EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE: TRANSPORT SECTOR

(January 2021 to October 2022)

MARCH 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at: www.enisa.europa.eu.

CONTACT

To contact the authors, please use etl@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Marianthi Theocharidou, Zoran Stanic, Athanasios Drougkas, Ricardo De Sousa Figueiredo, Eleni Tsekmezoglou, Rossen Naydenov, Ifigeneia Lella, Apostolos Malatras, ENISA

CONTRIBUTORS

Jasmin Ćosić, DEKRA SE

Marius Iulian Mihailescu, Spiru Haret University

ACKNOWLEDGEMENTS

We would like to thank the Members and Observers of the ENISA ad hoc Working Group on Cyber Threat Landscapes and the members of the Transport Resilience and Security Expert Group for their valuable feedback and comments in validating this report. We would like to thank the European Union Aviation Safety Agency and Eurocontrol's European Air Traffic Management Computer Emergency Response Team for contributing with incident data to this document.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-624-8, DOI:10.2824/553997, TP-04-23-081-EN-N

CONTENTS

EXECUTIVE SUMMARY

This is the first analysis conducted by the European Union Agency for Cybersecurity (ENISA) of the cyber threat landscape of the transport sector in the EU. The report aims to bring new insights into the reality of the transport sector by mapping and studying cyber incidents from January 2021 to October 2022. It identifies prime threats, actors and trends based on the analysis of cyberattacks targeting aviation, maritime, railway and road transport over a period of almost 2 years.

During this period, the prime threats identified include:

- ransomware attacks (38%),
- data related threats (30%),
- malware (17%),
- denial-of-service (DoS), distributed denial-of-service (DDoS) and ransom denial-of-service (RDoS) attacks (16%),
- phishing / spear phishing (10%),
- supply-chain attacks (10%).

During the reporting period, the threat actors with the biggest impact on the sector were state-sponsored actors, cybercriminals and hacktivists. We observed the following trends:

- Ransomware attacks became the prominent threat against the sector in 2022. Ransomware has been steadily increasing[1] and the transport sector has been affected similarly to the other sectors.
- Cybercriminals are responsible for the majority of attacks on the transport sector (54%), and they target all subsectors.
- Threat actors will increasingly conduct ransomware attacks with not only monetary motivations[1].
- The increased hacktivist activity targeting the transport sector is likely to continue.
- The increasing rate of DDoS attacks targeting the transport sector is likely to continue.
- The main targets of DDoS attacks by hacktivists are European airports, railways and transport authorities.
- During this reporting period, we did not receive reliable information on a cyberattack affecting the safety of transport.
- The majority of attacks on the transport sector target information technology (IT) systems. Operational disruptions can occur as a consequence of these attacks, but the operational technology (OT) systems are rarely being targeted.
- Ransomware groups will likely target and disrupt OT operations in the foreseeable future[1].

The aviation sector is facing multiple threats, with data-related threats being the most prominent, coupled by ransomware and malware. Customer data of airlines and proprietary information of original equipment manufacturers (OEM) are the prime targeted assets of the sector. In 2022, there has been a rise in the number of ransomware attacks affecting airports. Fraudulent websites impersonating airlines have become a significant threat in 2022.

The maritime sector experiences ransomware, malware, and phishing attacks targeted towards port authorities, port operators, and manufacturers. State-sponsored attackers often carry out politically motivated attacks leading to operational disruptions at ports and vessels.

The railway sector also experiences ransomware and data-related threats primarily targeting IT systems like passenger services, ticketing systems, and mobile applications, causing service disruptions. Hacktivist groups have

[1] ENISA Threat Landscape 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

been conducting DDoS attacks against railway companies with an increasing rate, primarily due to Russia's invasion of Ukraine.

The road transport sector faces predominantly ransomware attacks, followed by data-related threats and malware. Automotive industry, especially OEM and tier-X suppliers, has been targeted by ransomware leading to production disruptions. Data-related threats primarily target IT systems to acquire customer and employee data as well as proprietary information.

There is a limited number of cyber incidents that cannot be placed in one specific subsector. These include general campaigns targeting the whole transportation sector in particular countries. These campaigns are often attributed to hacktivists and state-sponsored actors and are linked to geopolitical tensions.

The report also highlights issues with the reporting of cyber incidents and the fact that we still have limited knowledge and information regarding such incidents. The analysis in this report indicates that publicly disclosed incidents are just the tip of the iceberg.

1. INTRODUCTION

This report brings insights into the cyber threat landscape of the transport sector, with a focus on the EU. The four transport sectors which are considered in scope are aviation, maritime[2], rail, and road transport, as these fall under the scope of the network and information security (NIS) directive[3]. The report considers a wider scope of the transport ecosystem, and includes transport manufacturers and suppliers[4], and national transport authorities, to ensure that the threat landscape of the sector is more detailed.

The ENISA Cybersecurity Threat Landscape Methodology[5] was applied. ENISA has analysed cyber incidents targeting the transport sector from January 2021 to October 2022. This time period is referred to as the "reporting period" throughout the report.

It should be noted that the data collection and analysis primarily focus on incidents observed in EU member states and then in other states around the world. This is by no means the complete list of incidents that occurred during the reporting period. ENISA gathered a list of major incidents based on open-source intelligence (OSINT)[6] and ENISA's own cyber threat intelligence capabilities. For the aviation sector specifically, these were complemented by incidents reported to EASA and the European Centre for Cybersecurity in Aviation[7], and by incidents provided by Eurocontrol's EATM-CERT for the aviation sector[8]. The data collected were further analysed by ENISA's threat landscape team.

These incidents serve as the foundation for identifying the list of prime threats and the source material for several trends and statistics in the report. The incidents were analysed in detail to identify their core elements, providing answers to some important questions, such as how the attacks happen, which systems are being targeted and which transport subsectors are most affected. An in-depth desk research of available literature from open sources, such as news media articles, expert opinions, intelligence reports, incident analyses and security research reports, were conducted by ENISA and external experts. Within the report, we differentiate between what has been reported by our sources and what is our assessment. When conducting an assessment, we convey probability by using words that express an estimate of probability [9].

The report is structured as follows.

- Chapter 1, Introduction, provides an overview of the scope and the method used to produce this report.
- Chapter 2, Cyber threats to the transport sector, analyses the observed activity observed during the reporting period. It provides insights on the prime threats, threat actors and their motivation, along with the assessed impact of these attacks.
- Chapter 3, Sector Analysis, analyses in more detail the prime threats and the targets on each of the four subsectors covered.
- Chapter 4, Conclusions, discusses the trends derived by the analysis and some considerations on the availability of data for incidents affecting the sector.
- Annex, Major incidents, gathers a summary of selected notable incidents collected during the reporting period.

[2] While we refer to the maritime sector throughout the report, we have also considered inland waterway transport in the analysis.
[3] https://digital-strategy.ec.europa.eu/en/policies/nis-directive
[4] In the road sector, original equipment manufacturers (OEM), tier-X suppliers and the whole automotive sector were considered in the analysis.
[5] ENISA Cybersecurity Threat Landscape Methodology, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
[6] This is a result of work by ENISA in the area of situational awareness in accordance with the EU Cybersecurity Act Article 7, Paragraph 6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
[7] European Centre for Cybersecurity in Aviation (ECCSA) https://www.easa.europa.eu/en/eccsa
[8] European Air Traffic Management Computer Emergency Response Team (EATM-CERT) https://www.eurocontrol.int/service/european-air-traffic-management-computer-emergency-response-team
[9] Malware Information Sharing Platform estimative language https://www.misp-project.org/taxonomies.html#_estimative_language

2. CYBER THREATS TO THE TRANSPORT SECTOR

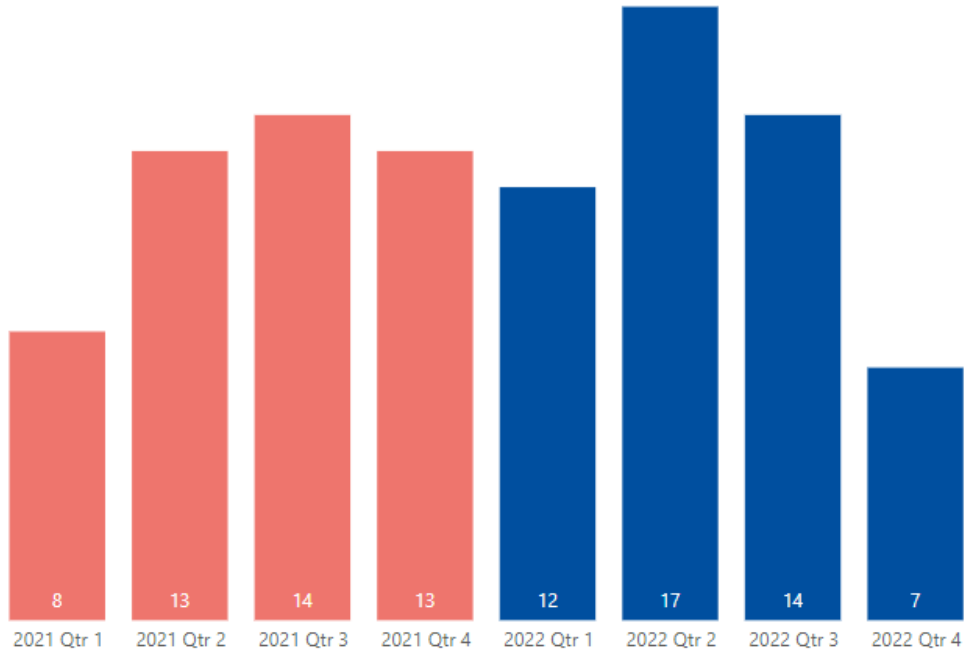
2.1 OBSERVED ACTIVITY

From January 2021 until October 2022, we analysed a total of 98 publicly reported incidents[10].

