cesnet

HSOC
HOSPITAL SECURITY OPERATION CENTER

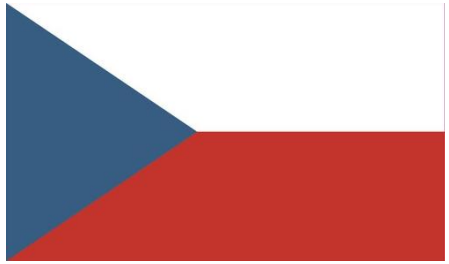
Community approach to cybersecurity in the Czech healthcare: Attacks, Challenges, Experiences and Lessons learned

Radovan Igliar, Jan Kolouch
CESNET

6 Oct. 2022
Telč

Czech healthcare system

- Financed **indirectly** through **health insurance system**
- **Fragmented system** of founding bodies
  - state, municipalities, cities, army, private, …
- **Different types** of Healtcare providers
  - teaching & faculty, regional, specialised, psychatric, maternity, polyclinics, spas, hospic, emergency service
- ICT at hospital perceived as marginal, no central authority, lack of vision in digitalization of heathcare
  - Cybersecurity - understaffed, under-funded
- **Cybersecurity act –** operators of essential services



REUTERS

INTERNET NEWS

APRIL 17, 2020 / 1:37 PM / UPDATED 2 YEARS AGO

Czech hospitals report cyberattacks day after national watchdog's warning

FRANCE 24

LIVE

#WAR IN UKRAINE #BURKINA FASO FRANCE AFRICA CULTURE SH

Cyber attackers disrupt services at French hospital, demand $10 million ransom

BBC

Home News Sport Reel ...

Tech

Advanced cyber-attack: NHS doctors' paperwork piles up

30 August

CNN politics

Audio Live TV Log In

Several hospitals targeted in new wave of ransomware attacks

By Vivian Salama, Alex Marquardt, Lauren Mascarenhas and Zachary Cohen, CNN

Updated 3:45 PM EDT, Thu October 29, 2020

Czech healthcare system / COVID

- **Political and social pressure - significant increase** in cyber attacks on medical facilities.
- **Technological dept - big differences in the level of IT support** and the needs of individual medical facilities.
- **Rapid need for digitalization - lack of a shared vision** of how to take advantage of digital technologies to transform healthcare.
- The issue of cyber security is fundamental in healthcare **personnel and financially underestimated.**
  - **> Health providers as easy and „wealthy“ target ☹**

+	Date	Vector	Malware	Impact	Damages (est).
Rudolf and Stefanie Hospital in Benešov 444 beds	11. 12. 2019	Phishing	EMOTET-TRICKBOT-RYUK (ransomware)	Decommissioning of hospital Malfunction of some ICT services	2,5 mil EUR
Faculty hospital Brno 1889 beds	12. 3. 2020	Phishing	DEFRAY (ransomware)	Decommissioning of hospital Unavailability of patient data	~ 6+ mil EUR
Psychiatric hospital Kosmonosy 600 beds	27. 3. 2020	Phishing	DEWAR (ransomware)	Encryption of shared storage, domain and application disks. Loss of part of the backups	
Faculty hospital Ostrava 1200 beds	17. 4. 2020	Spear phishing	Není znám	Not public	
Faculty hospital Olomouc 1198 beds	17. 4. 2020	Recoon scanning	Není znám	Not public	
Post-acute care hospital LDN Horažďovice 140 beds	Jan. 2021	Phishing	BURAN (ransomware)	Unauthorized use, damage and deletion of data.	150 000 Kč
Hospital in Česká Lípa	Feb. 2022	-	ransomware	Encryption of data Malfunction of ICT services	-


cesnet
REACTION

cesnet

No super-hero

https://allcore.ca/blog/what-does-managed-it-services-mean-to-you/

cesnet

Nobody will do instead of you...

https://www.information-age.com/creating-rolling-out-effective-cyber-security-strategy-123494607/

