EUROPEAN UNION AGENCY FOR CYBERSECURITY

CYBER EUROPE 2022

Overview & Findings

By Alexandros Zacharis

10 | 10 |2022

CYBER EUROPE LEGACY

ENISA manages the programme of pan-European exercises named “Cyber Europe”

- Organised biannually since 2010, together with Planners from MS
- Simulations of large-scale cybersecurity incidents that escalate to become cyber crises
- Offers opportunities to analyse advanced technical cybersecurity incidents & deal with complex business continuity and crisis management situations.
- Focus on a different Sector every year. (ex. ENERGY, ICT&CLOUD, HEALTHCARE)

CE2022 -SUMMARY

- 2 Day Event
- Scenario focuses on **Healthcare Sector**
- ISPs & Cloud Service Providers (secondary Target)
- Real-life inspired technical incidents
- The incidents will build-up into a major crisis at all levels: local, organisational, national, and European.
- Business continuity plans and crisis management procedures will be put to the test.
- Observers Program Available

TARGET AUDIENCE

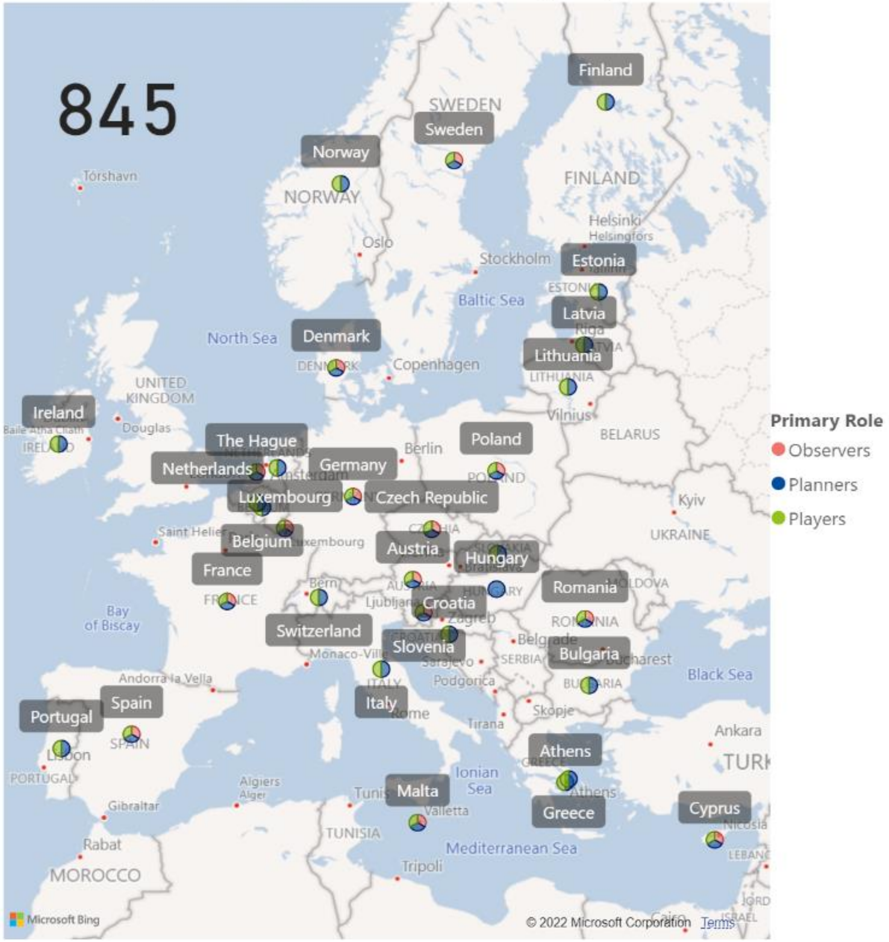
#	AUDIENCE	TYPE	ID
1	National/Governmental CSIRTs / Cyber Security Authorities	Public	CSA
2	Health Ministries/Authorities	Public	Government
3	Healthcare Organisations (e.g. hospitals/clinics/labs)	Public/Private	Healthcare Providers
4	eHealth Service Providers	Public/Private	Networks
5	Health industry	Private	Industry
6	Other: ENISA, CERT-EU, European Council, Europol	Public	EUBIs
7 *	ICT & Cloud Service Providers	Private	Industry

[1] This target audience includes the public organisations that participate in the related EU-level cooperation entities as defined in the NIS Directive, i.e. the CSIRTs Network (Art 12) and/or the Single Point of Contact (Art 8.4 and 14.5). The decision on participates is up to each country.

