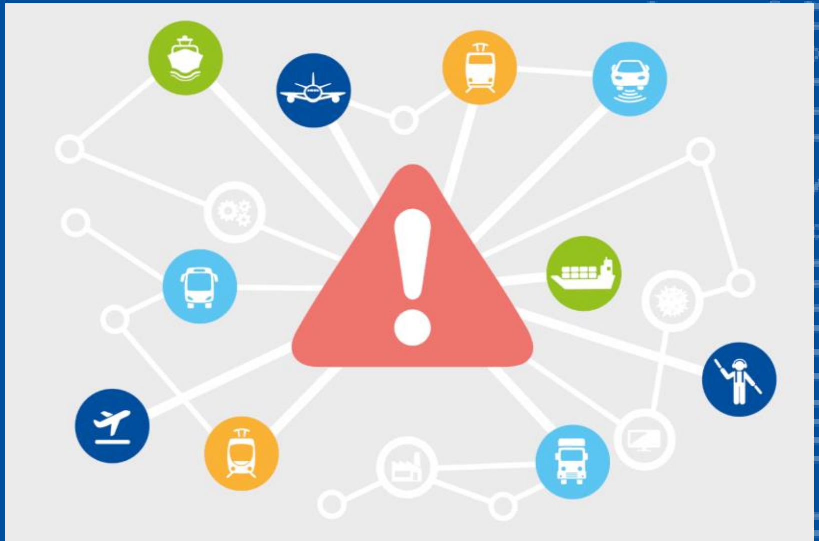
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE: TRANSPORT SECTOR



Marianthi Theocharidou

28 | 06 | 2023

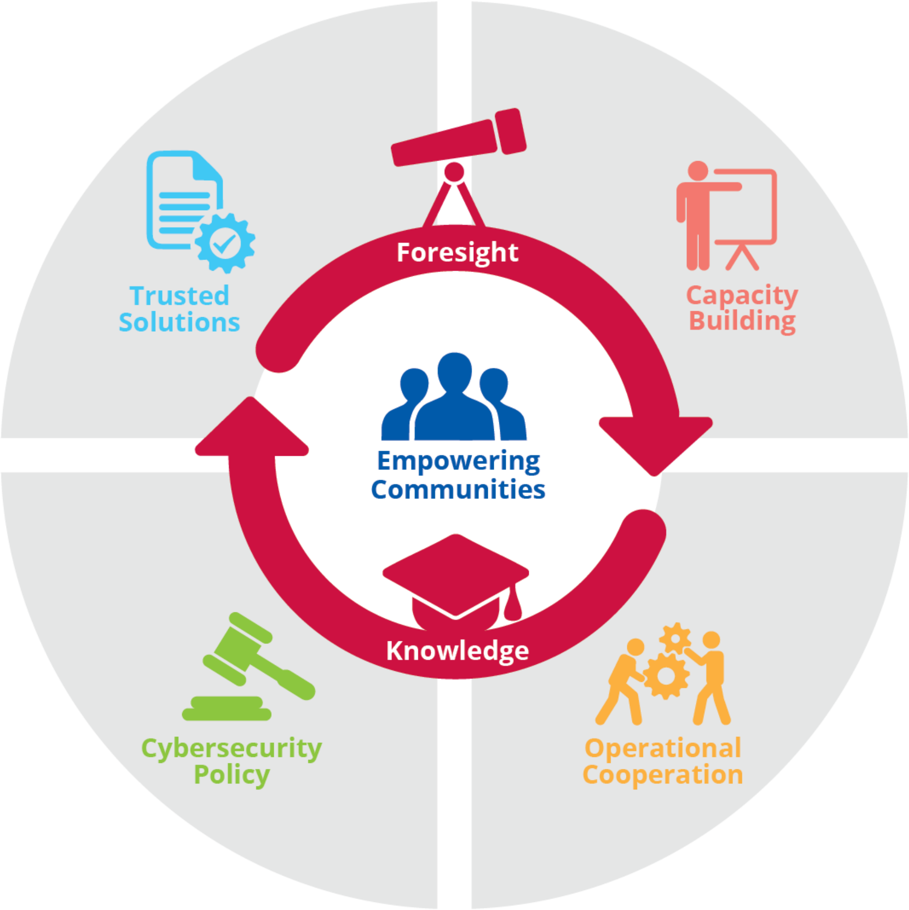
ROLE OF ENISA – WHO WE ARE

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve **a high common level of cybersecurity** across the Union in cooperation with the wider community



ENISA THREAT LANDSCAPE TRADITION

FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI) AND CYBERSECURITY THREAT LANDSCAPE

DECEMBER 2022

ENISA THREAT LANDSCAPE FOR 5G NETWORKS

Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)

DECEMBER 2020

AI CYBERSECURITY CHALLENGES

Threat Landscape for Artificial Intelligence

DECEMBER 2020

ENISA THREAT LANDSCAPE: TRANSPORT SECTOR

(January 2021 to October 2022)

MARCH 2023

ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

JULY 2021

ENISA THREAT LANDSCAPE 2021

April 2020 to mid-July 2021

OCTOBER 2021

ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS

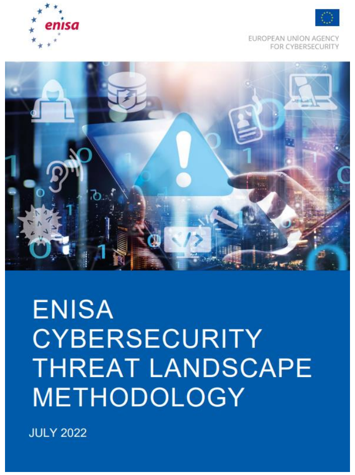
JULY 2022

ENISA THREAT LANDSCAPE 2022

(July 2021 to July 2022)

OCTOBER 2022

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
5G
THREAT LANDSCAPE
AI
CVE
ERROR



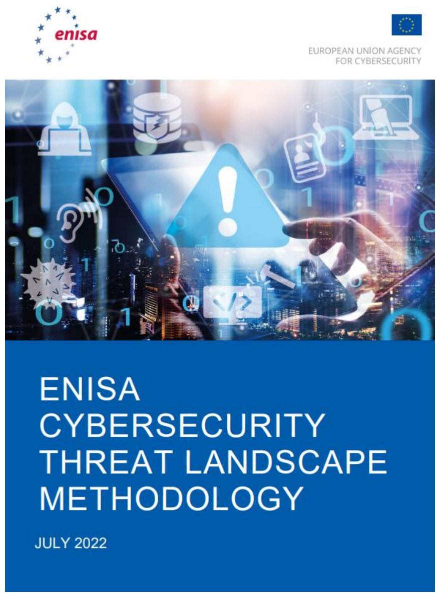
ENISA CYBERSECURITY THREAT LANDSCAPE METHODOLOGY

JULY 2022

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

It’s reflecting on the PAST to prepare for the FUTURE

METHODOLOGY

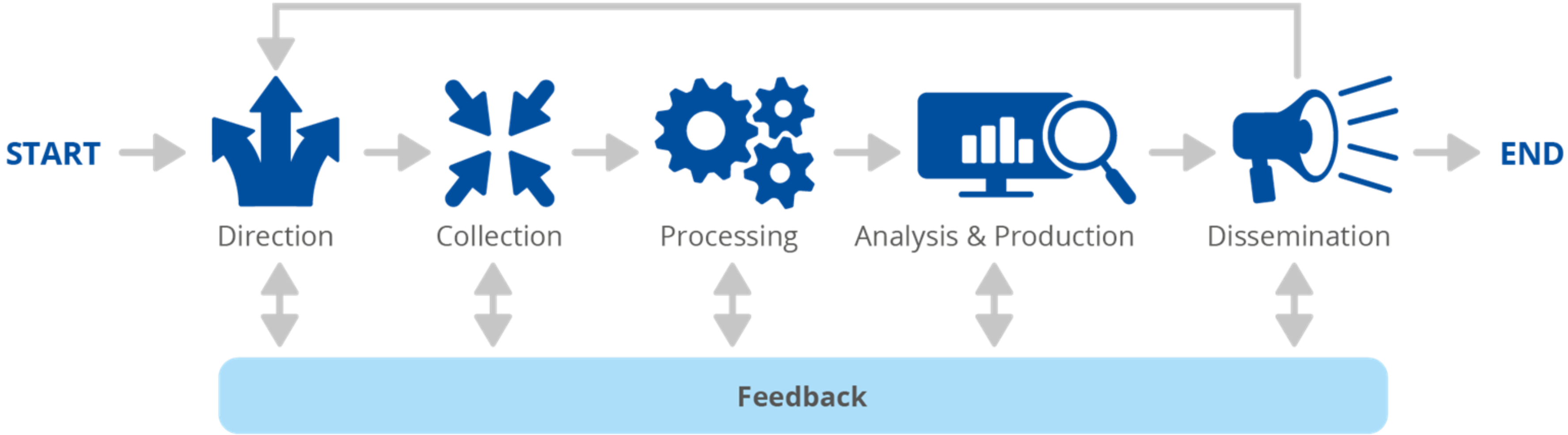


enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA CYBERSECURITY THREAT LANDSCAPE METHODOLOGY

JULY 2022



START → Direction → Collection → Processing → Analysis & Production → Dissemination → END

Feedback

- Collection based on open-source intelligence (OSINT) and ENISA's own cyber threat intelligence capabilities (situational awareness team, ETL team, two external experts)
- Processing, analysis and production: ENISA's threat landscape team with assistance of two experts

Disclaimer: The information provided in this presentation is based on publicly available data (OSINT) and on that provided by CTI contractors. It is intended to be used for Situational Awareness purposes within the scope of this presentation, and statements are limited to the reporting period of the analysis. Sources are referenced and verified to the possible extent on a best effort basis at the moment of reporting. Opinions expressed in referenced sources, if any, do not constitute an ENISA position.