Cooperation, Communication

https://jagwire.augusta.edu/free-virtual-cybersecurity-camps-offered-this-summer/

cesnet

HSOC

cesnet

hSOC iniciative

HSOC

HOSPITAL SECURITY OPERATION CENTER

Objective of the initiative

- **To establish the community** that will increase the number of health service providers operating secure information technologies with sufficient technical and personnel background.
- **Cooperation on building cyber security in healthcare sector**
- The goals and activities of the initiative are summarized in a memorandum:

  https://hsoc.cesnet.cz/_media/en/memorandum_en.pdf

  - **61 health institutions, 3 universities, 1 ministry**
  - **Support letter from Ministry of Health**

cesnet

HSOC
HOSPITAL SECURITY OPERATION CENTER

Objective of the initiative

- Cybersecurity must be part of the **basic principles** of how organizations operate
- Security **cannot be outsourced** … responsibility cannot be shirked (without lost of control)
- The need to **build competence**, develop expertise, responsibility, consistency
- Support the **cooperation** of key components of the system
- Don't wait for a saviour, **be inspired, share, cooperate**

cesnet

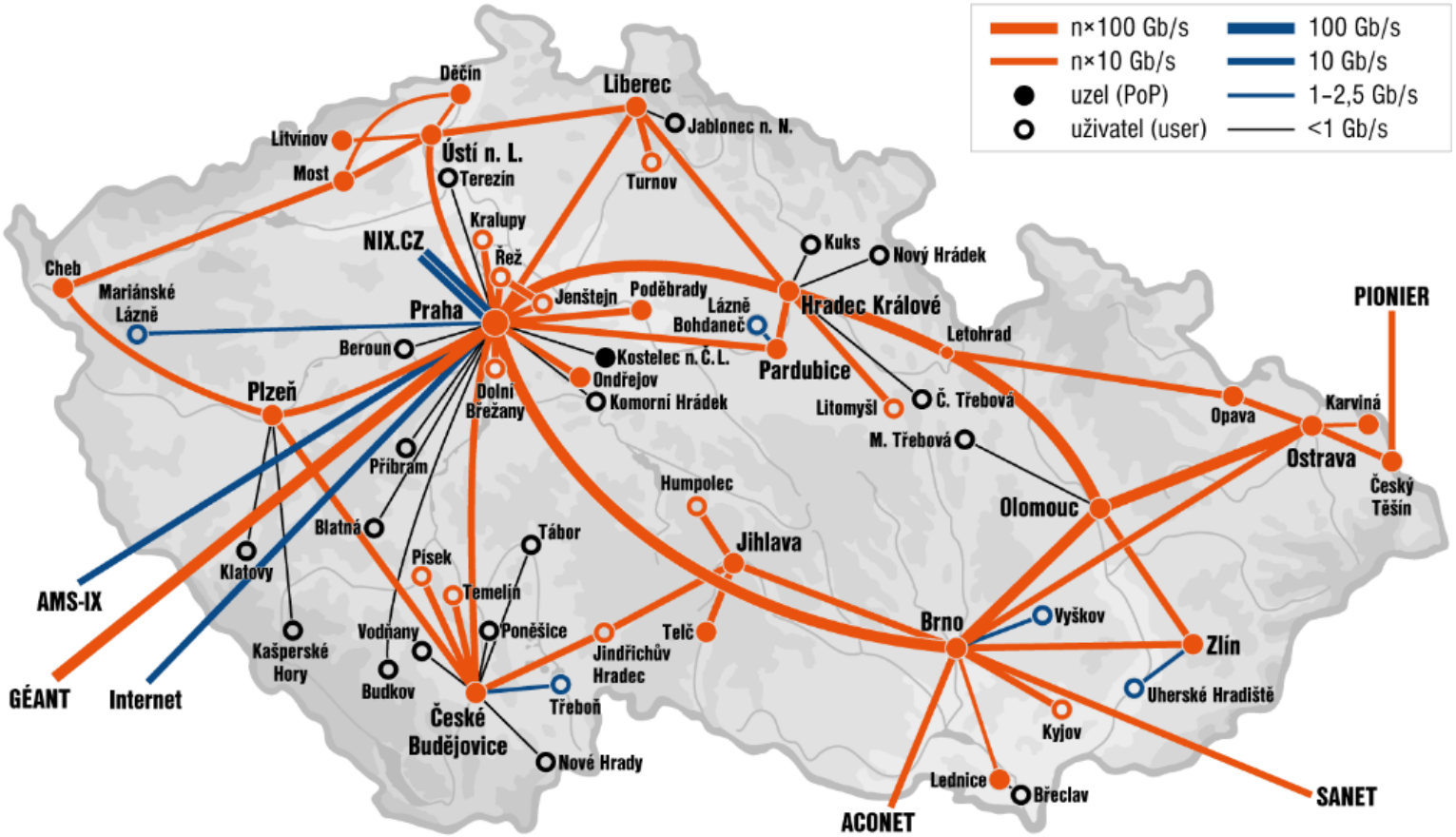
CESNET's ENGAGEMENT

cesnet

- **association of universities** of the Czech Republic **and the Czech Academy of Sciences.**
- operates and develops **the national e-infrastructure** for science, research and education which encompasses a computer network, computational grids, data storage, and collaborative environment.
- offers a rich set of services to connected institutions