In 2022, we observed a 25% increase in the monthly average number of reported incidents affecting the transport sector compared to 2021 (see quarterly results in Figure 1). The reporting period ends in October 2022 and the analysis of the incidents was concluded in December 2022. This is why the number of incidents appears lower in Q4 2022 compared with the previous quarters.

We are expecting a further increase of cyber incidents in 2022, especially if we consider that incident handling and analysis is ongoing and that the reporting of incidents often occurs at a later date. However, an increase in the number of reported cyber-attacks does not necessarily mean that the number of attacks has actually increased. This change could be due to the sector maturing in terms of incident detection and reporting. For example, this could be due to the effect of the legal obligation to report incidents under the NIS directive and/or national regulations. Alternatively, the attention of the media or the public could be focused on a particular sector for a particular time period, resulting in more incidents appearing in OSINT sources.

Figure 1: Number of incidents per quarter (January 2021 to October 2022)



[10] Incidents targeting the transport sector accounted for 4.8% and 4.3% of the total incidents identified in ENISA threat landscapes 2021 and 2022, respectively. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

An important aspect involves the proximity of transport related cyber threats with respect to the European Union. We classify incidents according to the proposed classification for the EU common security and defence policy[11], as follows.

Near – Affected networks, systems, controlled and assured within EU borders. Affected population within the borders of the EU.

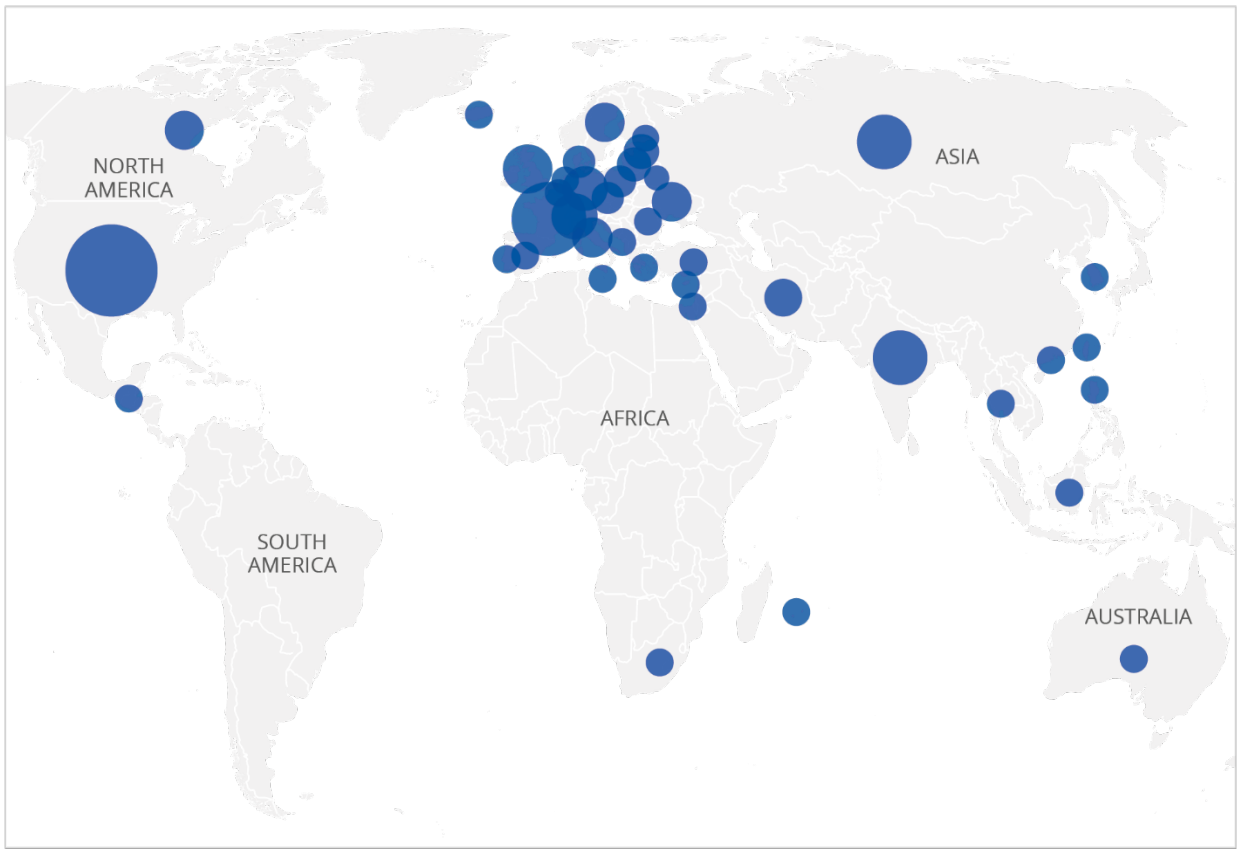
Mid – Networks and systems considered vital for operational objectives within the scope of the EU digital single market and the NIS directive sectors, but their control and assurance rely on non-EU institutional authorities or Member State public or private authorities. Affected population in geographical areas close to EU borders.

Far – Networks and systems that, if influenced, will have a critical impact on operational objectives within the scope of the EU digital single market and the NIS directive sectors. Control and assurance of those networks and systems lies beyond EU institutional authorities and Member States' public or private authorities. Affected population in geographical areas Far from the EU.

Global – All the aforementioned areas.

The following map gives an overview of the incidents observed in the world for the reporting period, while Figure 3 and Figure 4 show the proximity of incidents to the EU for 2021 and 2022 respectively.

Figure 2: Map of observed incidents (January 2021 to October 2022)



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

[11] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

As mentioned above, the data collection process prioritises incidents that occur in the EU. Even with this limitation, we can safely assess that in 2022 there was a significant increase of incidents that were made public and affected the EU (category 'Near') and areas close to the EU (category 'Mid'), compared to 2021. This comes as no surprise considering the current geopolitical situation in which the EU is involved and the significance which was placed on the transport sector during Russia's unprovoked invasion of Ukraine.

Figure 3: Proximity of observed incidents (January 2021 to December 2021)

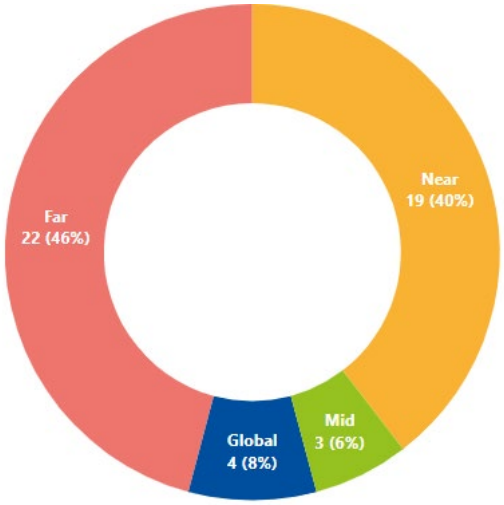
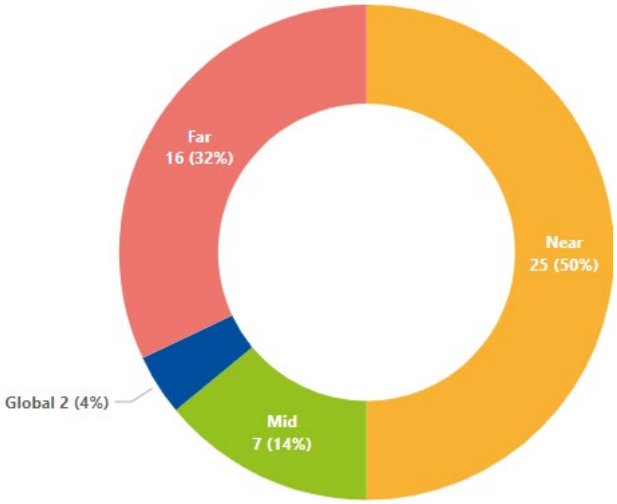