SAMPLE

- **January 2021 to October 2022**
- **Analysis of the incidents concluded in December 2022**
- **98 publicly reported incidents**

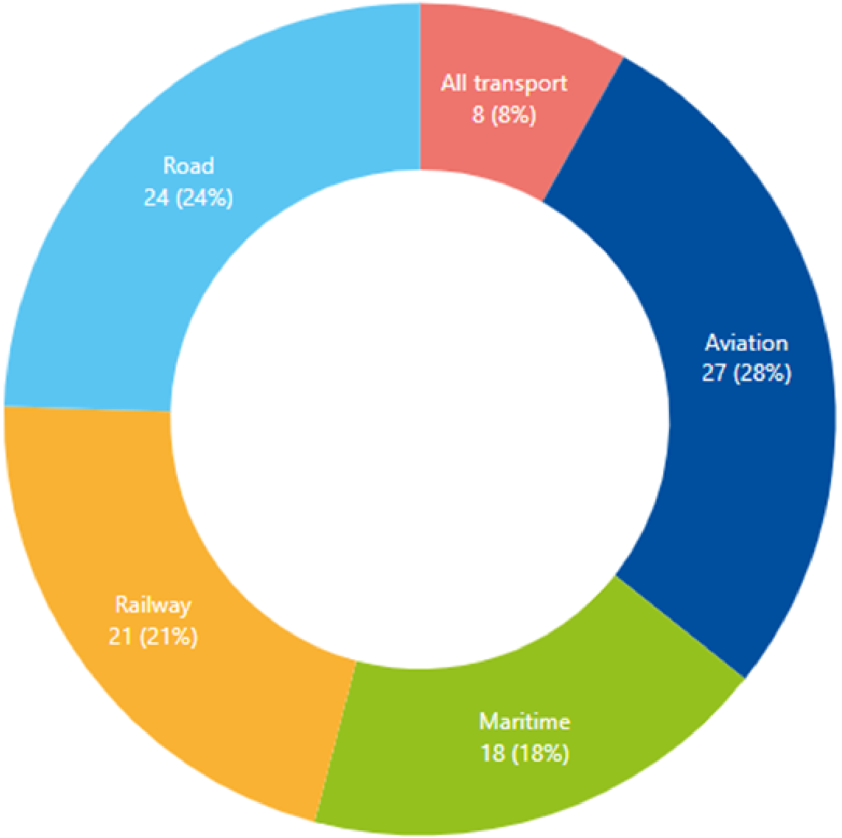
enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA THREAT LANDSCAPE: TRANSPORT SECTOR

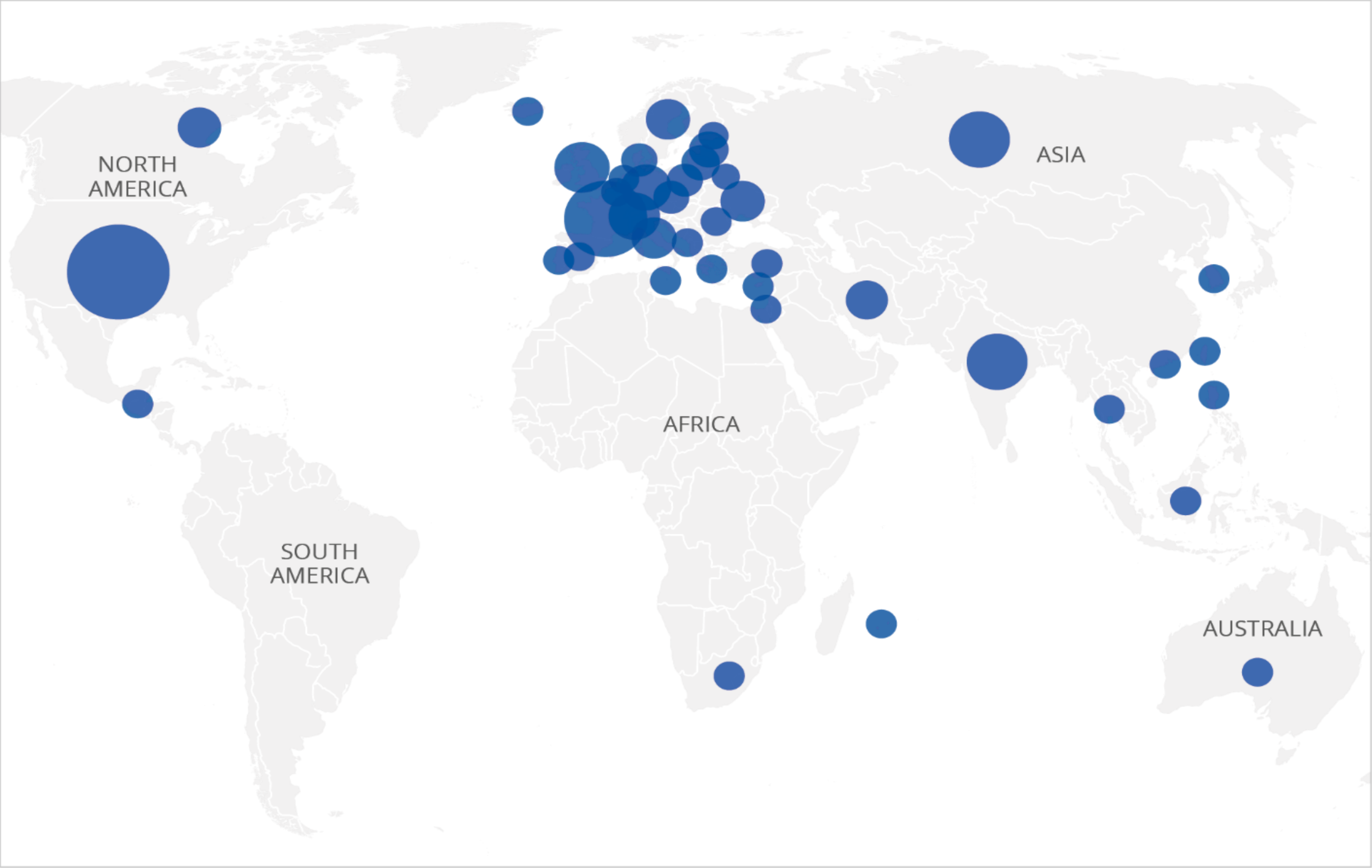
(January 2021 to October 2022)

MARCH 2023



https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

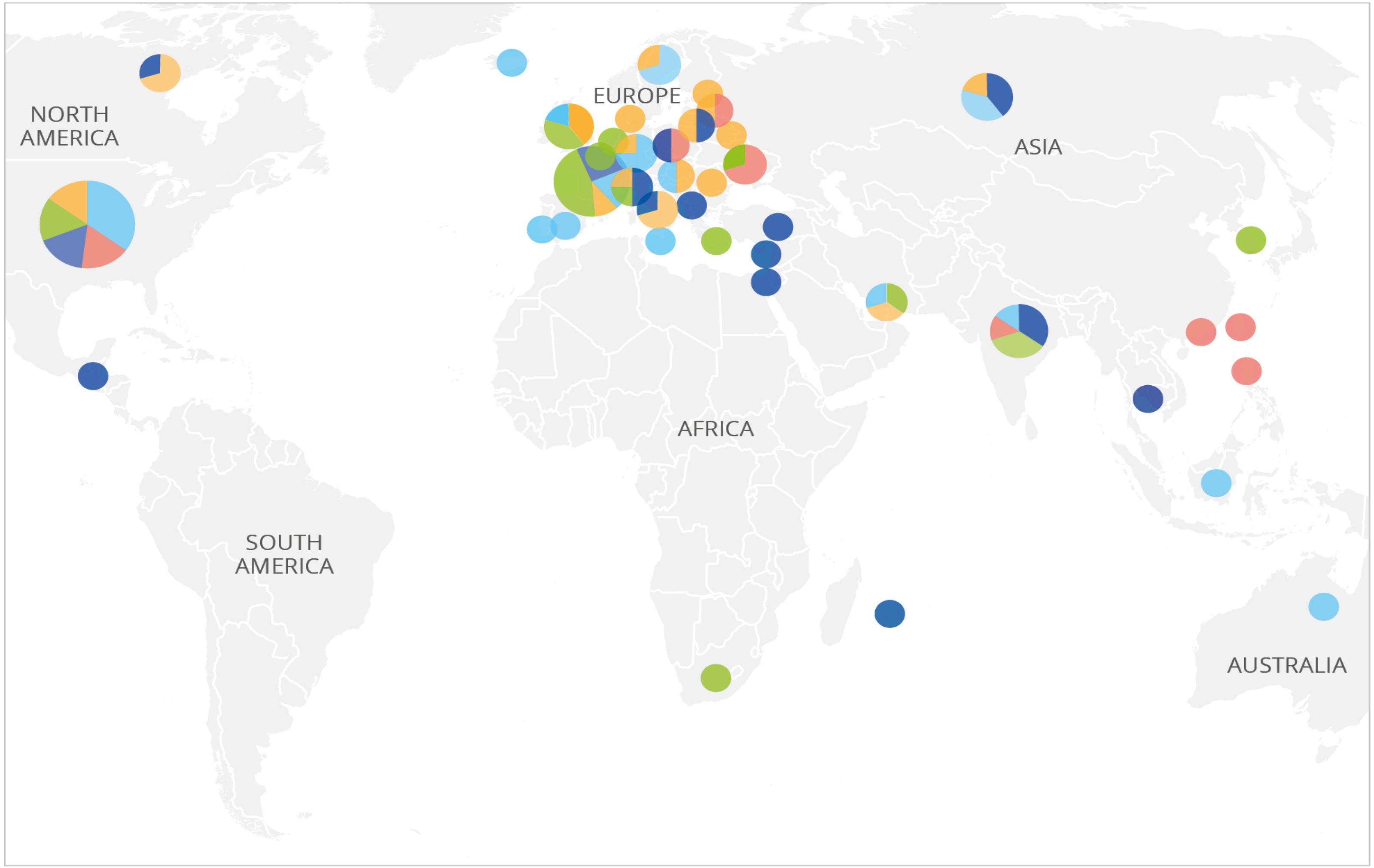
MAP OF OBSERVED INCIDENTS: TRANSPORT



Proximity:
Near (44),
Mid (10),
Far (38),
Global (6)

Note: the size of the circle refers to the sum of observed incidents in the country during the reporting period.