https://www.cesnet.cz/services/

National Research Education Network



Service oriented

350 institutions

500 000 end-users

400 Gbps backbone

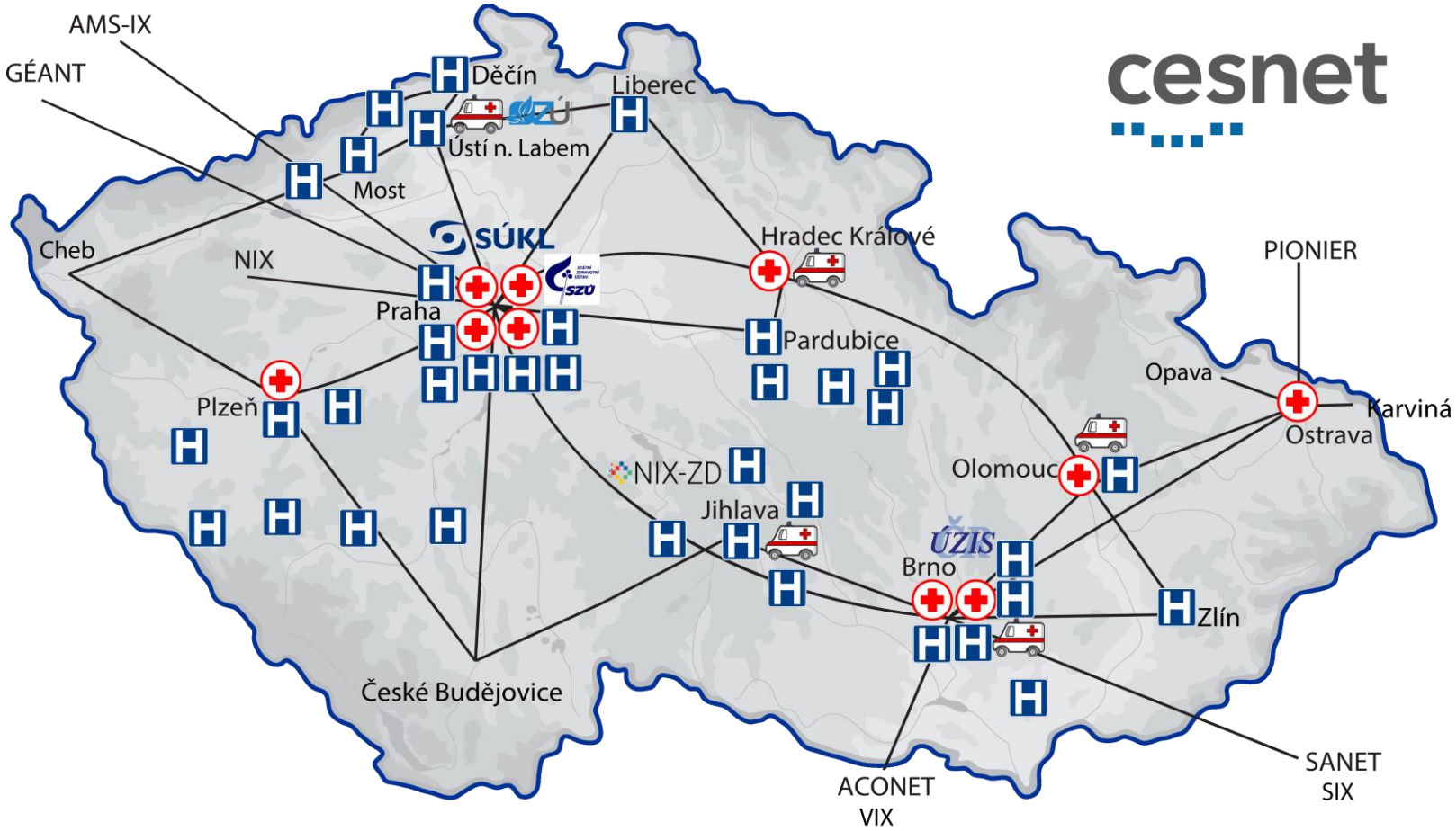
34 000 CPU cores

100 PB storage

Monitoring and Security tools

ISP and Technological partner

NREN and hospitals



cesnet

LESSONS LEARNED

What IS and is NOT the goal of hSOC

cesnet

hSOC is...

- **A platform** for the exchange of information and good practice
- **Warning and coordination communication channel**
- A platform for **the operation of shared services and technologies**
- A community of IT and security professionals and enthusiasts
- **education platform**

cesnet

hSOC is NOT...

- **Universal solution** for the safety of medical facilities
- Subject …**WE ARE COMMUNITY**…
- Security Surveillance Center