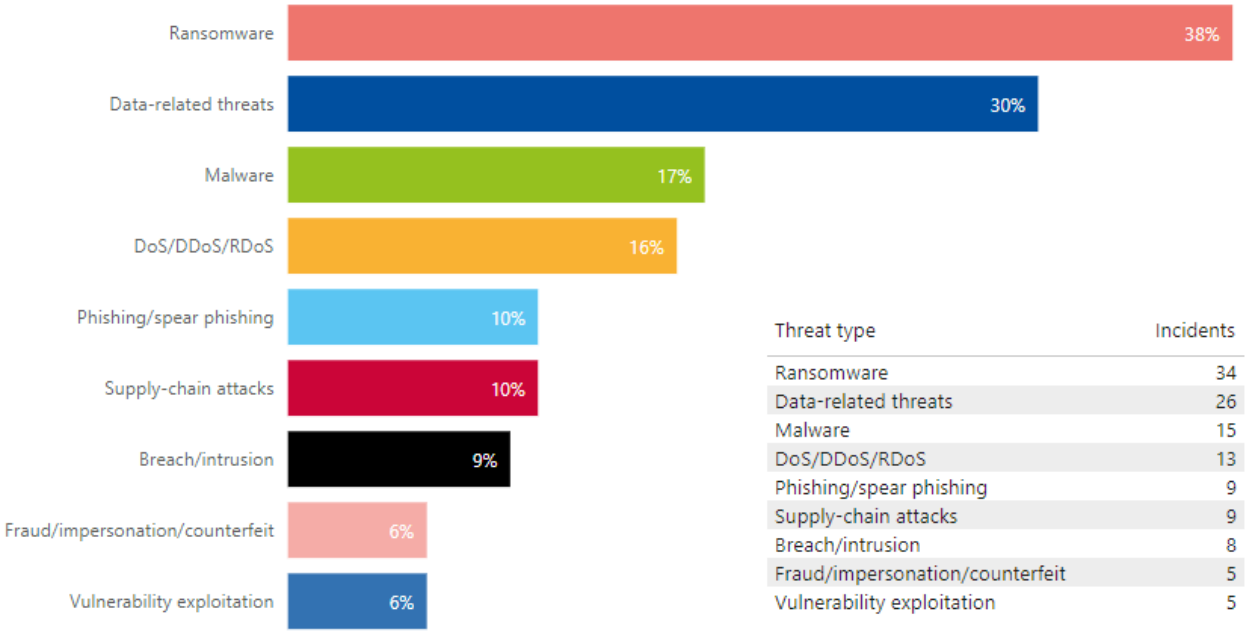
Figure 4: Proximity of observed incidents (January 2022 to October 2022)



2.2 PRIME THREATS

During the reporting period, we observed the following types of threats (Figure 5) to the transport sector. An incident can be categorised in more than one threat category, which means that the total percentage of the threats shown in Figure 5 exceeds 100%. For example, the attack vector for initial access may include a phishing campaign, which is then followed by a compromise with ransomware. Likewise, incidents which included an attack to a supplier were categorised both as supply-chain attacks and as the type of attack used for the compromise.

Figure 5: Prime threats to the transport sector (January 2021 to October 2022)



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

Ransomware

Ransomware is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability[12]. Ransomware incidents are presented separately from malware, as they are significant portion of the identified incidents (38%) during the reporting period, with several high profile and highly publicised incidents.

Threats against data

Sources of data are being targeted with the aim of unauthorised access and disclosure and manipulating data to interfere with the behaviour of systems. These threats are also the basis of many other threats, also discussed in this report. For instance, ransomware, or DDoS attacks aim to deny access to data and possibly collect a payment to restore this access. Technically speaking, threats against data can mainly be classified as data breaches and data leaks. A data breach is an intentional attack brought by a cybercriminal with the goal of gaining unauthorised access and the release of sensitive, confidential or protected data. A data leak is an event that can cause the unintentional release of sensitive, confidential or protected data due to, for example, misconfigurations, vulnerabilities or human errors. In this reporting period, around 30% of the observed incidents were a form of threat against the data of transport organisations.

Malware

Malware is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system. Traditionally,

[12] ENISA Threat Landscape for Ransomware Attacks https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

examples of malicious code types include viruses, worms, trojan horses, spyware, adware or other code-based entities that infect a host. During this reporting period, 17% of incidents targeting the transport sector involved malware.

Denial of service

Availability is the target of a plethora of threats and attacks, among which DDoS stands out. DDoS attacks target system and data availability and, though not a new threat, have a significant role in the cybersecurity threat landscape of the transport sector. Attacks occur when users of a system or service are not able to access relevant data, services or other resources. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure. During the reporting period, geopolitical developments and hacktivist activity increased the number of DDoS attacks against transport organisations, reaching 16% of total incidents.

Vulnerability exploitation

Vulnerability exploitation refers to exploitation of known or zero-day vulnerabilities[13].

Social engineering

Social engineering encompasses a broad range of activities that attempt to exploit a human error or human behaviour with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information. In cybersecurity, social engineering lures users into opening documents, files or emails, visiting websites or granting unauthorised persons access to systems or services. This threat canvas consists mainly of the following vectors: phishing, spear-phishing, whaling, smishing, vishing, business email compromise, fraud, impersonation and counterfeiting. In this reporting period, we primarily observed phishing and spear phishing attacks targeting transport users (10%) and fraud, impersonation and counterfeit incidents (6%).

Attacks to suppliers and supply-chain attacks

A supply-chain attack targets the relationship between organisations and their suppliers. For this report we use the definition as stated in the *ENISA Threat Landscape for Supply Chain*, where an attack is considered to have a supply-chain component when it consists of a combination of at least two attacks. For an attack to be classified as a supply-chain attack, both the supplier and the customer have to be targets. It seems that threat actors are continuing to feed on this source to conduct their operations and gain a foothold within organisations, in an attempt to benefit from the widespread impact and potential victim base of such attacks. In this reporting period, we observed both supply-chain attacks, as defined above, and attacks to suppliers that caused disruptions or losses to entities in the transport sector (10% of total incidents). This impact was not necessarily the effect of a secondary attack.

Breach/intrusion

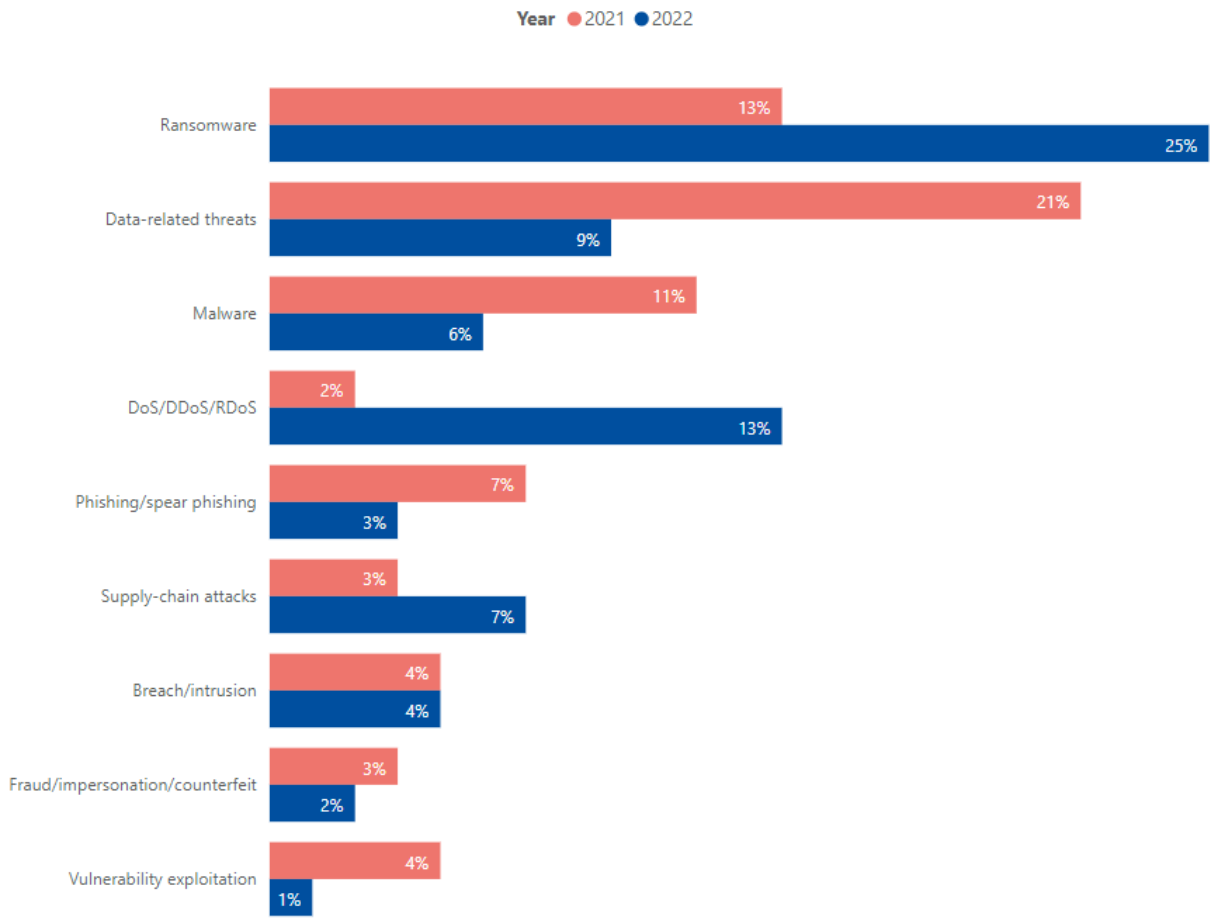
Breach/intrusion refers to incidents where an attack to a system has been confirmed or made public and attackers have gained access to systems, but the details of how the breach or the intrusion took place are not clear. These types of incidents account for 9% of the total number of incidents.

