CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Università di Roma Tor Vergata
Dipartimento di Ingegneria Elettronica

Scenari di Cyber Threat Information Sharing per la Sanità Digitale

Lorenzo Bracciale

Docente di Sanità Digitale

Dipartimento di Ingegneria Elettronica

lorenzo.bracciale@uniroma2.it

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Cooperation is the key of success

Editorial | Published: 09 July 2018

The cooperative human

Nature Human Behaviour **2**, 427–428 (2018) | Cite this article

Human beings are a social species that relies on cooperation to survive and thrive. Understanding how and why cooperation succeeds or fails is integral to solving the many global challenges we face.

Cooperation lies at the heart of human lives and society – from day-to-day interactions to some of our greatest endeavours. Understanding cooperation – what motivates it, how it develops, how it happens and when it fails to happen – is therefore an important part of understanding all kinds of human behaviour. In this focus issue of *Nature Human Behaviour*,

The cooperative human. Nat Hum Behav 2, 427–428 (2018).

Cyber criminals cooperate indeed...

- Organized cyber criminal groups
  - Lazarus Gang (Sony Pictures hack in 2014, WannaCry Ransomware)
  - Cobalt Cybercrime Gang (100 financial firms hacked in more than 40 countries)
  - Russian Ryuk gang (at least 235 hospitals with ransomware since 2018) → allegedly kill a newborn baby in US in 2019
- ...share and trade informations on darknet marketplaces
  - UniCC (carding) Closed
  - Genesis Market (login credentials, device fingerprints, website vulnerabilities, bots) Open since 2018
  - AlphaBay (malware, services) Resurrected after 5 years

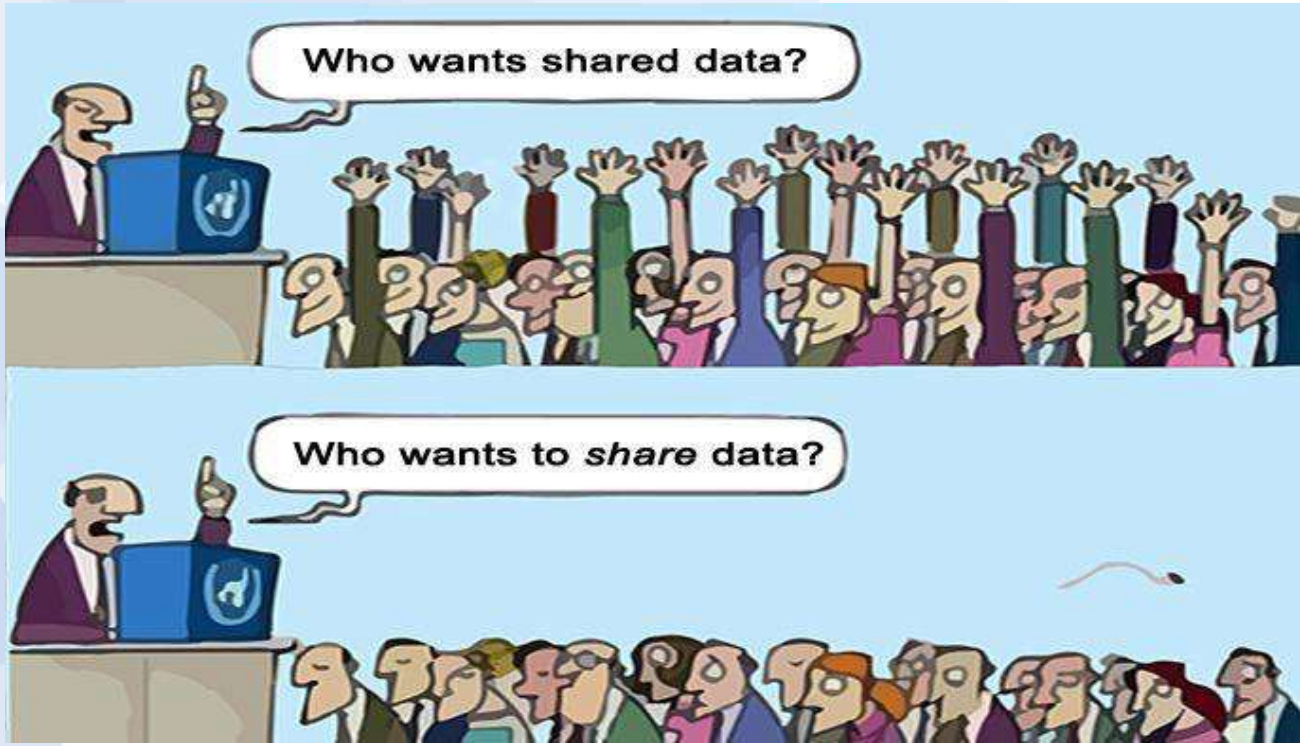
Recent attacks to Italian healthcare

- More than 10 attacks in the last 10 months:
  - Regione Lazio: ransomware August 2021 (RansomEXX)
    - Stop of vaccinations
  - Ulss di Padova: ransomware (LockBit 2.0 group)
    - Stop of laboratories and sampling, vaccines; publication of tens of Medical Records
  - Usl Napoli 3: ransomware (Sabbath group)
    - infrastructure paralysis; dissemination of sensitive data
  - Asst Fatebenefratelli Sacco: ransomware
    - Website owned (no patient data leaks)
- Motivation? **Cybercrime** in 86% of the cases (+16% wrt 2020)

Rapporto Clusit edizione marzo 2022

Increase cooperation to improve protection

Where to start? Sharing data



img src: https://www.ictsecuritymagazine.com/

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Sharing: what?