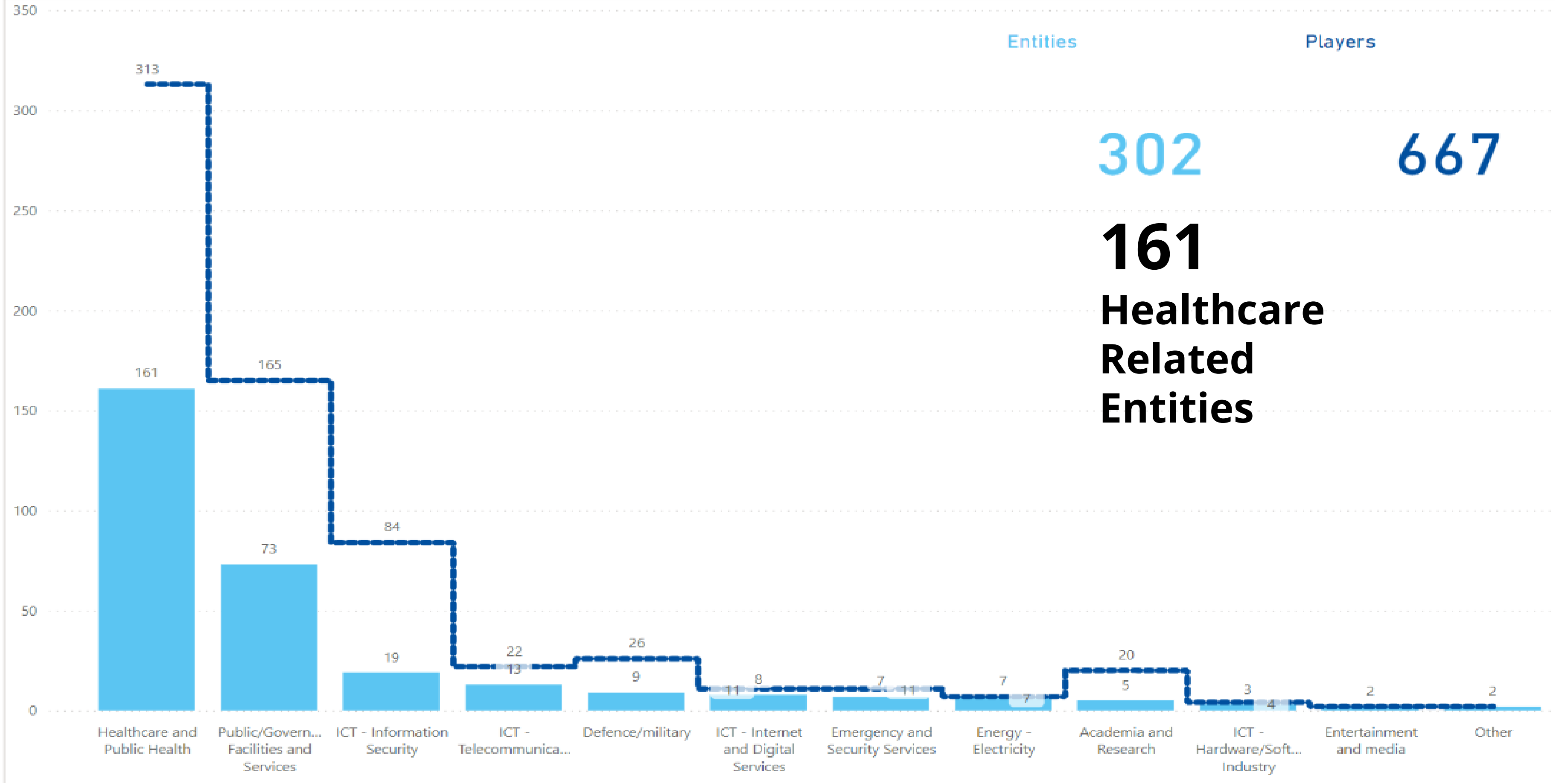
PARTICIPATION (1/2)