Other threats include single occasions of **credential harvesting** and **spoofing of geolocation** in the maritime sector.

Finally, there is a small percentage of incidents where even though a cyberattack took place, there is insufficient information to allow for the incident to be categorised. This accounts for a total of 7% of incidents (**unknowns**).

[13] For more information regarding the common vulnerabilities and exposures (CVE) that were discovered and used from July 2021 to June 2022, see ENISA Threat Landscape 2022 (annex C). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Figure 6: Prime threats to the transport sector: 2021 v 2022

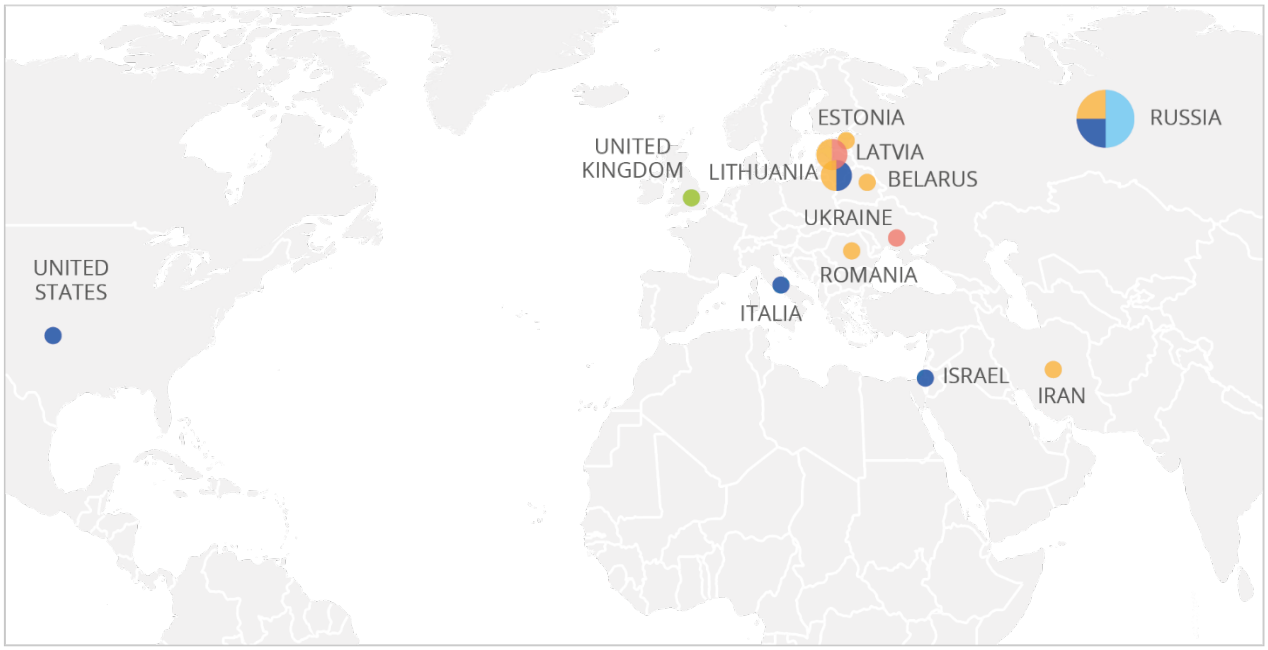


The data on incidents collected until October 2022 indicate an increase in reporting of ransomware attacks during 2022. The number of ransomware attacks reported to the transport sector almost doubled, rising to 25% in 2022 from 13% during 2021. Contrary to ransomware, we observed a decline in malware incidents in 2022 compared to 2021 (from 11% to 6%).

Data related threats (breaches, leaks) declined compared to ransomware, but remain significant. The attacks observed in 2021 and 2022 targeted credentials, the personal data of employees and passengers, corporate data and intellectual property.

We also observed an increase in DDoS attacks in 2022, which is mostly linked to recent activity by hacktivists. The rates of these attacks are focused on specific regions and are affected by current geopolitical tensions. The current geopolitical situation and its effect on the transport sector can be seen in Figure 7. The map depicts selected incidents in all transport sectors which were attributed to hacktivism. The motivation was primarily operational disruption and ideological.

Figure 7: 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.

2.3 THREAT ACTORS & MOTIVATION

Similarly to the *ENISA Threat Landscape 2021*[14] and *ENISA Threat Landscape 2022*[15], we considered four categories of cybersecurity threat actors: state-sponsored actors, cybercriminals, hackers-for-hire, and hacktivists.

- **Cybercriminals**' primary motive is financial gain, often stealing data or demanding ransom.
- **Hackers-for-hire** sell their services to people who do not have the skills or capabilities to do so.
- **State-sponsored** actors target organisations to compromise, steal, change, or destroy information. These groups are usually affiliated with a nation state[16].
- **Hacktivists** are politically, socially, or ideologically motivated and target victims for publicity or to effect change.

For the cases in which one of these types of actors was not identified, we either categorised the incident as an individual actor or as unknown. During the reporting, we did not have information on hacker-for-hire actors targeting the transport sector, so they are not included in Figure 8.