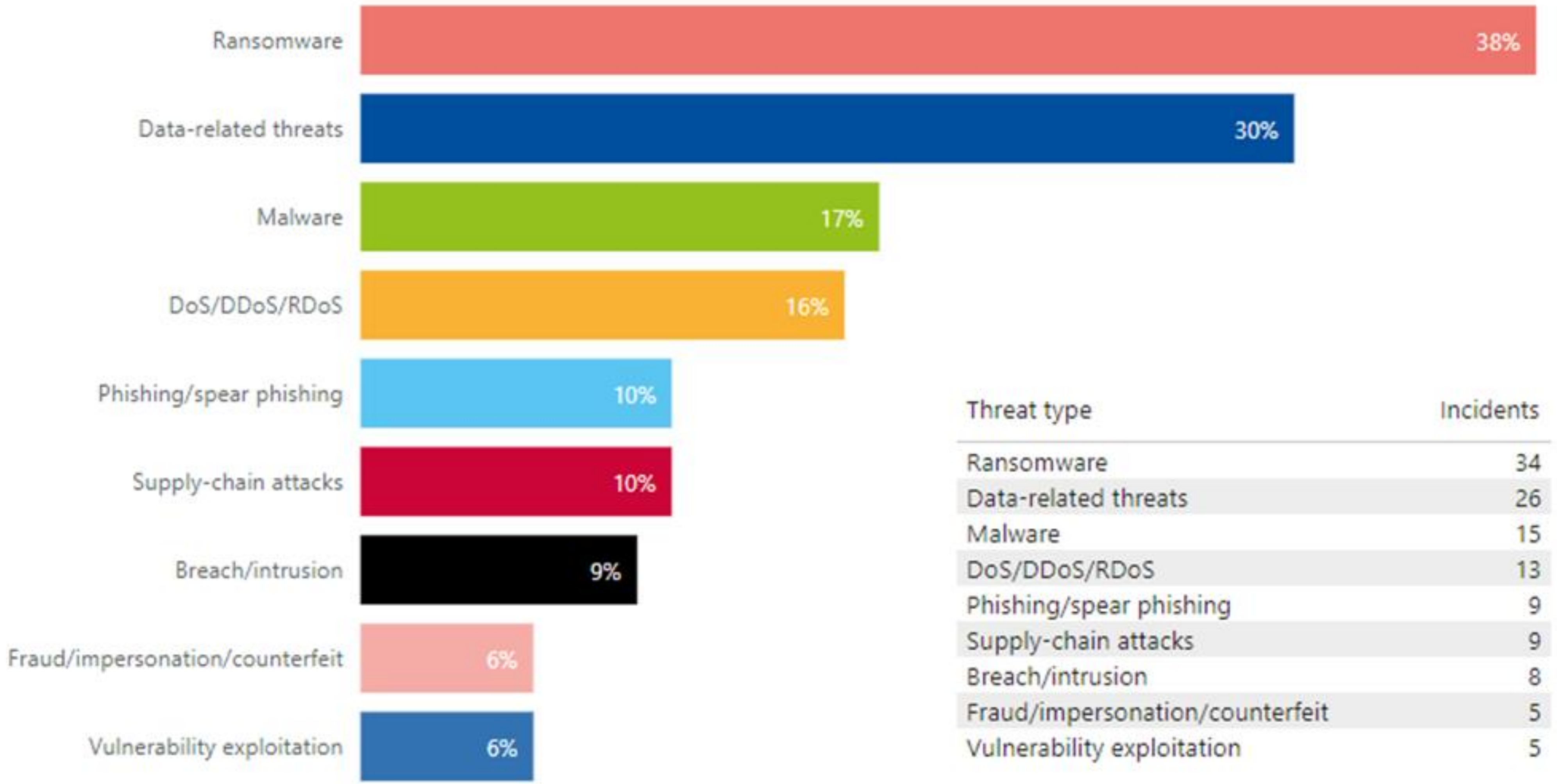
MAP OF OBSERVED INCIDENTS: PER SECTOR



Note: the size of the circle refers to the sum of observed incidents in the country during the reporting period.

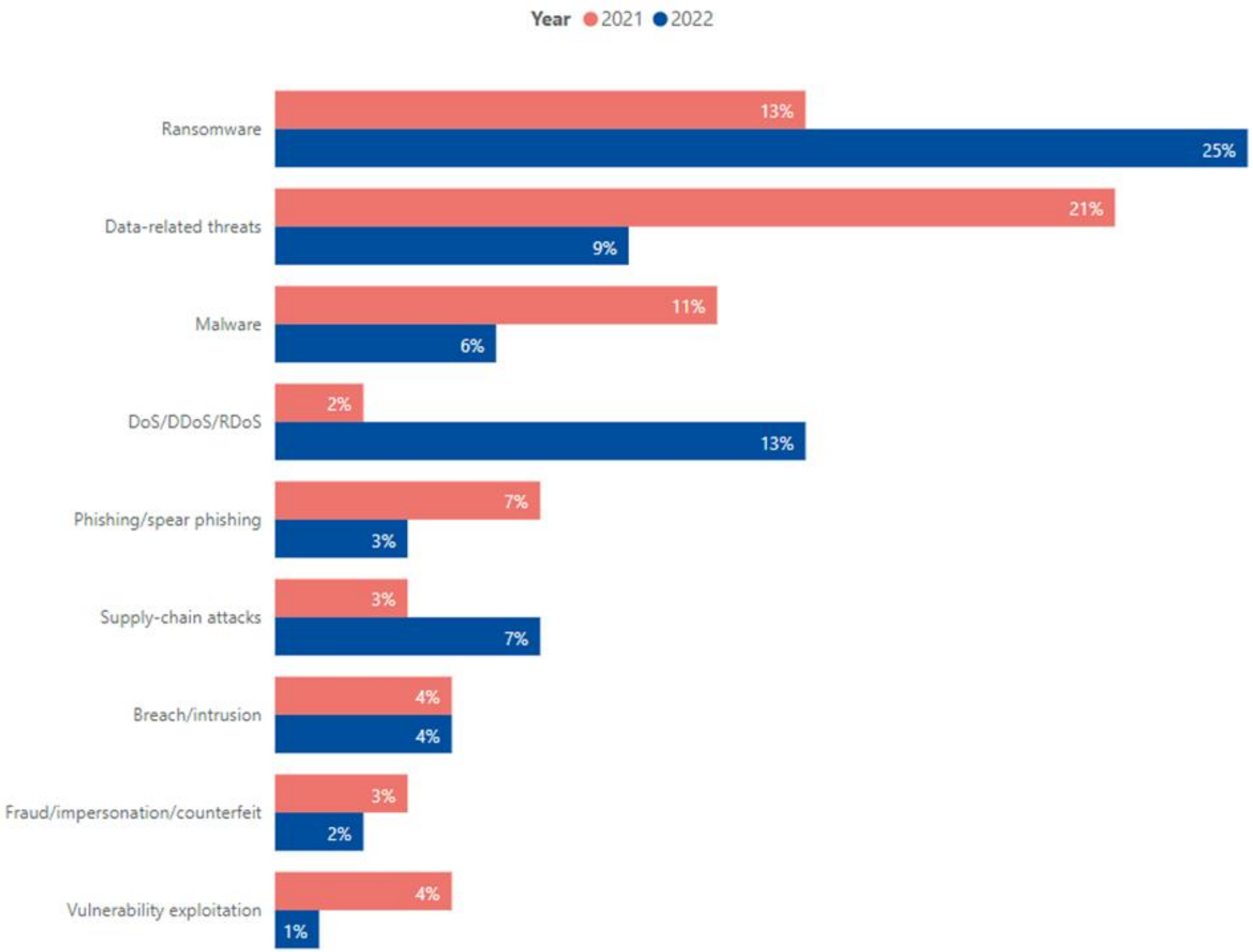
Sector
🟥 All transport 🟦 Aviation 🟩 Maritime 🟧 Railway 🟦 Road

TRANSPORT: THREATS



Threat type	Incidents
Ransomware	34
Data-related threats	26
Malware	15
DoS/DDoS/RDoS	13
Phishing/spear phishing	9
Supply-chain attacks	9
Breach/intrusion	8
Fraud/impersonation/counterfeit	5
Vulnerability exploitation	5