- 845 registered participants
- 26 EU Member States Represented
- 2 EFTA countries (Norway and Switzerland)
- Several EU institutions and agencies, including CERT-EU, EAAS, EDPS, EUSPA, EUROPOL and the European Commission

Fraction of registered participant accounts in CEP by role per Country/EUIBA



PARTICIPATION (2/2)



161

Healthcare Related Entities

SCENARIO

- Two hacking groups are behind a massive scale of Cyber Attacks against EU Healthcare Infrastructure.
- The First group is monetary motivated with previous access to a large number of institutions. Access to suppliers of healthcare related software has been achieved.
- The Second Group is a state sponsored actor that tries to discredit EU.
- Hidden attacks from the second group masquerading as the first one.

MAIN THREAT ACTORS AND CAPABILITIES

Group 1: cyber-crime hacking group

Group behind general hacking attacks/incidents

Motivation: Profit/Glory

- Dark market
  - Buy/sell of infected medical devices and software
  - Sell of sensitive personal data, resulted from data breaches
- Cryptocurrency halving event motivation

Group 2: state sponsored APT group

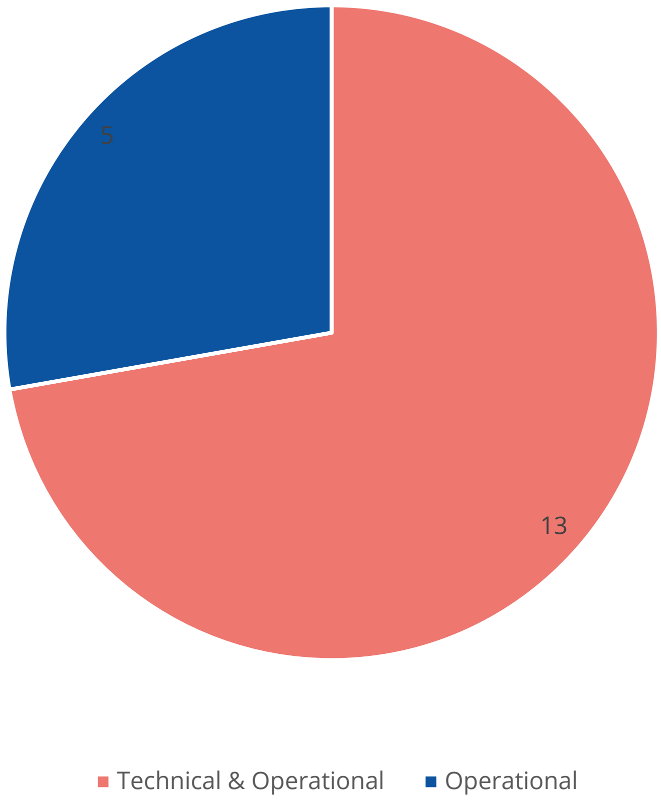
Tactical goal: Defamation and disinformation campaigns (to harm winning EU teams of last Olympic games)

- Data breaches
- Targeted attacks on specific victims
  - e.g. evil twin type of attacks
- Cyberespionage

18 INCIDENTS IN TOTAL

5 Operational only incidents

13 Technical incidents that can be played operationally as well



MEDICAL DATA SERVER ATTACKS (PACS /DICOM)

- Picture Archive and Communications Systems (PACS) are commonly used in Hospitals to store medical images.
- Along with Radiology Information System (RIS) constitute the core Clinical Information Systems (CIS).