Work organised into working groups

- **HSOC - EMERGENCY**

Emergency communication channel

Threat inteligence, alerts

- **HSOC - TECH**

Standards, best-practice sharing, Network/security analysis

Workshops, knoledge sharing

- **HSOC – MKB (Cybersecurity managers)**

Best practice sharing, ISMS, audits

- **HSOC – Education and HR**

Capacity buiding, resources development and education

- **HSOC - Working Group**

Main governing and coordination body

- **hSOC – Board**

Operations group

- **HSOC – MANAGEMENT / CIOs**

Legislative and institutional aspects

Community management, Transparency, Community sharing platform

> https://hsoc.cesnet.cz/en/index

cesnet

SHARED SERVICES

Closed secure hSOC network

- 10 hospitals involved

FAKULTNÍ NEMOCNICE U SV. ANNY V BRNĚ

NEMOCNICE NA HOMOLCE

FAKULTNÍ NEMOCNICE OLOMOUC

VFN PRAHA
VŠEOBECNÁ FAKULTNÍ NEMOCNICE

ÚVN
ÚSTŘEDNÍ VOJENSKÁ NEMOCNICE
Vojenská fakultní nemocnice Praha

NEMOCNICE JIHLAVA

Krajská nemocnice Liberec, a.s.
Liberec a Turnov

NEMOCNICE TOMÁŠE BATI VE ZLÍNĚ

VFN OLOMOUC

KLAUDIÁNOVA NEMOCNICE

- More in the connection process

FAKULTNÍ NEMOCNICE BULOVKA

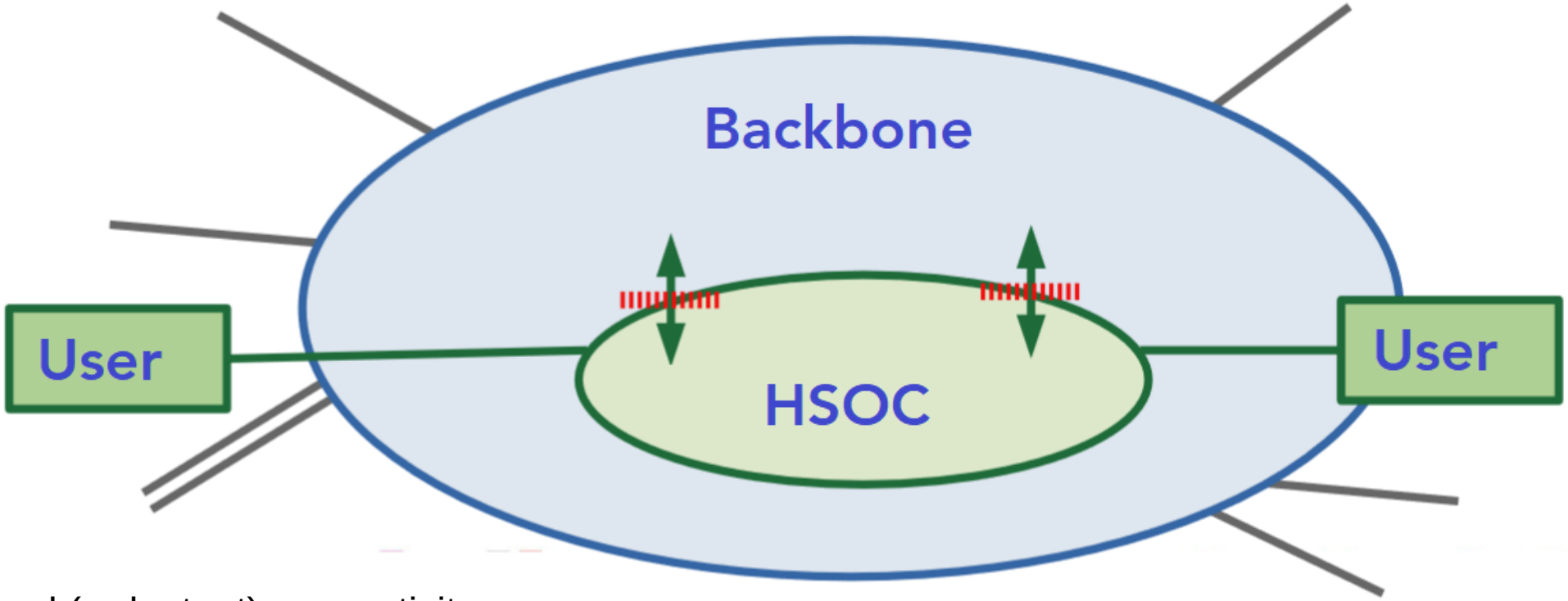
NEMOCNICE HAVLÍČKŮV BROD

ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA KRAJE VYSOČINA

Krajská zdravotní, a.s.