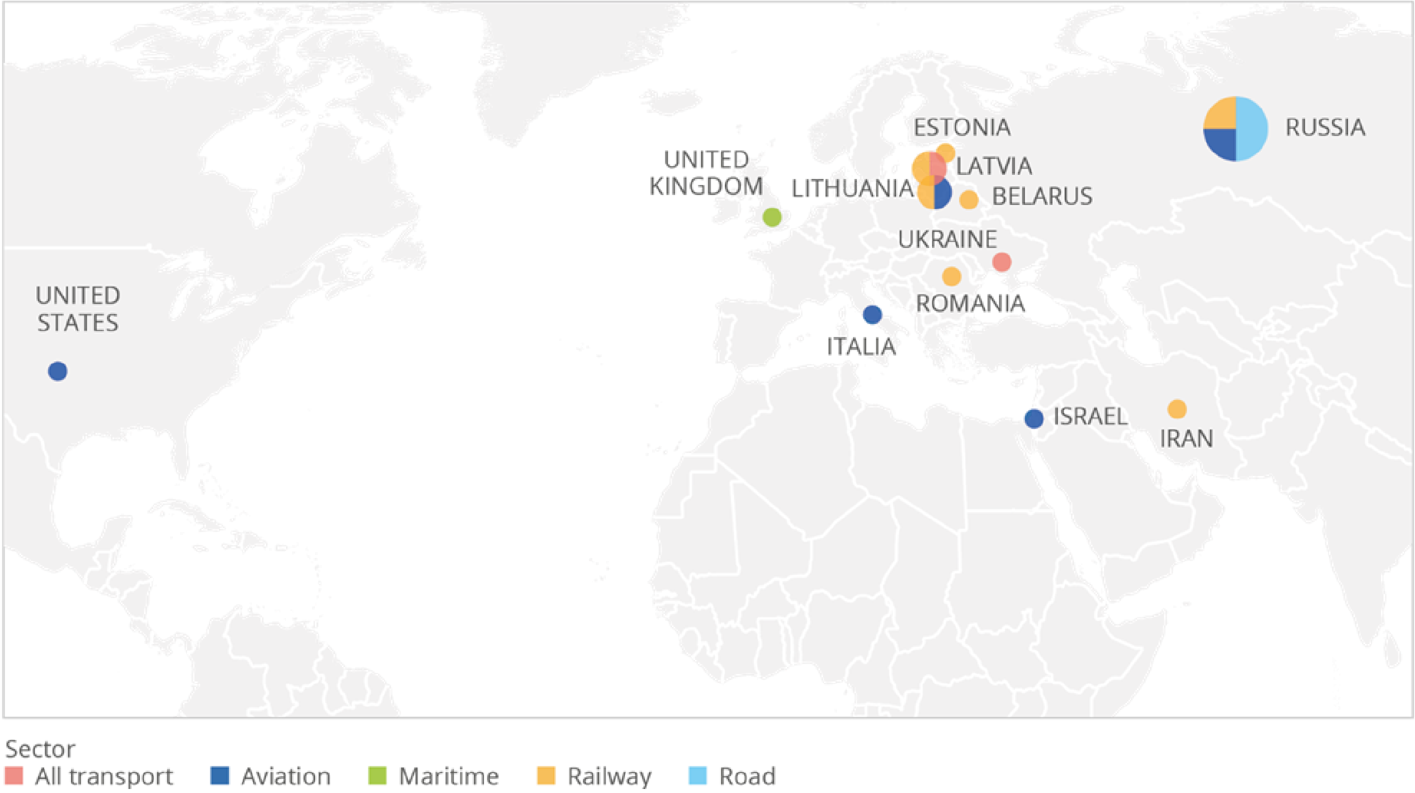
TRANSPORT: THREATS



Findings

- Reported **ransomware attacks almost doubled.**
- Decline **in malware incidents** in 2022 compared to 2021 (from 11% to 6%).
- **Data related threats** (breaches, leaks) declined compared to ransomware, but **remain significant**.
  - Targets: **credentials**, **personal data of employees and passengers**, **corporate data and intellectual property**.
- **DDoS attacks in 2022:**
  - due to increased activity by **hacktivists,**
  - are focused on specific regions, and
  - affected by current geopolitical tensions.

GLOBAL MAP OF INCIDENTS (HACKTIVISM)

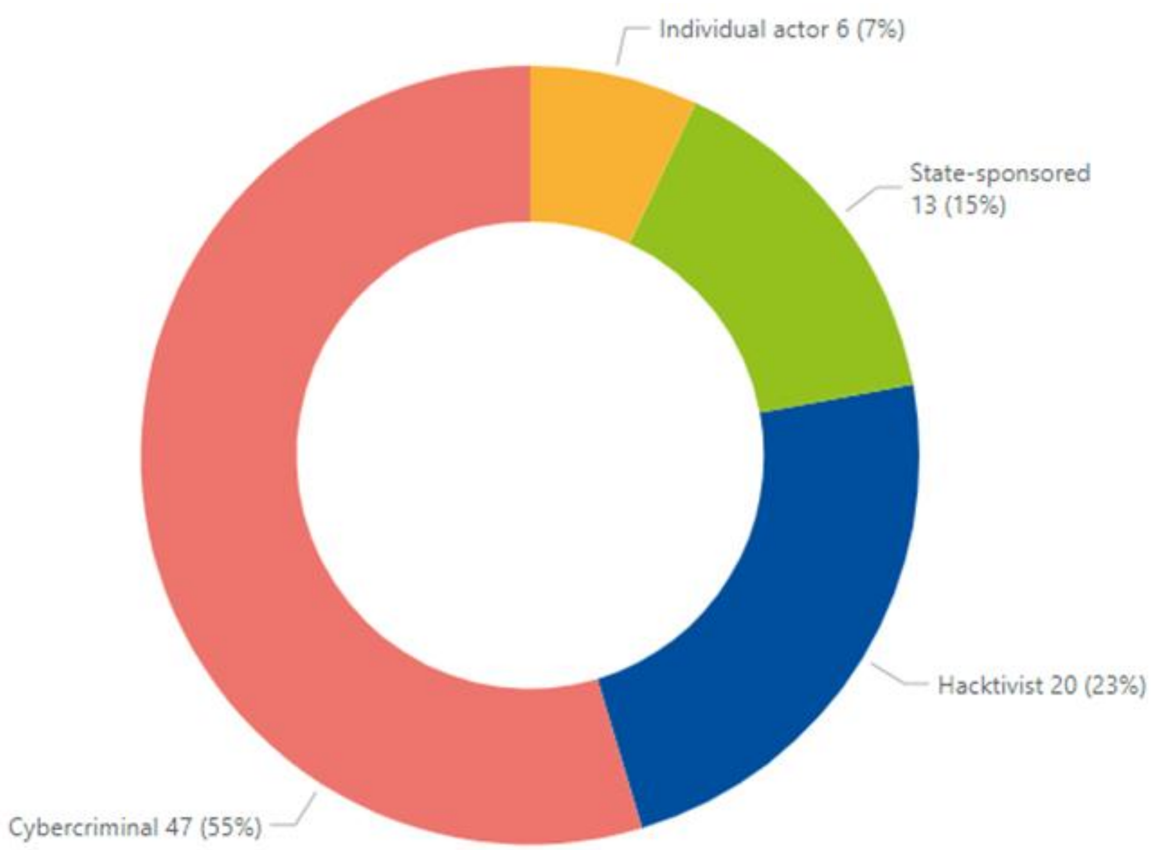


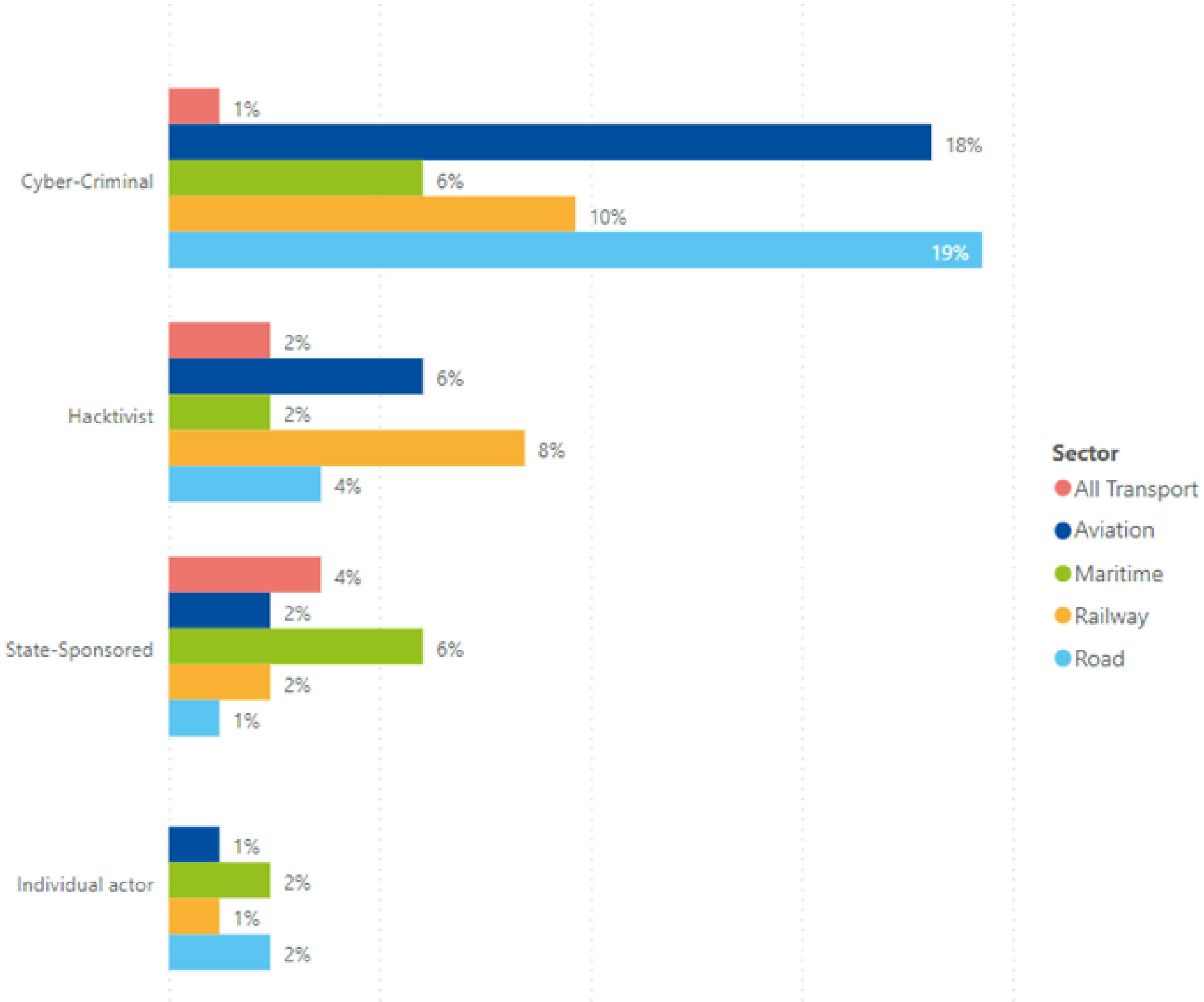
Note: the size of the circle refers to the sum of observed incidents in the country during the reporting period.