Figure 8: Actors

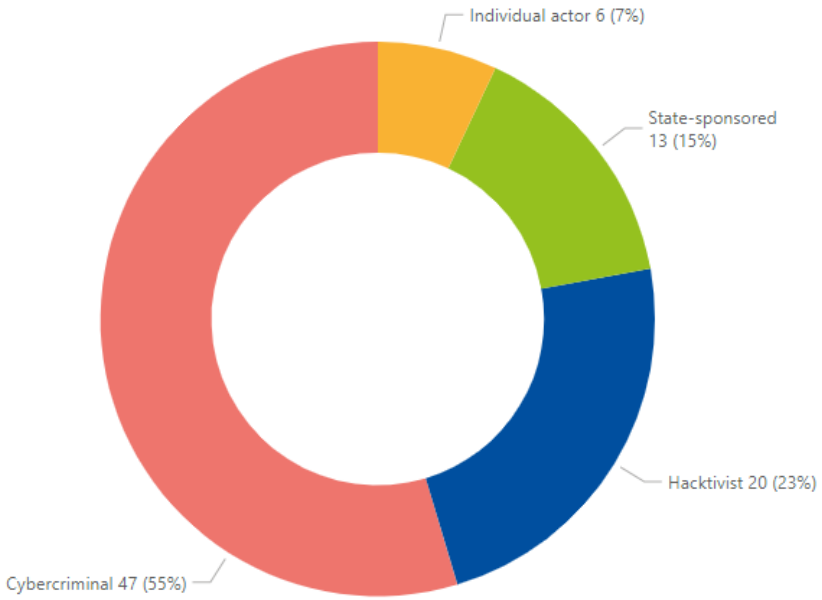
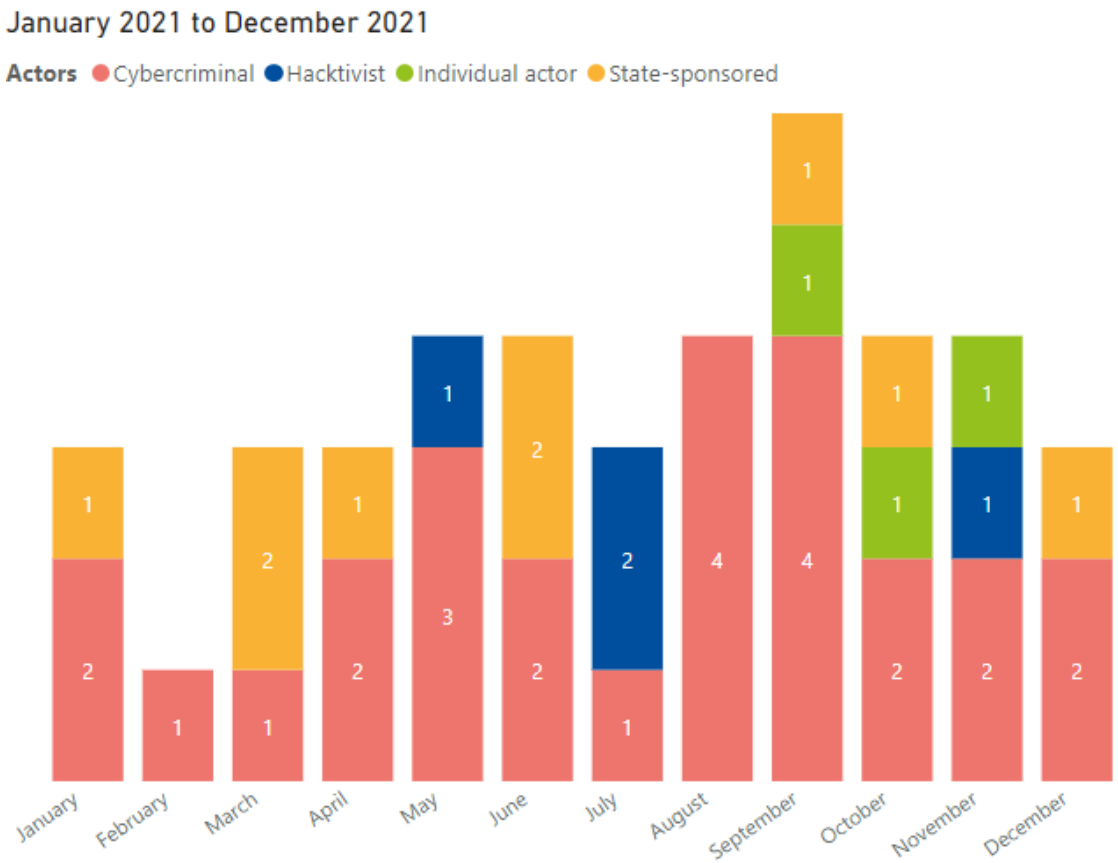
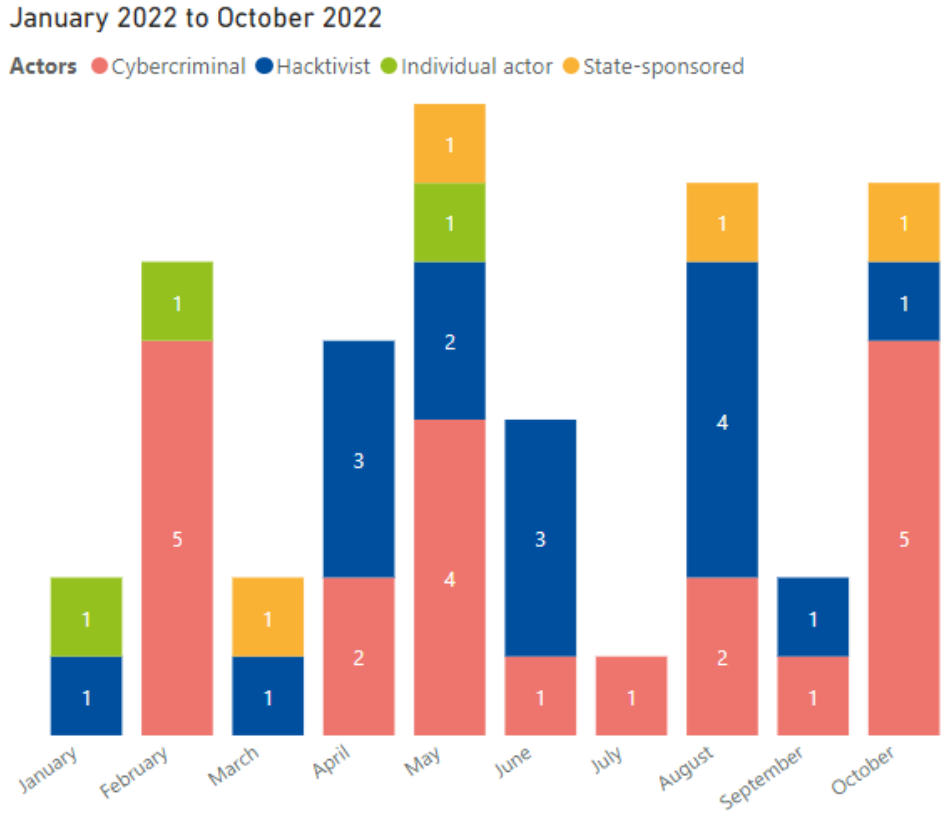


Figure 8 shows the overall activity of actors targeting the sector, while Figure 9 analyses this activity on a monthly basis.

[14] ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[15] ENISA Threat Landscape 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[16] The term has been used interchangeably with Advanced Persistent Threat (APT), however APT refers to a type of activity conducted by a range of actors.

Figure 9: Actor activity (January 2021 to October 2022)

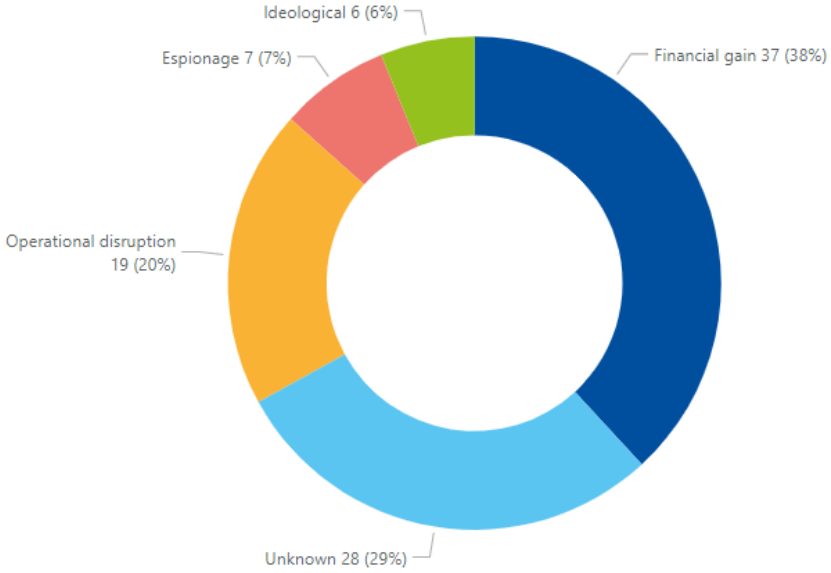




For the analysis of the incidents, we have considered the following motivations.

- Espionage, when the aim of the attack is information gathering (either intellectual property or information of national importance).
- Financial gain, when there is a clear monetary claim behind the attack, such as extortion, selling of stolen data, etc.
- Ideological, when the attack is linked to hacktivist activity and there are clear declarations on the aim of the attack by the actor.
- Operational disruption, when the attack is aiming at disrupting services, as opposed to cases where a disruption of operations is a side effect of an attack.

Figure 10: Motivation



More than half of the incidents observed in the reporting period were linked to cybercriminals (55%). This is also linked with the motivation behind these attacks which is predominately financial gain (38%). The transport sector is considered a lucrative business for cybercriminals, with customer data considered a commodity and with highly valuable proprietary information when transport supply chain is being targeted. One fourth of the attacks are linked to hacktivist groups (23%), with the motivation of their attacks usually being linked to the geopolitical environment and aiming at operational disruption (20%) or ideological motivation (6%).

2.4 IMPACT

When considering the impact of an incident to the sector, we analysed who was the target of the attack (Figure 11) and which were the affected assets (Figure 12).

As the types of targeted entities differ between subsectors, Figure 11 offers a breakdown of the targets by subsector. Please note that one incident may be targeting multiple transport entities.

All subsectors had authorities and bodies that were being targeted, in fact 38% of the incidents targeted transport authorities. In the railway sector, incidents almost exclusively targeted railway undertakings and infrastructure managers. Similarly, port operators were the most affected entities in the maritime sector. These two sectors had only a few incidents targeting supply chain or service providers. This was not the case in the road sector, where OEM, tier-X suppliers and service providers were targeted, along with public transport operators. In the aviation sector, airlines and airport operators are the main targets, followed by service providers, surface transport operators and the supply chain.