- Monitoring and security tools (SOC tools)
- Common strict rules and policies

Closed secure hSOC network



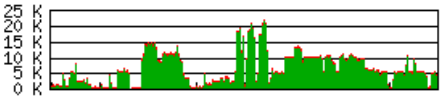
Dual (reduntant) connectivity

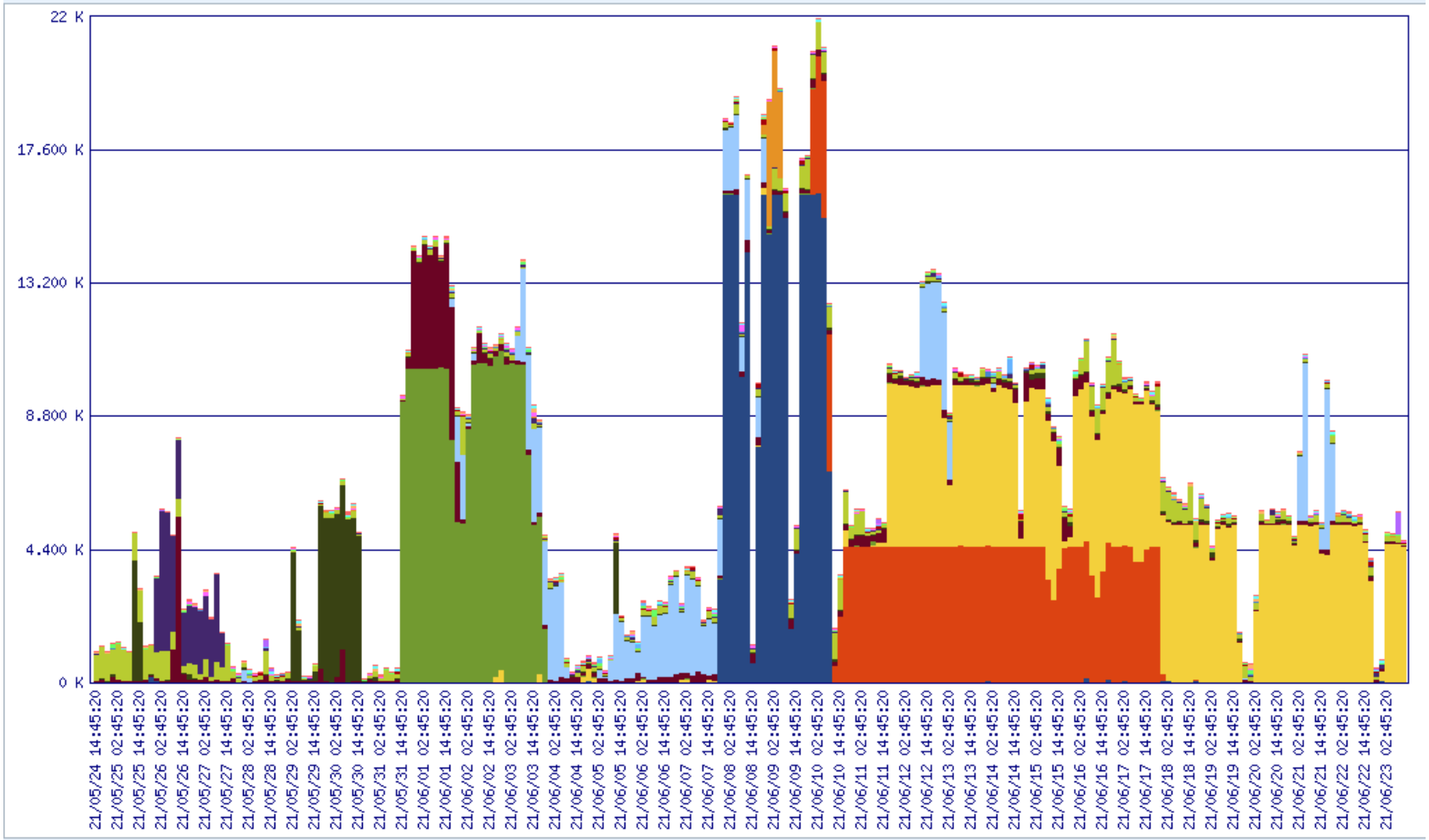
- **Geographic redundancy of Internet connections in two locations**
- **Protection**
  - against IP spoofing,
  - against forgery of reported prefixes by peering partners,
  - against amplification (volumetric) DDoS attacks,
  - against aggressive and slow scans,
  - tools for users for analysis and regulation of their operation in the CESNET e-infrastructure network,
  - automatic redirection of traffic for cleaning in the core of the global Internet (global mitigation against detected sources of unwanted traffic.
- **Harder limits and policies**
  - Possibility of restriction, dropping the attack still on the backbone network

Detected-Event-Cnt: *sums/time steps, 21/05/24 13:15:20-21/06/23 13:15:20, value per 3 hours, cumulative*

