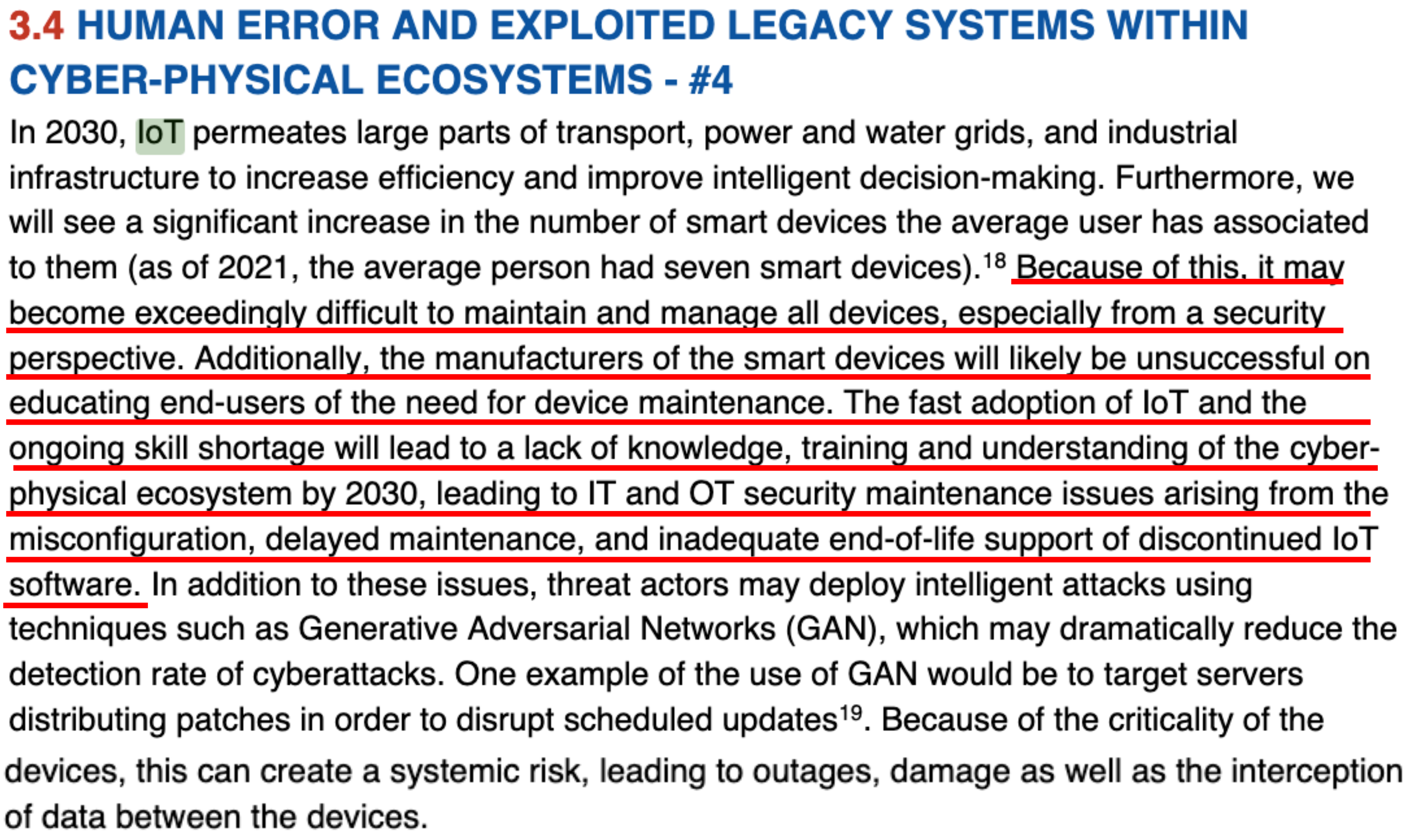
TABLE OF CONTENTS

2



enisa

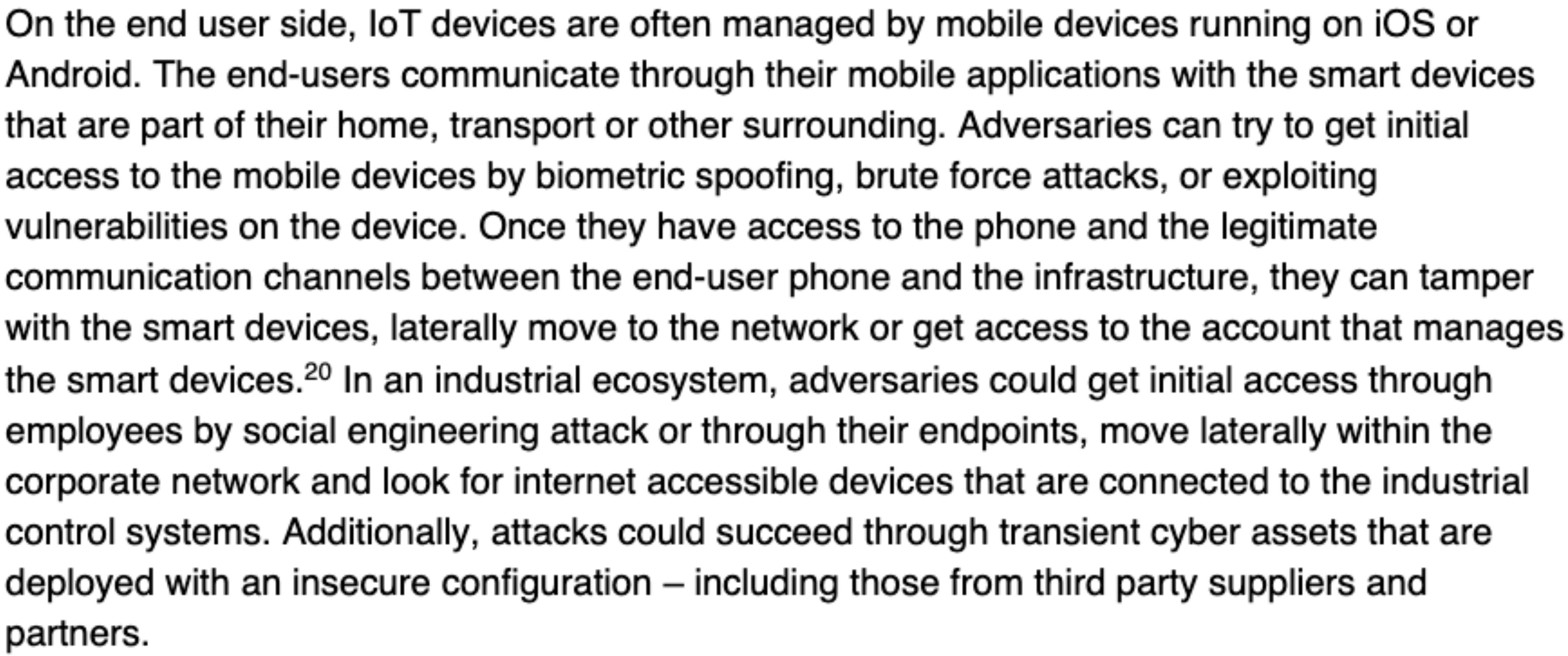
IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030
March 2023