Figure 11: Targets (number of incidents per entity type)

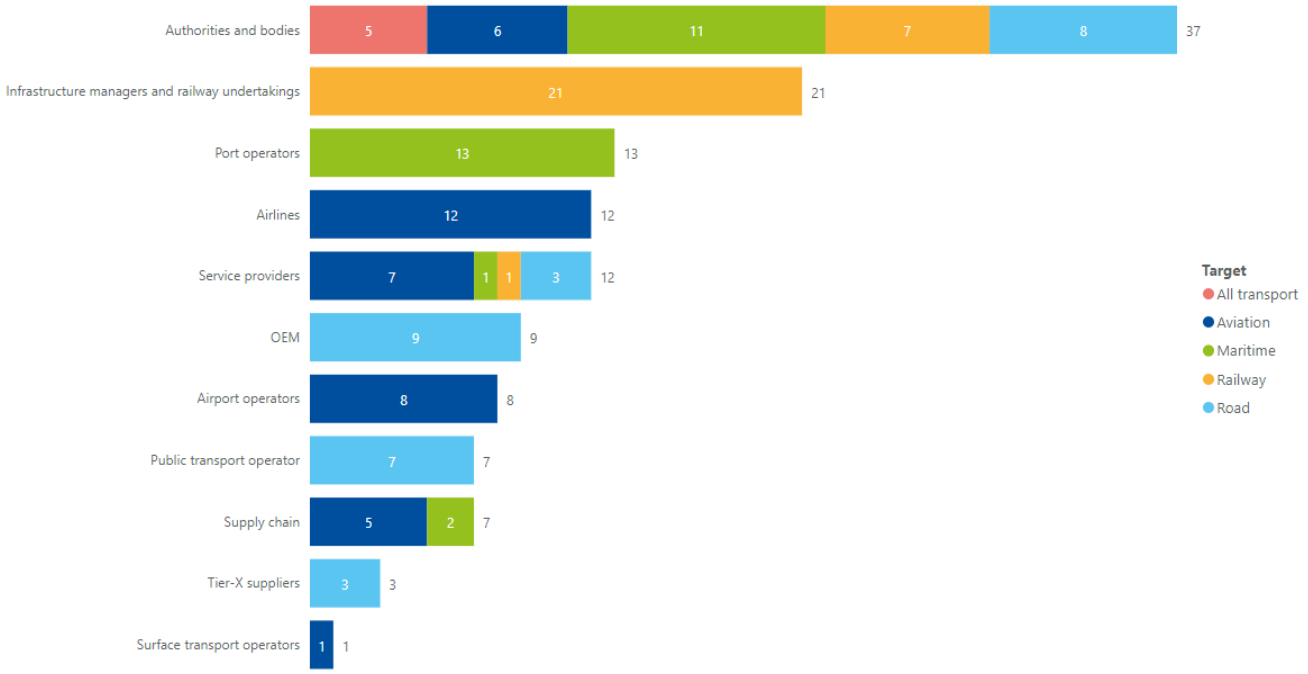
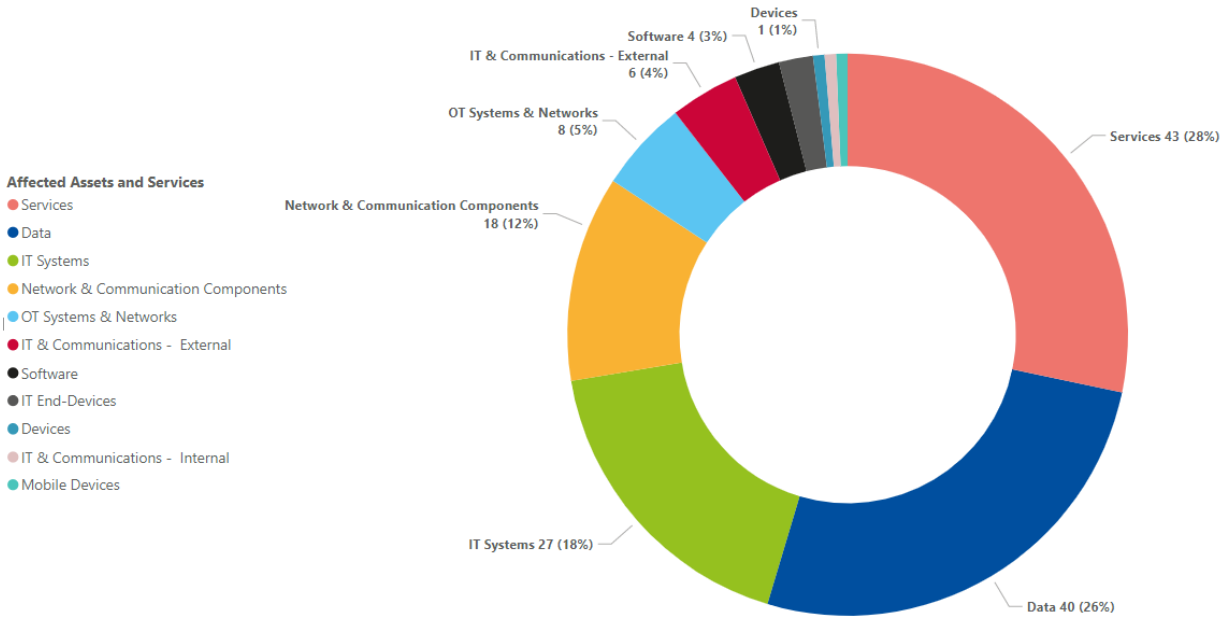
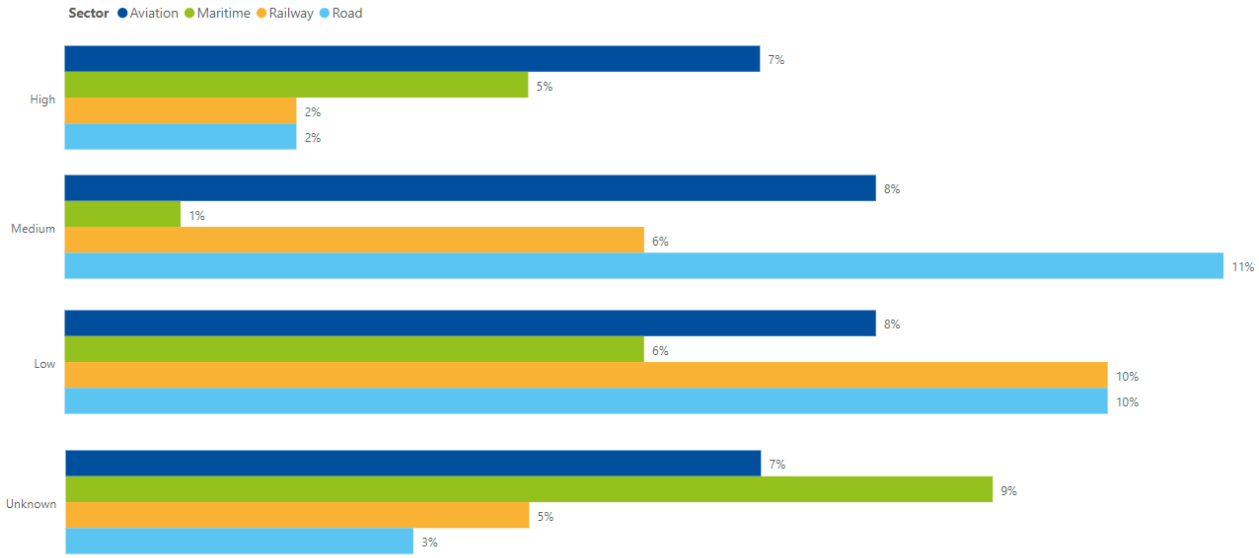


Figure 12: Affected assets



Detailed and reliable information about the impact of incidents is not readily available in OSINT reports. It can often be deduced from the description of the incident, but the impact assessment can often include a lower level of confidence. In particular, reputational, legal and social impacts are particularly difficult to assess. Similarly, financial impact can be calculated in various ways by the affected party and it can change over time as the effect of an incident develops and its long-term consequences are assessed. For this reason, we were able to include only reported digital or physical impact in the analysis.

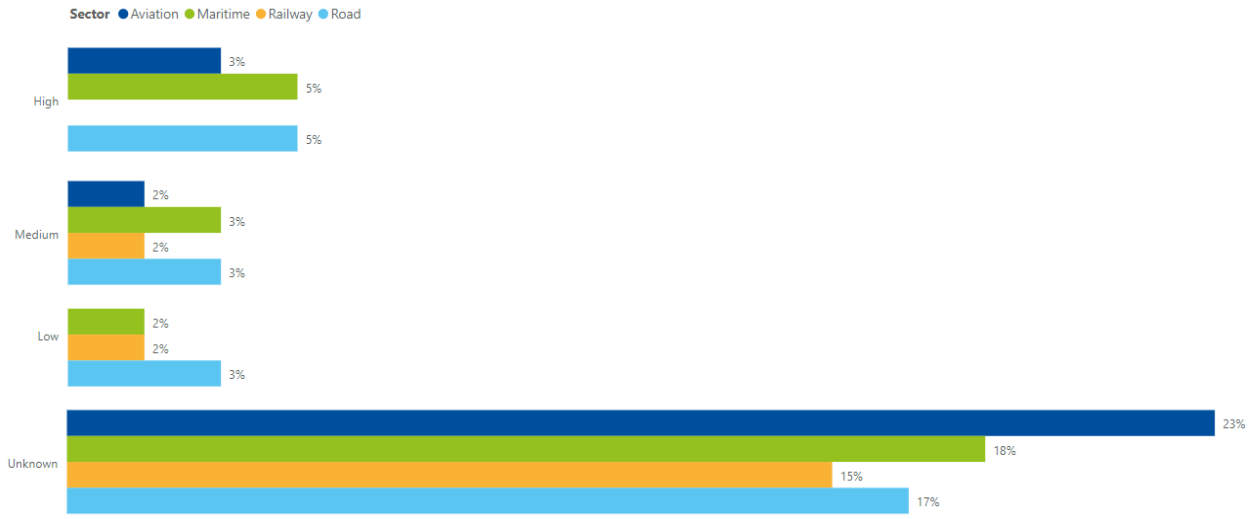
Figure 13: Digital impact



Digital impact (Figure 13) refers to any effect of the attack on the information and communications technology (ICT) systems of the affected entity, while physical impact (Figure 14) refers to cases where the incident causes operational disruption or even destruction of the infrastructure. As we observe, we have more rich information when it comes to the digital impact of cyberattacks on the transport sector. For physical impact, we could not find information of the

actual physical impact for the majority of incidents, as either information was not disclosed or physical impact did not take place.