Geopolitical situation and its effect on the transport sector

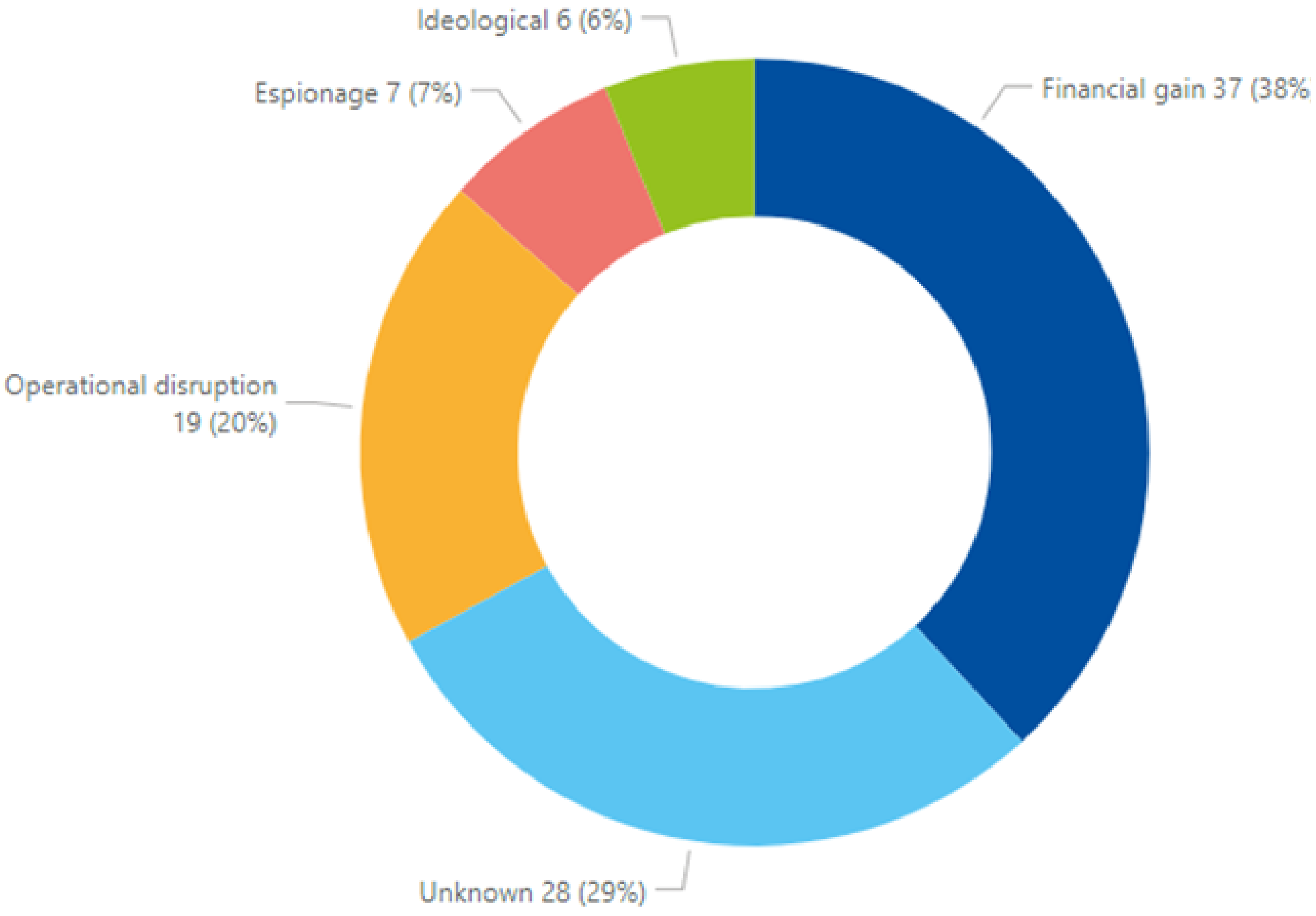
- Incidents in all transport sectors which were attributed to hacktivism.
- Motivation was primarily operational disruption and ideological.

ACTORS

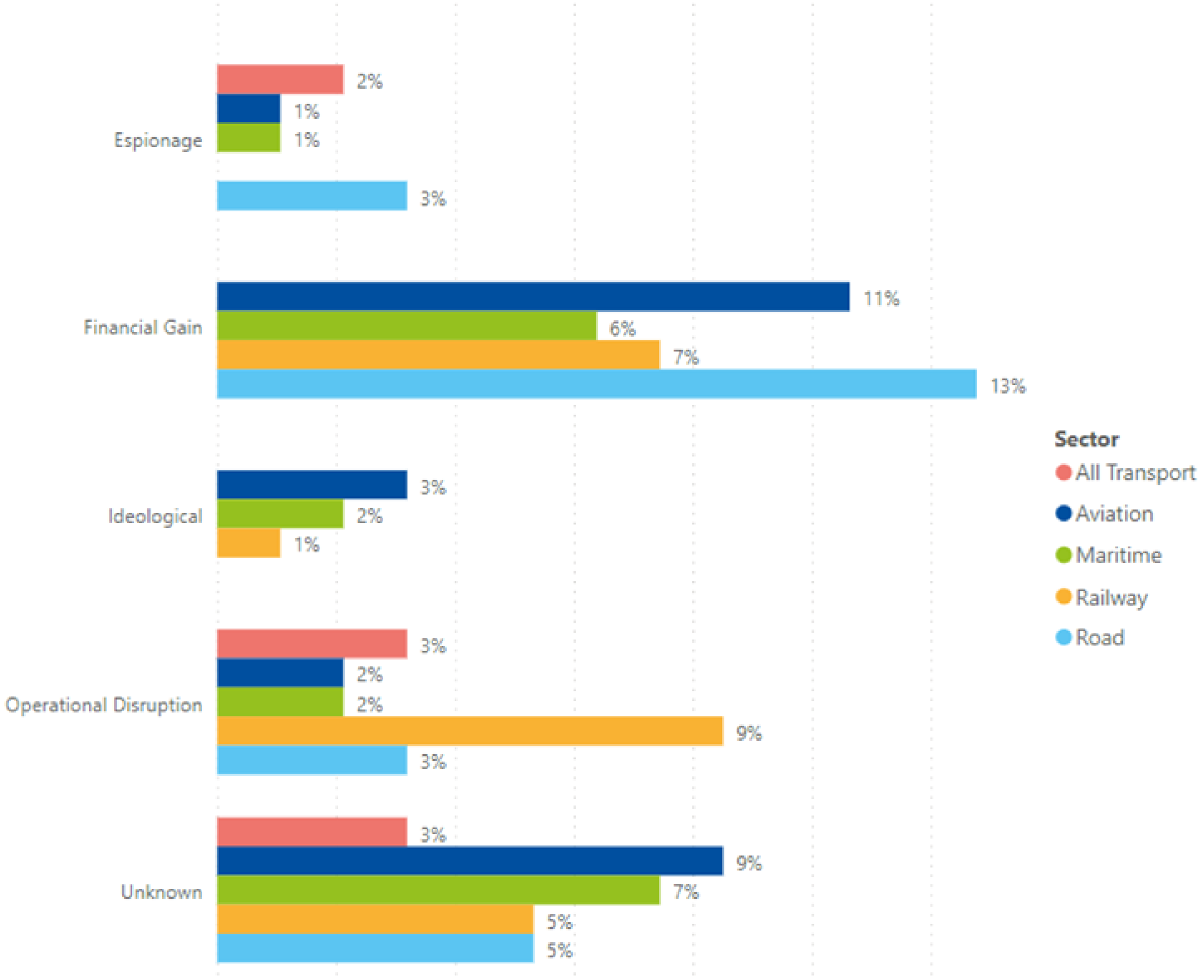

Individual actor 6 (7%)
State-sponsored 13 (15%)
Hacktivist 20 (23%)
Cybercriminal 47 (55%)


Cyber-Criminal
1%
18%
6%
10%
19%
Hacktivist
2%
6%
2%
8%
4%
State-Sponsored
4%
2%
6%
2%
1%
Individual actor
1%
2%
1%
2%
Sector
All Transport
Aviation
Maritime
Railway
Road