- Intelligence on threats, incidents and vulnerabilities
  - Indicators of compromise (IoC)
  - Tactics, techniques and procedures (TTPs) of threat actors
  - Advice and best practices
  - Mitigation strategies
- Among:
  - Human-to-human
  - Machine-to-machine

H-ISAC™
HEALTH - ISAC

Sharing: how?

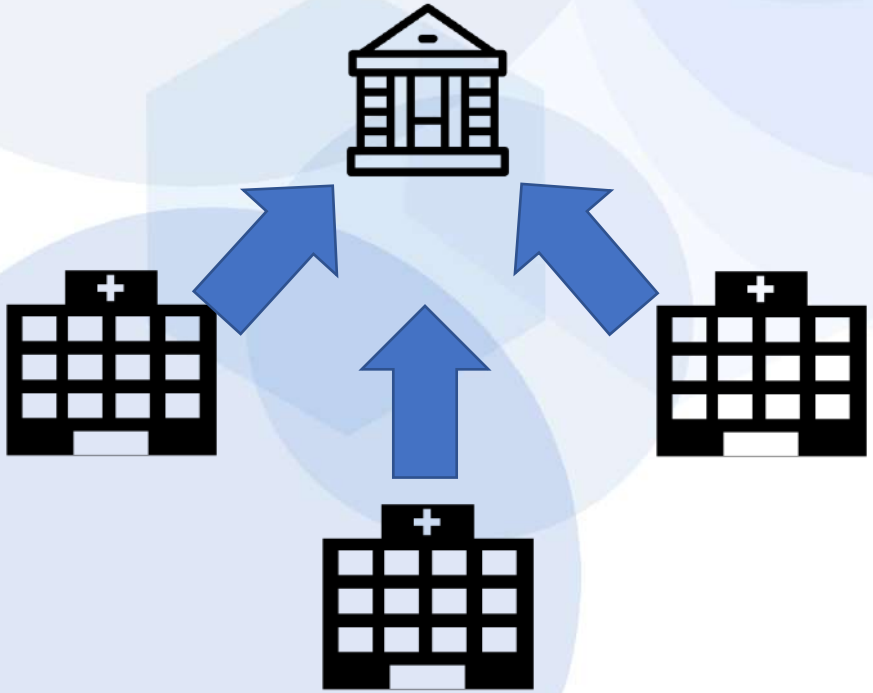
- Use Cyber Threat Intelligence Platforms (e.g. MISP)
  - Prefering open protocols and data formats
- Use Incident Response Platform with sharing functionality (e.g. The Hive)
- Increment sharing
  - More data
  - With more peers
- Use the sharing data with integration
  - E.g. integration with IDS and H-IDS

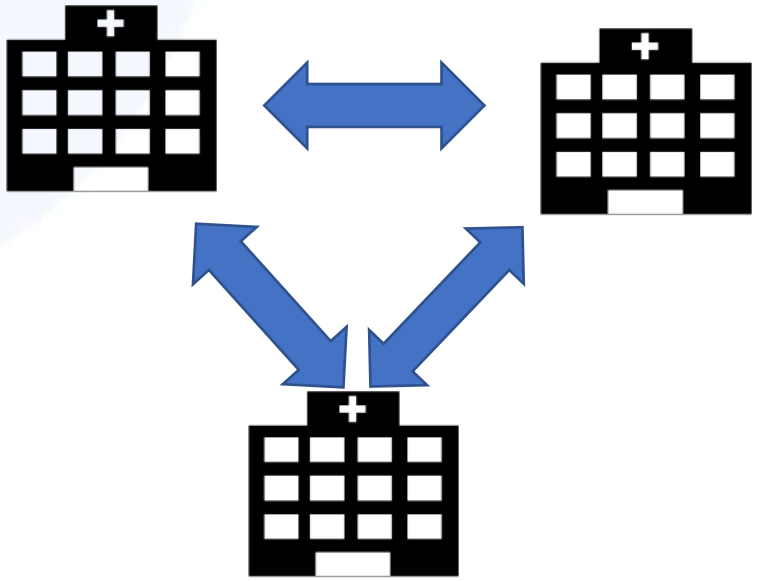
https://www.misp-project.org/

When sharing is not possible?

- Investigate trade-off between utility and privacy with **aggregated data**
  - A trusted Third Party is not always needed...
    - Secure Multiparty Computation
    - Homomorphic encryption

Everybody knows the aggregated data without disclosing any individual data





Design dedicated tool for healthcare

- In 2021 we had more targeted attacks to:
  - Governmental/military objective: 15% (+36,4%);
  - IT: 14% (+3,3%)
  - Multiple targets: 13% (-8%)
  - Healthcare: 13% (+24,8%)
  - Education: 9% (stable)
- Targeted attacks call for targeted defense:
  - Often similar organizations are targeted by the same threat actor
  - Consider the specific needs of healthcare sectors

Rapporto Clusit edizione marzo 2022

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Conclusion

- Increased cooperation from attackers calls for more cooperation from healthcare providers
- Need to work on technology:
  - Improve the usage of tools for data sharing
  - Design dedicated tools for healthcare
  - Test techniques to improve privacy vs utility
  - Improve automation of processes
- Work on the human factor:
  - Motivation and incentives for cooperation driving attacks and defense
  - Education and community
  - Mentality: fighting the SILO mentality