Figure 14: Physical impact



An alternative dataset which gives a better indication of the impact of attacks are the incidents reported to ENISA by national authorities under the provisions of the NIS directive[17]. These refer to incidents that cause significant impact. At the time of publication data for 2022 were not yet available, data were available only for 2021. In 2021, 34 incidents had a significant impact on transport entities. They account for 6% of the total number of incidents reported to ENISA in 2021. In fact, 65% of these incidents were the result of malicious actions, 32% were due to system failures and 3% were due to human error. These data highlight a significant gap in finding information on non-malicious incidents that can cause disruptions to the transport sector, as these are rarely available in OSINT reports.

[17] In the EU, critical service providers have to report cybersecurity incidents that have a significant impact to the national authorities in their country. At the end of each year, the summary reports about these incidents are collected, anonymised, aggregated and analysed by ENISA. The visualisation tool shows the overall statistics for the EU. https://ciras.enisa.europa.eu/

3. SECTOR ANALYSIS

In this section we further analyse the findings for each transport sector. We distinguish between incidents targeting aviation, maritime, railway and road transport, while we also include a category called 'all transport' which refers to attacks that target either all four sectors or, more commonly, ministries of transport. For the reporting period, we studied 27 incidents targeting aviation (28%), 18 incidents targeting maritime (18%), 21 incidents targeting railway (21%) and 24 incidents targeting road transport (24%). We also included 8 incidents (8%) that targeted the transport sector as a whole, or incidents targeting transport ministries.

Figure 15: Observed incidents in each sector

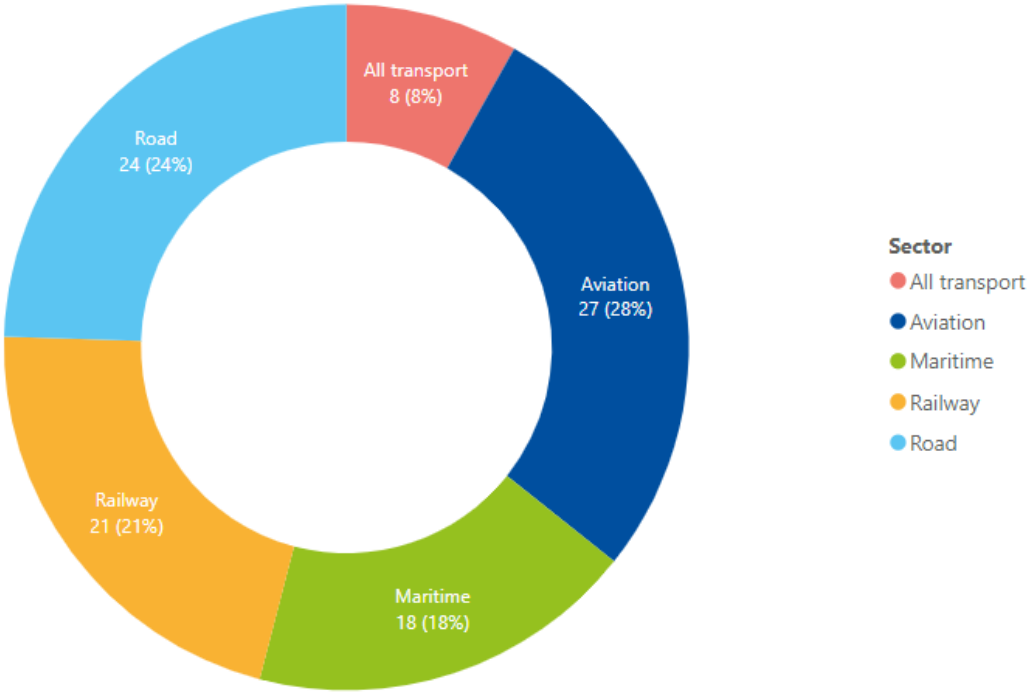


Figure 16: Annual observed incidents in each sector (January 2021 to December 2021, January 2022 to October 2022)

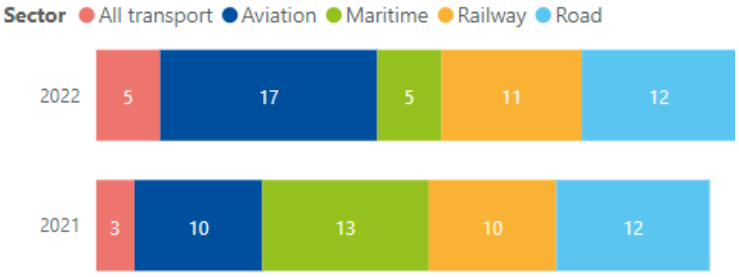


Figure 17 shows the monthly incidents in each sector for the reporting period.