3.4 HUMAN ERROR AND EXPLOITED LEGACY SYSTEMS WITHIN CYBER-PHYSICAL ECOSYSTEMS - #4

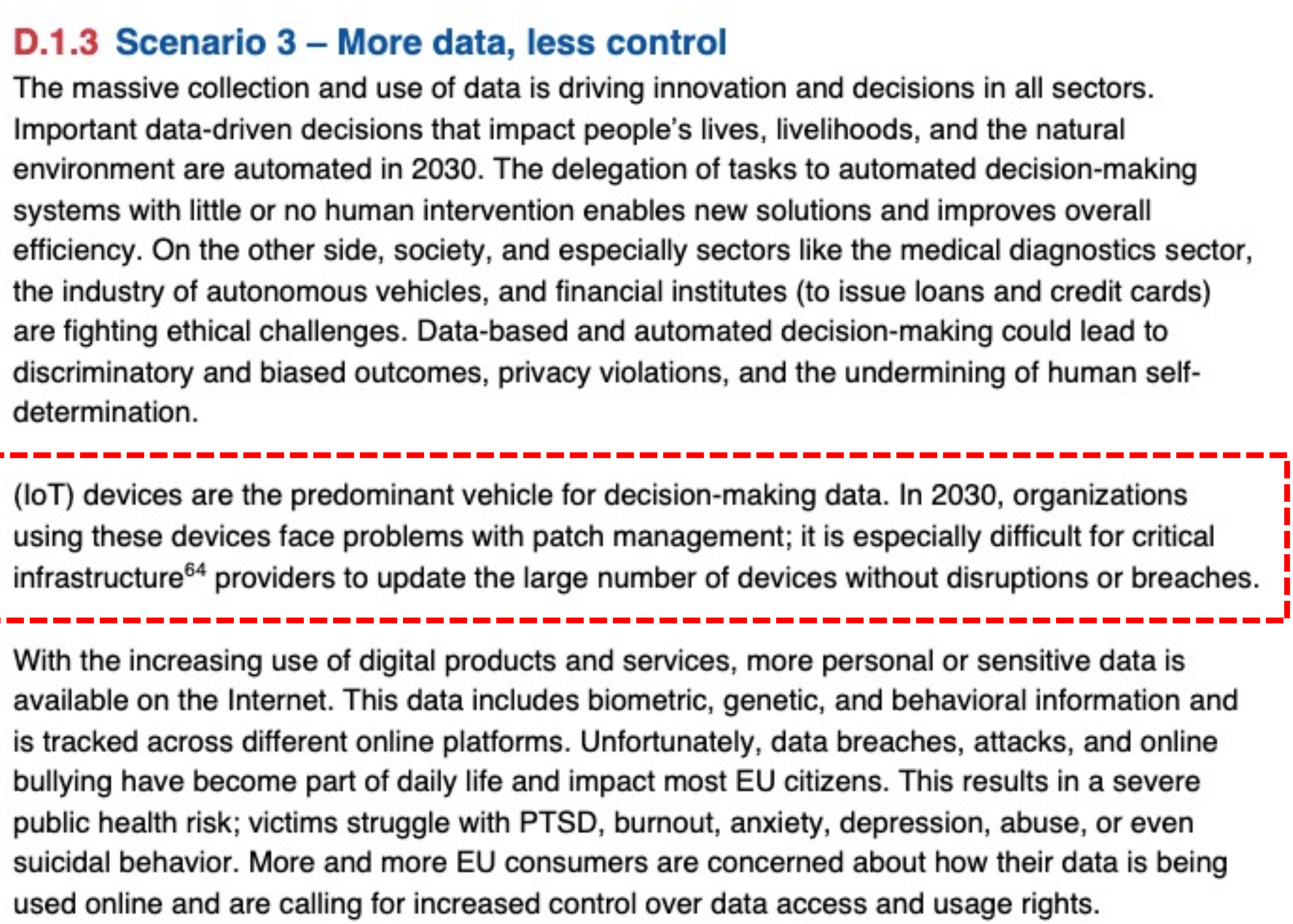
In 2030, IoT permeates large parts of transport, power and water grids, and industrial infrastructure to increase efficiency and improve intelligent decision-making. Furthermore, we will see a significant increase in the number of smart devices the average user has associated to them (as of 2021, the average person had seven smart devices).[18] Because of this, it may become exceedingly difficult to maintain and manage all devices, especially from a security perspective. Additionally, the manufacturers of the smart devices will likely be unsuccessful on educating end-users of the need for device maintenance. The fast adoption of IoT and the ongoing skill shortage will lead to a lack of knowledge, training and understanding of the cyber-physical ecosystem by 2030, leading to IT and OT security maintenance issues arising from the misconfiguration, delayed maintenance, and inadequate end-of-life support of discontinued IoT software. In addition to these issues, threat actors may deploy intelligent attacks using techniques such as Generative Adversarial Networks (GAN), which may dramatically reduce the detection rate of cyberattacks. One example of the use of GAN would be to target servers distributing patches in order to disrupt scheduled updates[19]. Because of the criticality of the devices, this can create a systemic risk, leading to outages, damage as well as the interception of data between the devices.

Ora ci si mette anche l’Intelligenza Artificiale…….



On the end user side, IoT devices are often managed by mobile devices running on iOS or Android. The end-users communicate through their mobile applications with the smart devices that are part of their home, transport or other surrounding. Adversaries can try to get initial access to the mobile devices by biometric spoofing, brute force attacks, or exploiting vulnerabilities on the device. Once they have access to the phone and the legitimate communication channels between the end-user phone and the infrastructure, they can tamper with the smart devices, laterally move to the network or get access to the account that manages the smart devices.