AIM:
Use Vulnerabilities of Digital Imaging and Communications in Medicine (DICOM) & DB related vulnerabilities (SQLi) -> Take over PACS and CIS

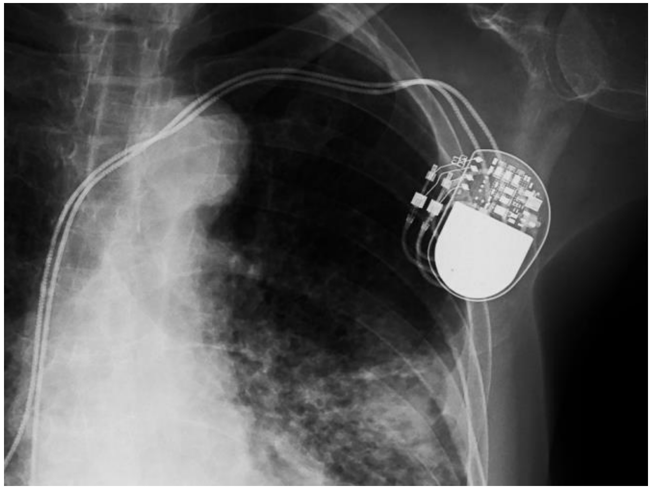
ATTACK ON MEDICAL DEVICES (IOT)

Medical devices that in general have little to no security controls.

- **A certain backdoor in the firmware of a drug infusion pump will be used.**
- **The backdoor was placed in the software after a successful supply chain attack.**

VULNERABLE IMPLANTABLE DEVICES (CARDIAC DEVICES)

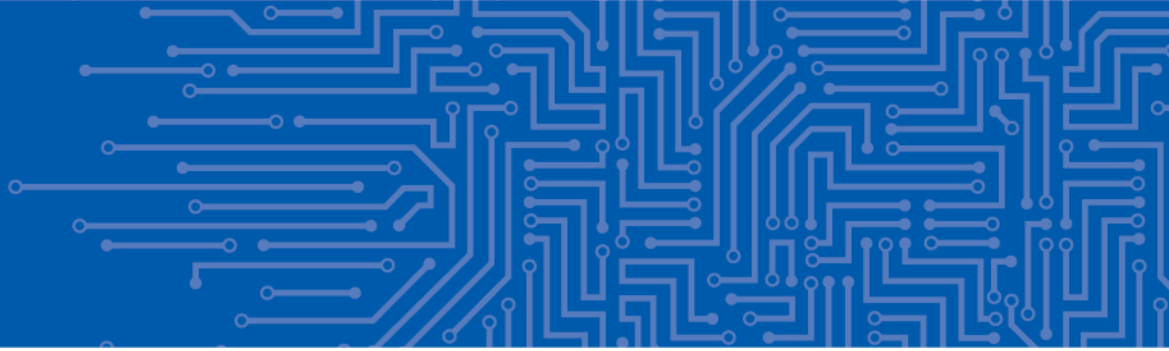
- **The first pacemaker hacks emerged about a decade ago.**
- **Different variations exist depending not on manipulating radio commands or even on malware installed directly on an implanted pacemaker.**
- **The attacks are targeted to persons of interest after a patients data leak**



VIDEO TIME

https://dy7e87ahrzs9p.cloudfront.net/enisa_np2.mp4

FINDINGS (1/2)



- Attacks that impacted Healthcare Sector during 2020-2022 supported our choice of sector
- Additional sectors succeeded in engaging more players as intended
- Smaller Hospitals / Clinics struggle with Cyber Security. Procedures (Incident Handling, Backup Policy) & Technical expertise is missing!
- Awareness of Employees is Critical
- Players of the Healthcare Sector grasped the opportunity to present to their Higher Management:
  - Existing gaps in their cyber security posture
  - The need for further investment in cyber security

FINDINGS (2/2)

- Next Cyber Europe should become less Sector focused and more Threat focused.
- Better prepared Planners lead to more engaged and satisfied Players
- The Observers programme was well received and showcased the full potentials a large-scale cyber exercise to the international cyber security community

THANK YOU FOR YOUR ATTENTION

Ethnikis Antistaseos 72 & Agamemnonos 14,
Chalandri 15231, Attiki, Greece

exercises@enisa.europa.eu

www.enisa.europa.eu