MOTIVATION

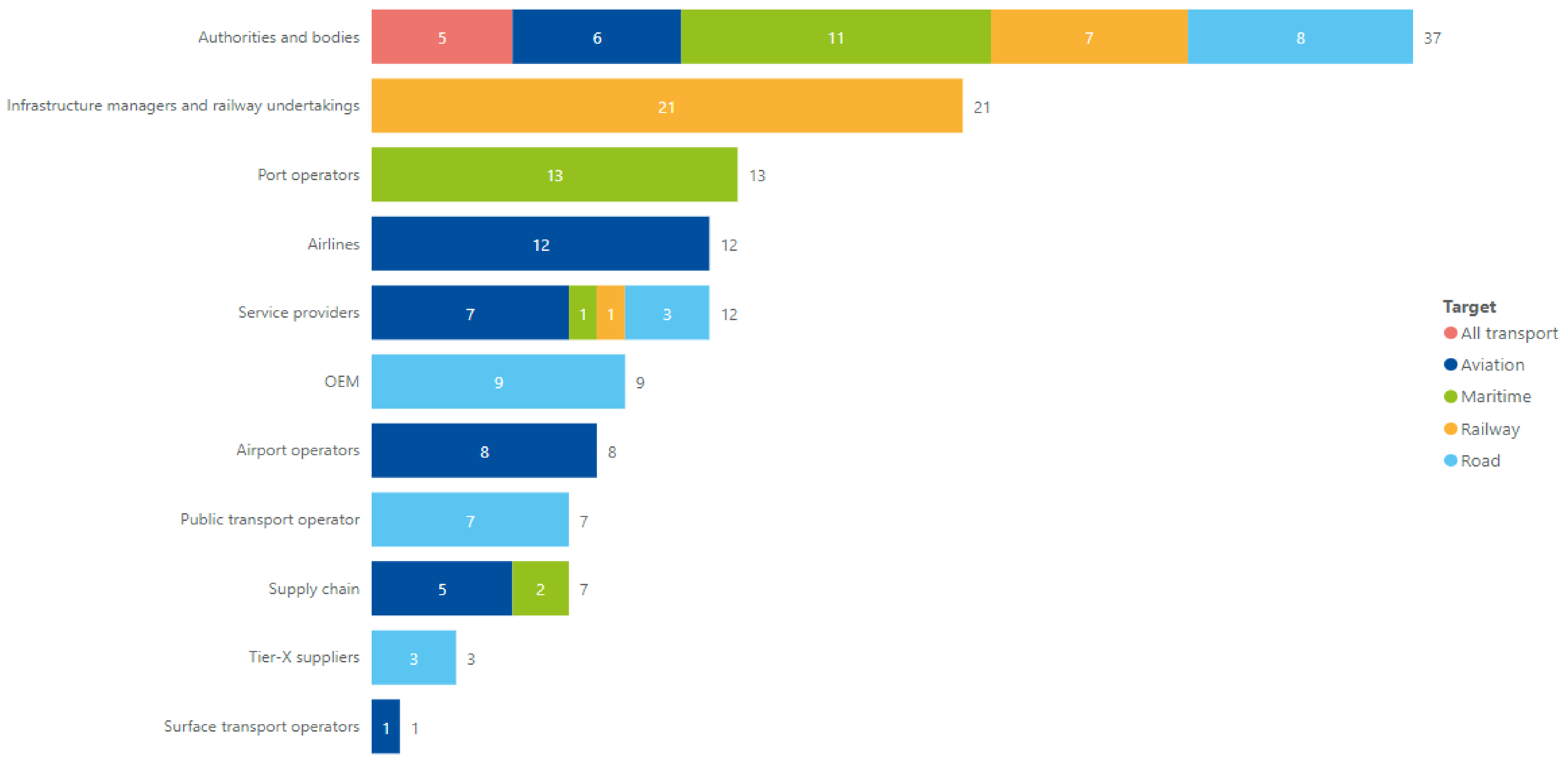


Ideological 6 (6%)
Espionage 7 (7%)
Financial gain 37 (38%
Operational disruption 19 (20%)
Unknown 28 (29%)



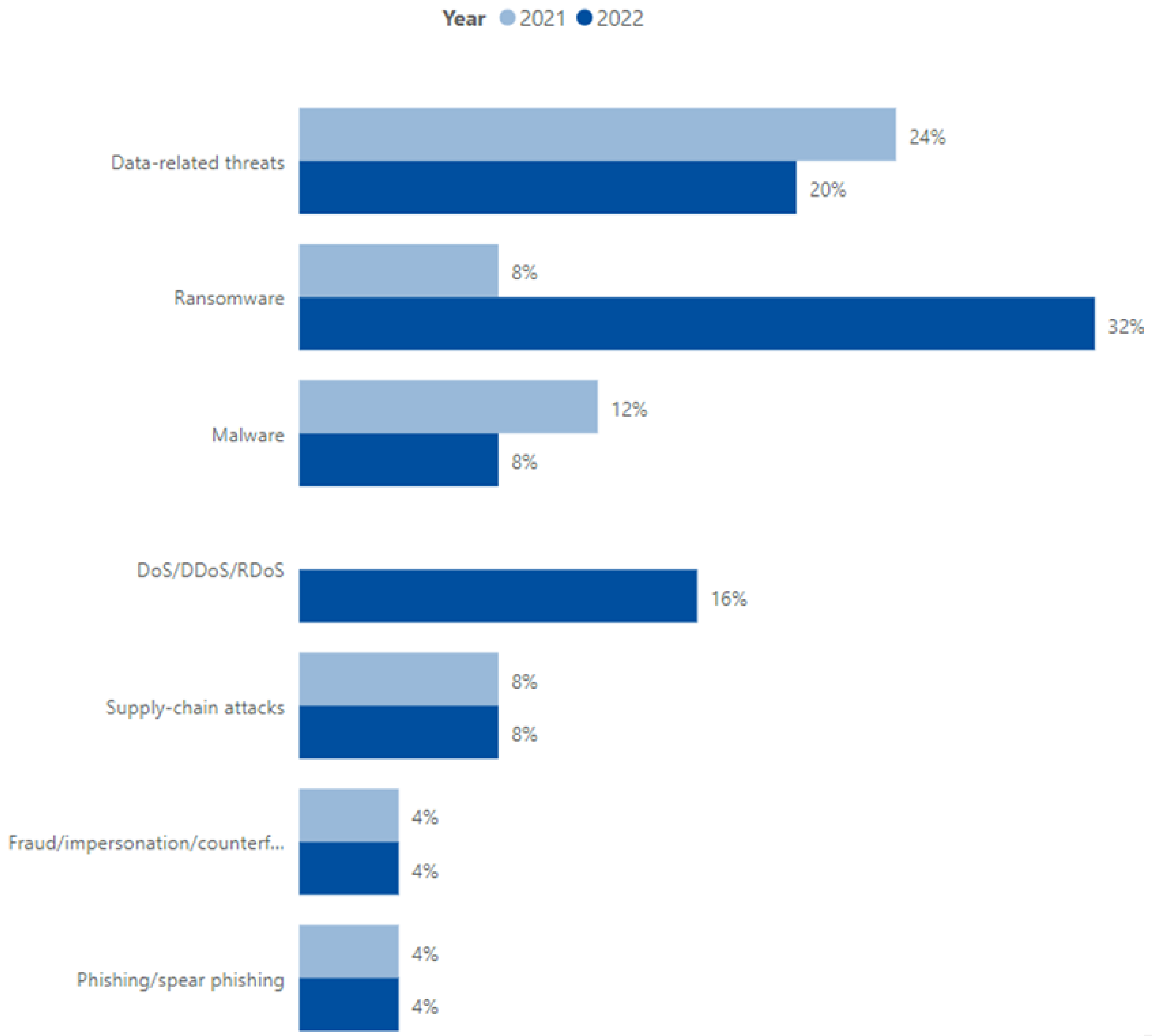
Espionage
2%
1%
1%
3%
Financial Gain
11%
6%
7%
13%
Ideological
3%
2%
1%
Operational Disruption
3%
2%
2%
9%
3%
Unknown
3%
9%
7%
5%
5%
Sector
● All Transport
● Aviation
● Maritime
● Railway
● Road

TARGETS



Authorities and bodies
5
6
11
7
8
37
Infrastructure managers and railway undertakings
21
21
Port operators
13
13
Airlines
12
12
Service providers
7
1
1
3
12
OEM
9
9
Airport operators
8
8
Public transport operator
7
7
Supply chain
5
2
7
Tier-X suppliers
3
3
Surface transport operators
1
1
Target
All transport
Aviation
Maritime
Railway
Road