Summary

In graph	1.625 M	99.07%
Rest of results	0.015 M	0.93%
Total	1.641 M	100.00%

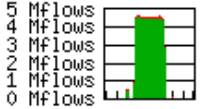


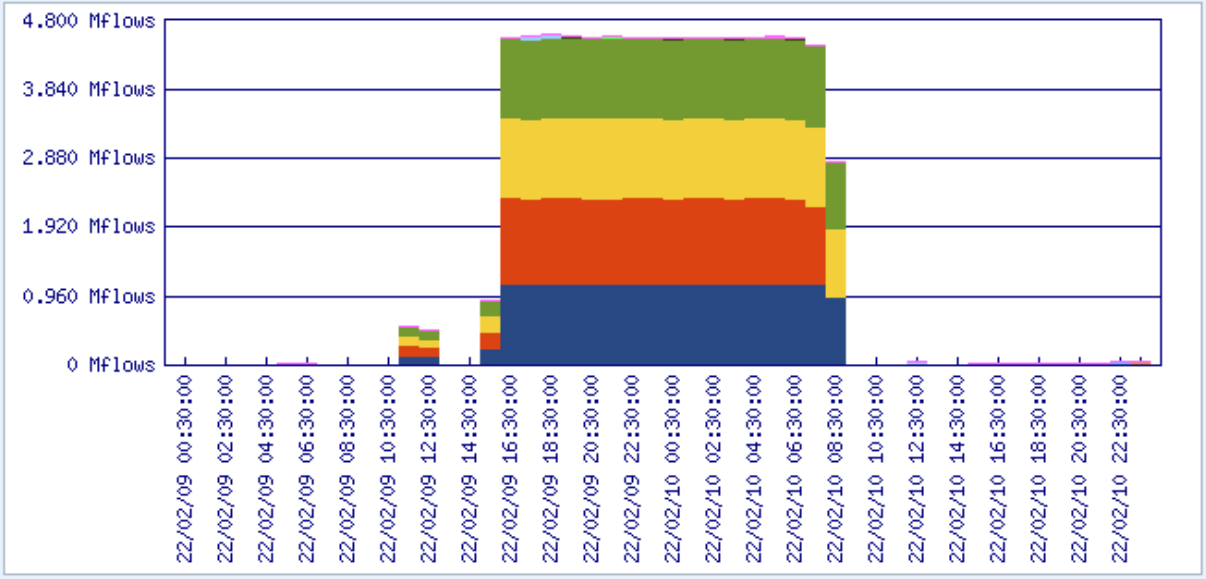


Flow-Cnt-Drop: *sums/time steps, 22/02/09 00:00:00-22/02/11 00:00:00, value per 1 hour, cumulative*

Summary

In graph	78.051 Mflows	99.58%
Rest of results	0.328 Mflows	0.42%
Total	78.379 Mflows	100.00%





o	>	Src-IP	Src-GeoIP	Flow-Start	Flow-End	Bytes-measured	Bytes-estimated	Pkts-measured	Pkts-estimated	Flow-Cnt	Flow-Cnt-Drop
1.	>	[redacted]		22/02/09 11:31:00.000	22/02/10 08:50:48.000	794.470 MB	794.470 MB	19.597 Mp	19.597 Mp	19589981	19502770
2.	>			22/02/09 11:29:52.000	22/02/10 07:54:28.000	791.902 MB	791.902 MB	19.691 Mp	19.691 Mp	19684338	19599917
3.	>			22/02/09 11:32:20.000	22/02/10 08:50:48.000	781.825 MB	781.825 MB	19.283 Mp	19.283 Mp	19276531	19190849
4.	>			22/02/09 11:31:30.000	22/02/10 08:50:42.000	780.890 MB	780.890 MB	19.257 Mp	19.257 Mp	19250179	19163519

Next activities and plans

- Standards and Best practice sharing
- Distributed CSIRT team
- Services
  - Redundant connectivity
  - Connection to private government network (eHealth)
  - Monitoring and Security tools, Community SIEM
  - Disaster recovery
  - Phishing tests
  - Community sharing platform
- Emergency platform and communication procedures
- Education and capacity building
- Community support and assistance
- Negotiations with Ministry of Health

cesnet

THANK YOU FOR THE ATTENTION

QUESTIONS?

Radovan Igliar
radovan@cesnet.cz