[20] In an industrial ecosystem, adversaries could get initial access through employees by social engineering attack or through their endpoints, move laterally within the corporate network and look for internet accessible devices that are connected to the industrial control systems. Additionally, attacks could succeed through transient cyber assets that are deployed with an insecure configuration – including those from third party suppliers and partners.

Ora ci si mette anche l’Intelligenza Artificiale…….



D.1.3 Scenario 3 – More data, less control

The massive collection and use of data is driving innovation and decisions in all sectors. Important data-driven decisions that impact people's lives, livelihoods, and the natural environment are automated in 2030. The delegation of tasks to automated decision-making systems with little or no human intervention enables new solutions and improves overall efficiency. On the other side, society, and especially sectors like the medical diagnostics sector, the industry of autonomous vehicles, and financial institutes (to issue loans and credit cards) are fighting ethical challenges. Data-based and automated decision-making could lead to discriminatory and biased outcomes, privacy violations, and the undermining of human self-determination.

(IoT) devices are the predominant vehicle for decision-making data. In 2030, organizations using these devices face problems with patch management; it is especially difficult for critical infrastructure[64] providers to update the large number of devices without disruptions or breaches.

With the increasing use of digital products and services, more personal or sensitive data is available on the Internet. This data includes biometric, genetic, and behavioral information and is tracked across different online platforms. Unfortunately, data breaches, attacks, and online bullying have become part of daily life and impact most EU citizens. This results in a severe public health risk; victims struggle with PTSD, burnout, anxiety, depression, abuse, or even suicidal behavior. More and more EU consumers are concerned about how their data is being used online and are calling for increased control over data access and usage rights.

Meditate gente, meditate…..