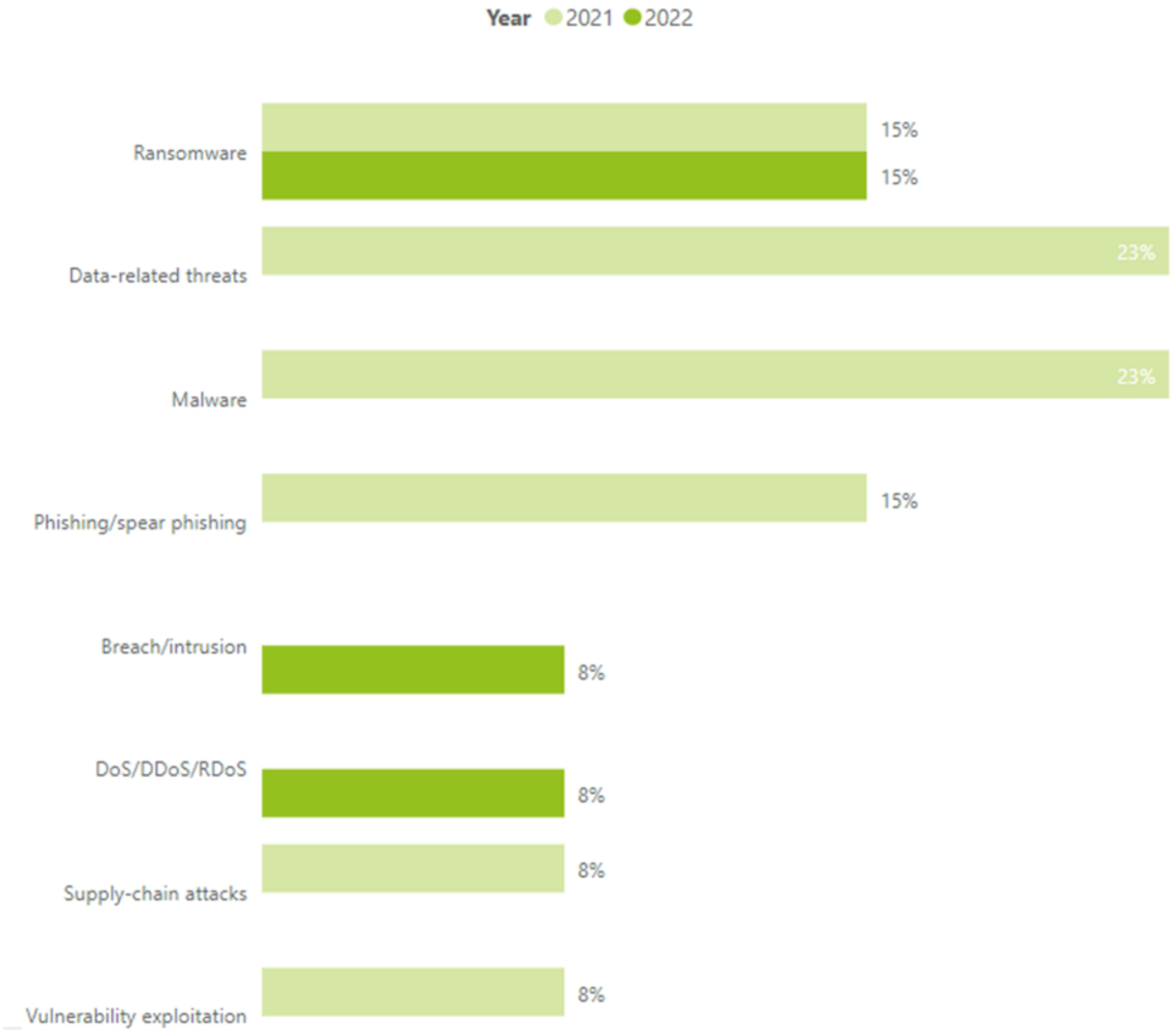
AVIATION



Findings

- In 2022, an increase in the number of ransomware attacks affecting airports.
- The main threat which is being reported to Eurocontrol is fraudulent websites impersonating airlines. From January 2022 to June 2022, fraudulent websites accounted for 46% of incidents reported to Eurocontrol.
- DDoS attacks were primarily observed by ENISA in 2022 and were linked with hacktivist activity against airports and aviation authorities.
- Airspace users/airlines are the main victims of attacks (systems and customers are targeted)

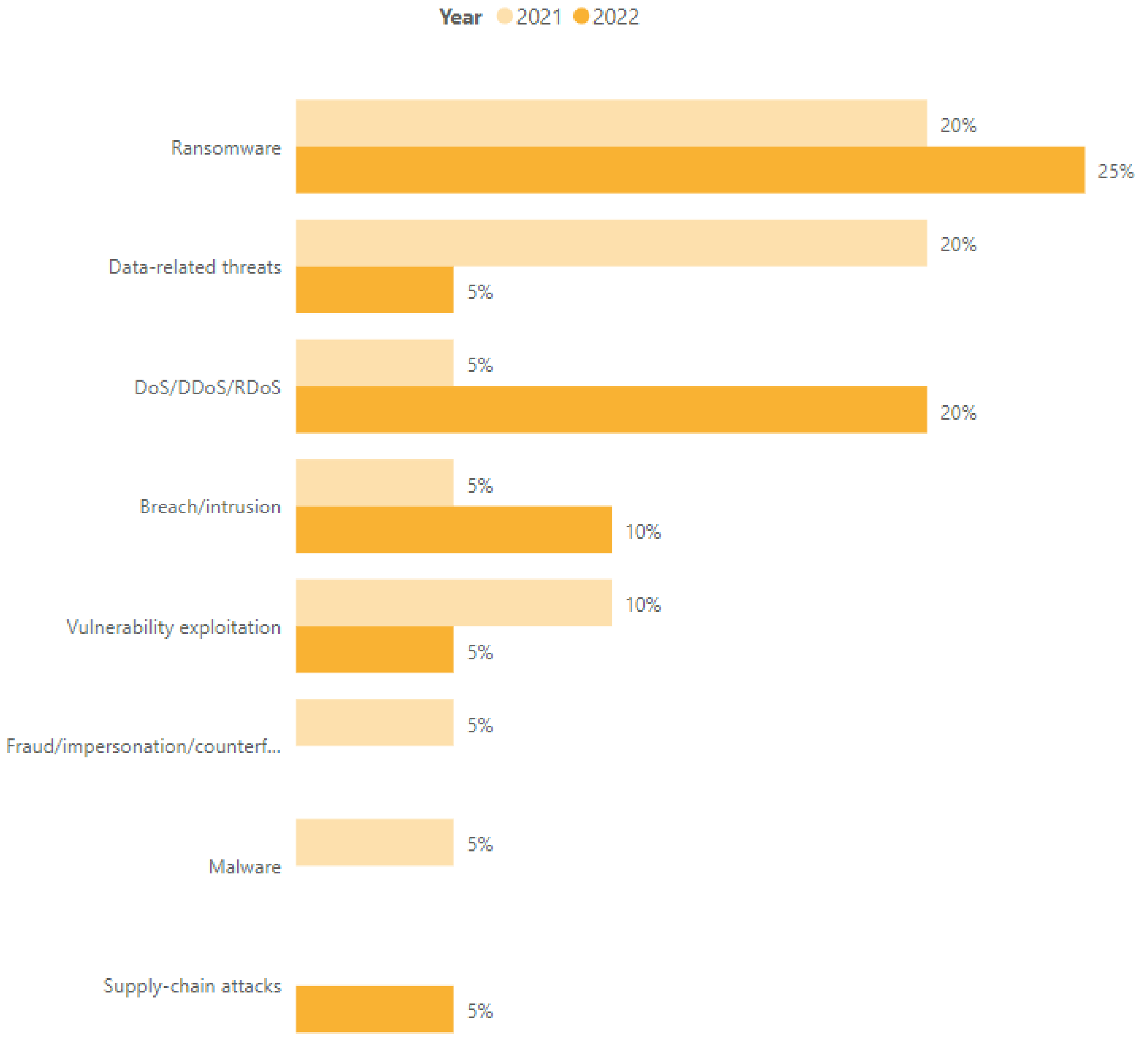
MARITIME



Findings

- State-sponsored attackers: politically motivated attacks targeting ports and vessels
  - Spoofing of the automatic identification system by a hostile state
- Cyber criminals: Ransomware, malware and phishing / spear-phishing attacks targeting:
  - port authorities,
  - port operators or
  - manufacturers (supply chain)
- Major disruptions in ports where we lack information on what type of attack took place (South Africa 2021, Northern EU oil hubs 2022).

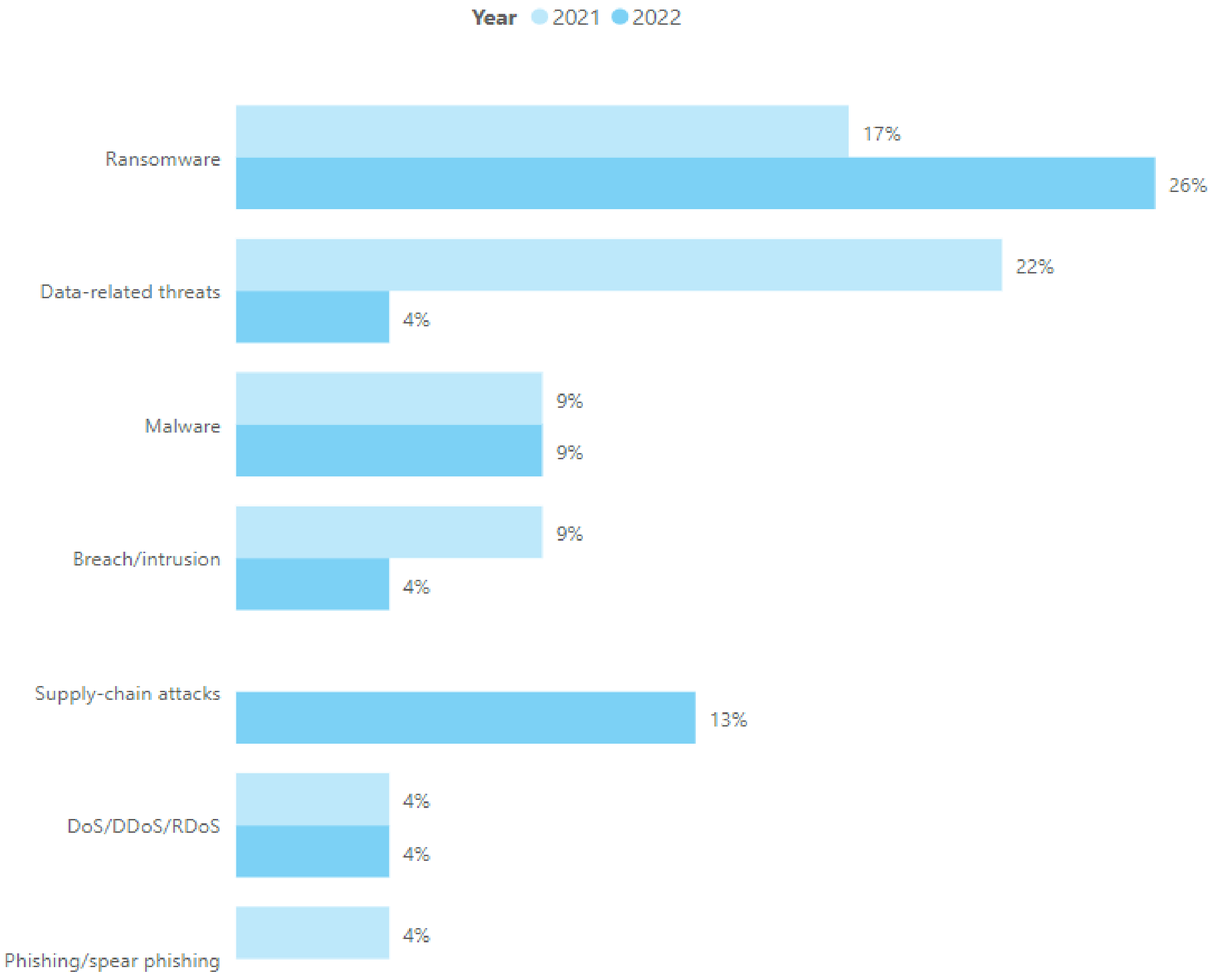
RAILWAY



Findings

- IT systems being targeted (passenger services, ticketing systems, mobile application, display boards, etc.): disruptions due to the unavailability of IT services.
- Notable data thefts
- OT systems and networks affected:
  - Only when entire networks were down or when safety-critical IT systems were unavailable, e.g. service disruptions to the a train operator due to an attack on one of its ICT service providers (DDoS attack).
- DDoS attacks on the rise in 2022, reaching one fifth of the attacks on the railway sector (20%).
  - Hacktivists launching ransomware attack.

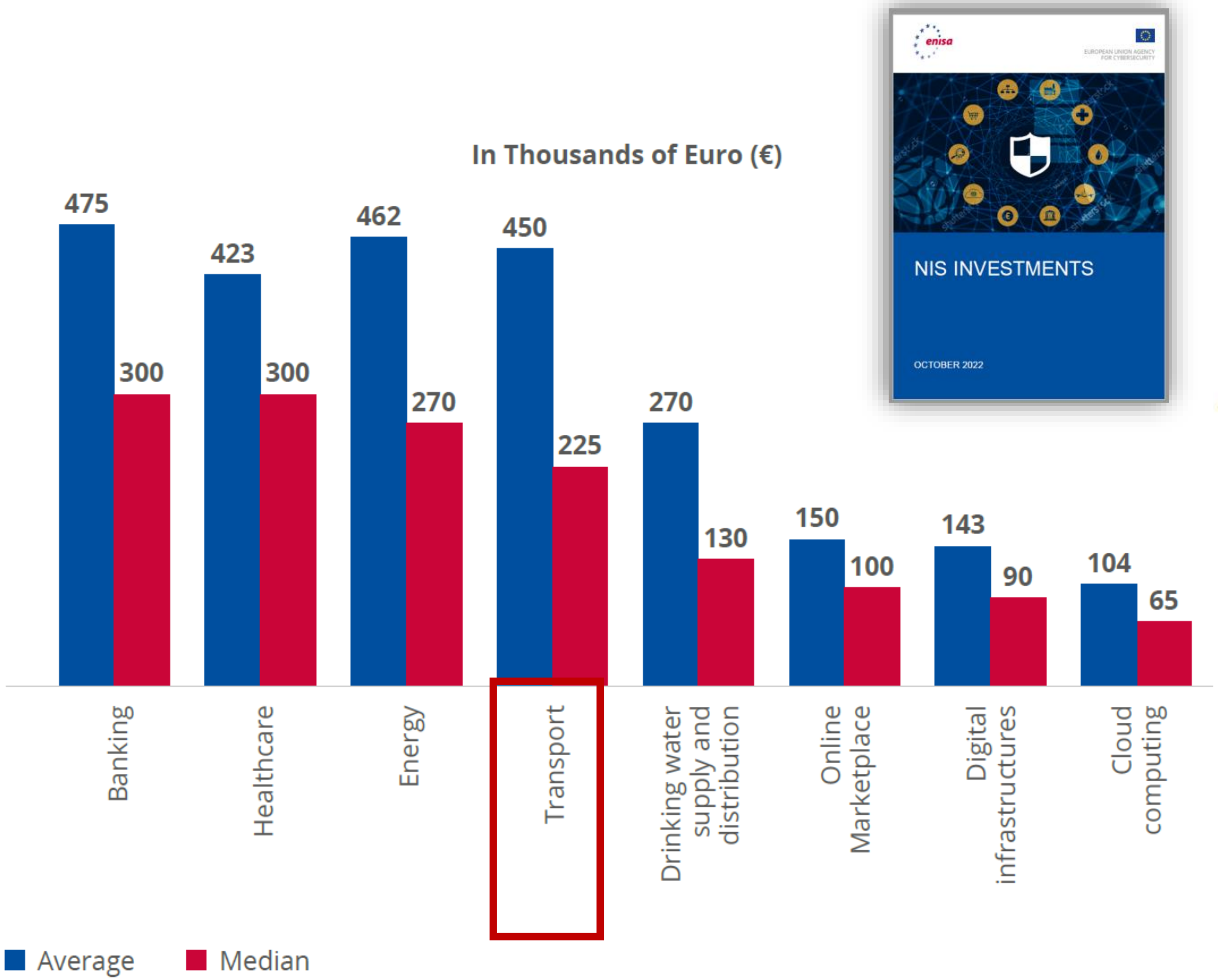
ROAD

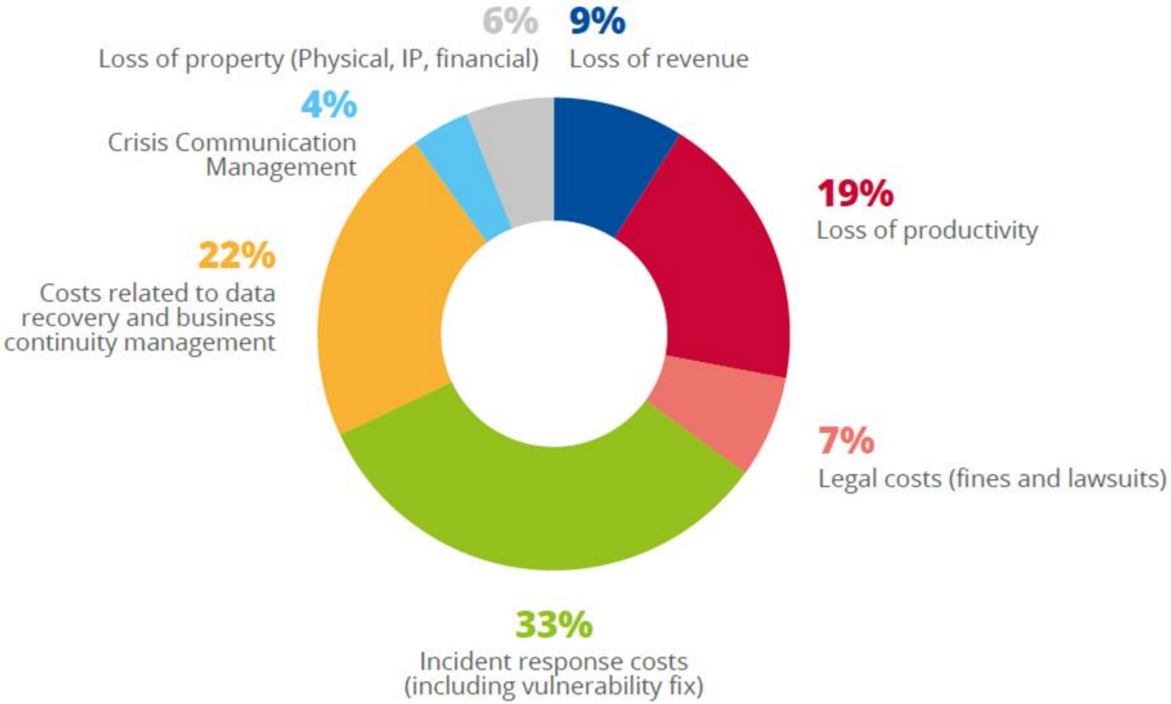


Findings

- Ransomware has targeted the automotive industry, in particular OEMs and tier-X suppliers. In some cases, the production of vehicles or parts had to stop due to an attack.
- Notable cases of proprietary information being stolen or leaked from OEMs and tier-X suppliers.
- Data-related threats primarily targeted IT systems in an effort to acquire customer or employee data and proprietary information.

COST OF INCIDENTS





The estimated median direct cost of a major security incident is EUR 225 000.

FINDINGS & ASSESSMENT

Ransomware attacks became the most significant threat against the sector during 2022.

- Surpassing data-related threats
- Ransomware groups opportunistic and relatively indiscriminate in their targeting.
- Not only monetary motivations (hacktivism)

The significant increase in hacktivist activity and the increasing rate of DDoS attacks are highly likely to continue.

- Main targets were European airports, railways and transport authorities.

Majority of attacks to the transport sector target IT systems

- They can result in operational disruptions.

We have not received reliable information on a cyber-attack affecting the safety of transport.

Ransomware groups will likely target and disrupt OT operations in the foreseeable future.

We have not observed notable **attacks on global positioning systems**, the potential effect of this type of threat to the transport sector remains a concern.

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

☎

✉ etl@enisa.europa.eu

🌐 www.enisa.europa.eu