Figure 17: Monthly observed incidents in each sector

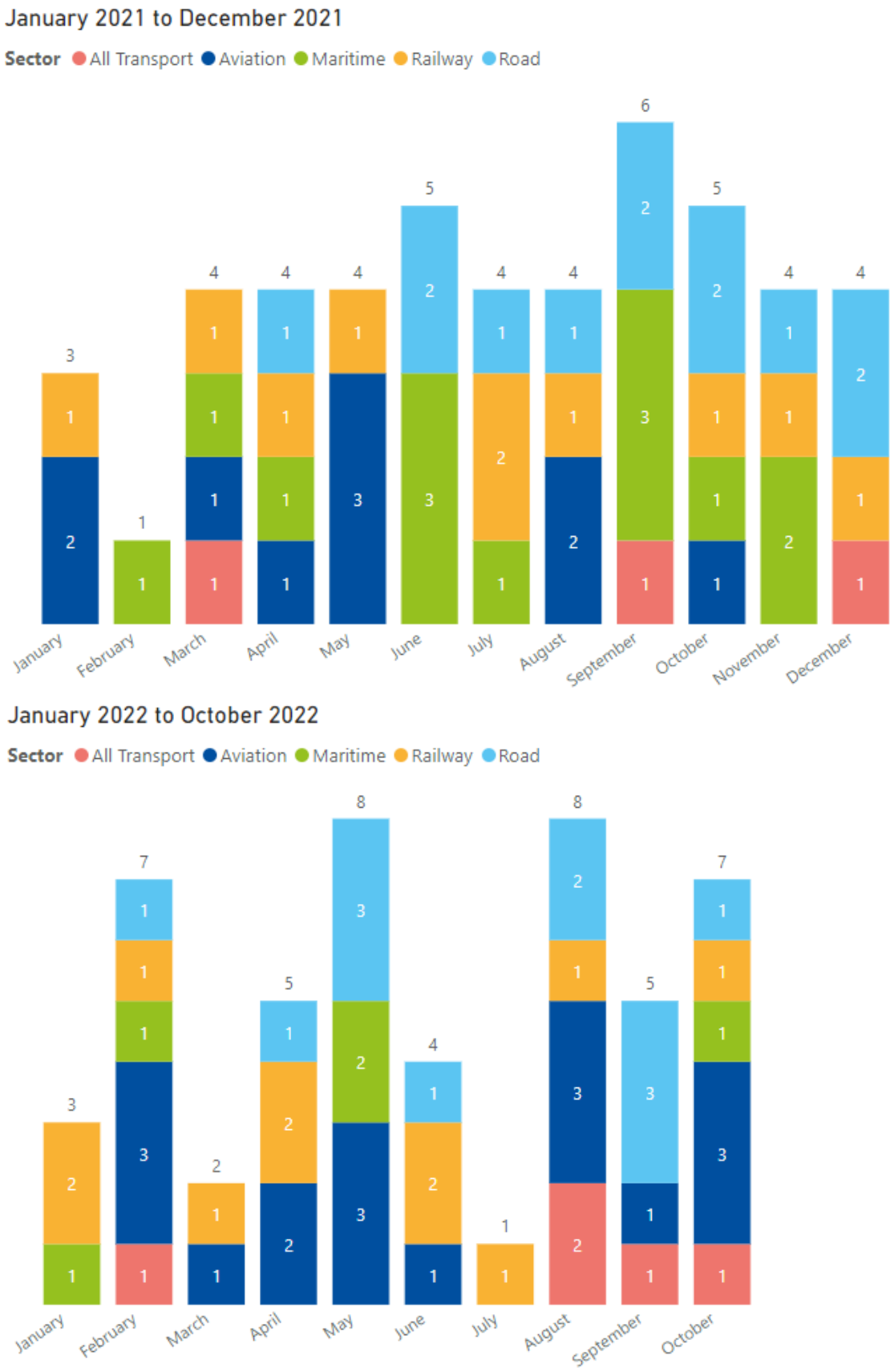
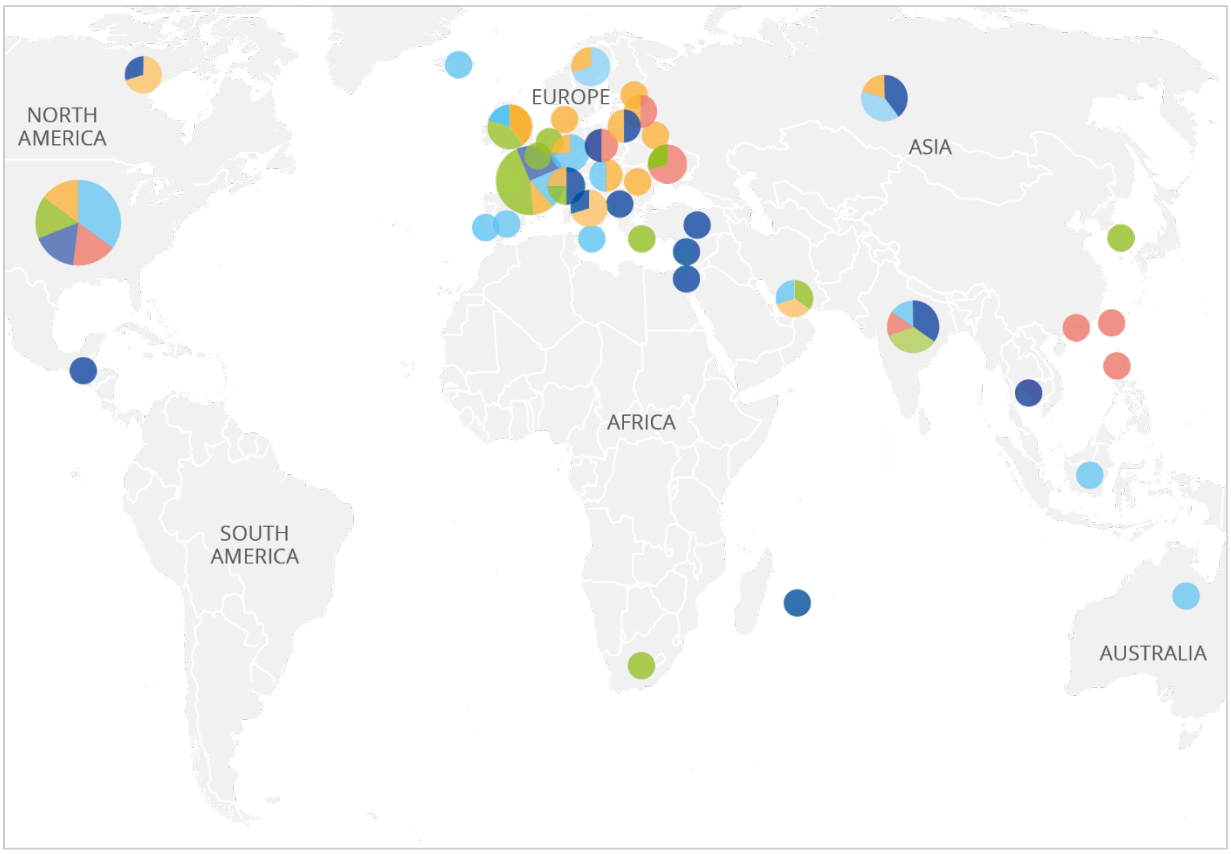


Figure 18 shows the geographical spread of the observed incidents. We can see here that the focus of the report is on the incidents that affect EU transport and the neighbouring countries. However, we have included significant incidents from the world, targeting transport entities primarily in North America and Asia. The map also gives an indication of the geographical spread of affected subsectors.

Figure 18: Global map of observed incidents



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

In Figure 19 and Figure 20 we depict the motivation and the actors of the observed incidents for each sector.

Figure 19: Motivation in each sector

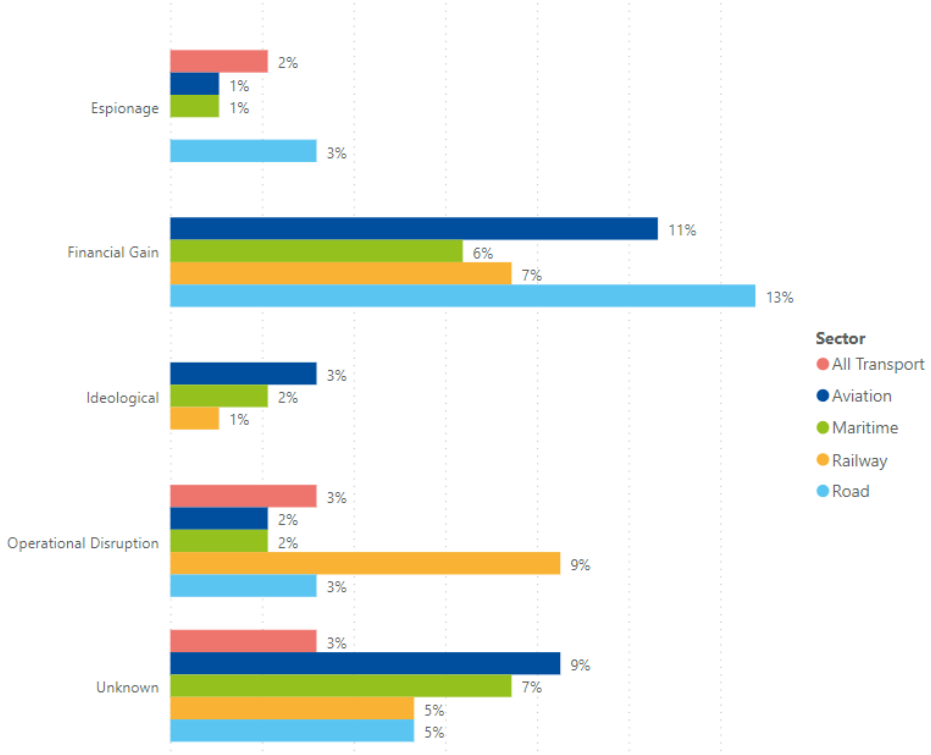
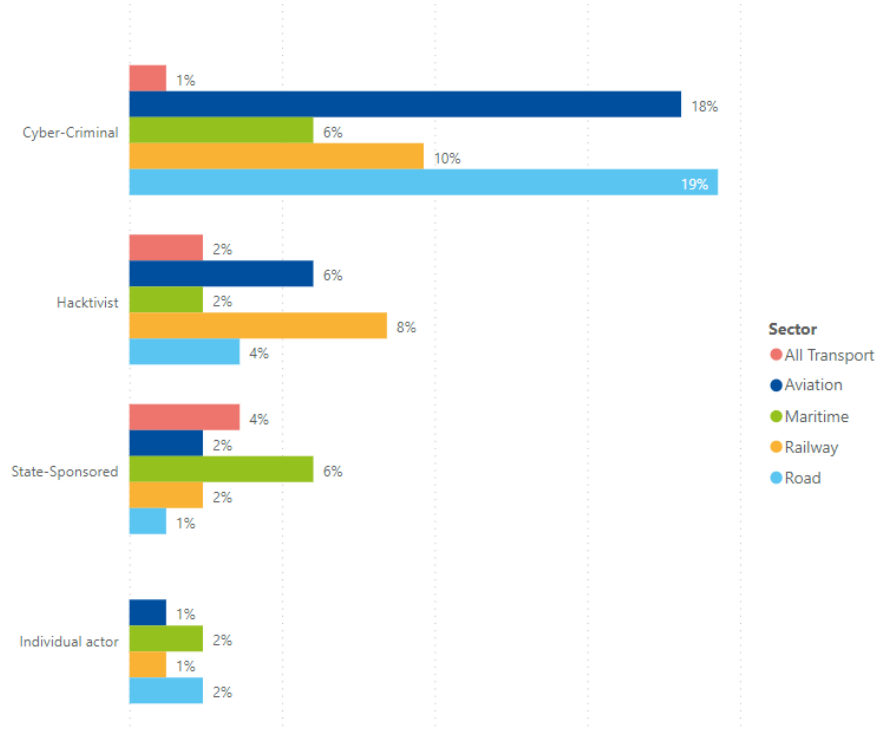


Figure 20: Actor in each sector



Cybercriminals are the main actors responsible for attacks on the transport sector (54% of the total number of incidents) and they target all subsectors. They use the 'follow the money' philosophy in their modus operandi. Almost

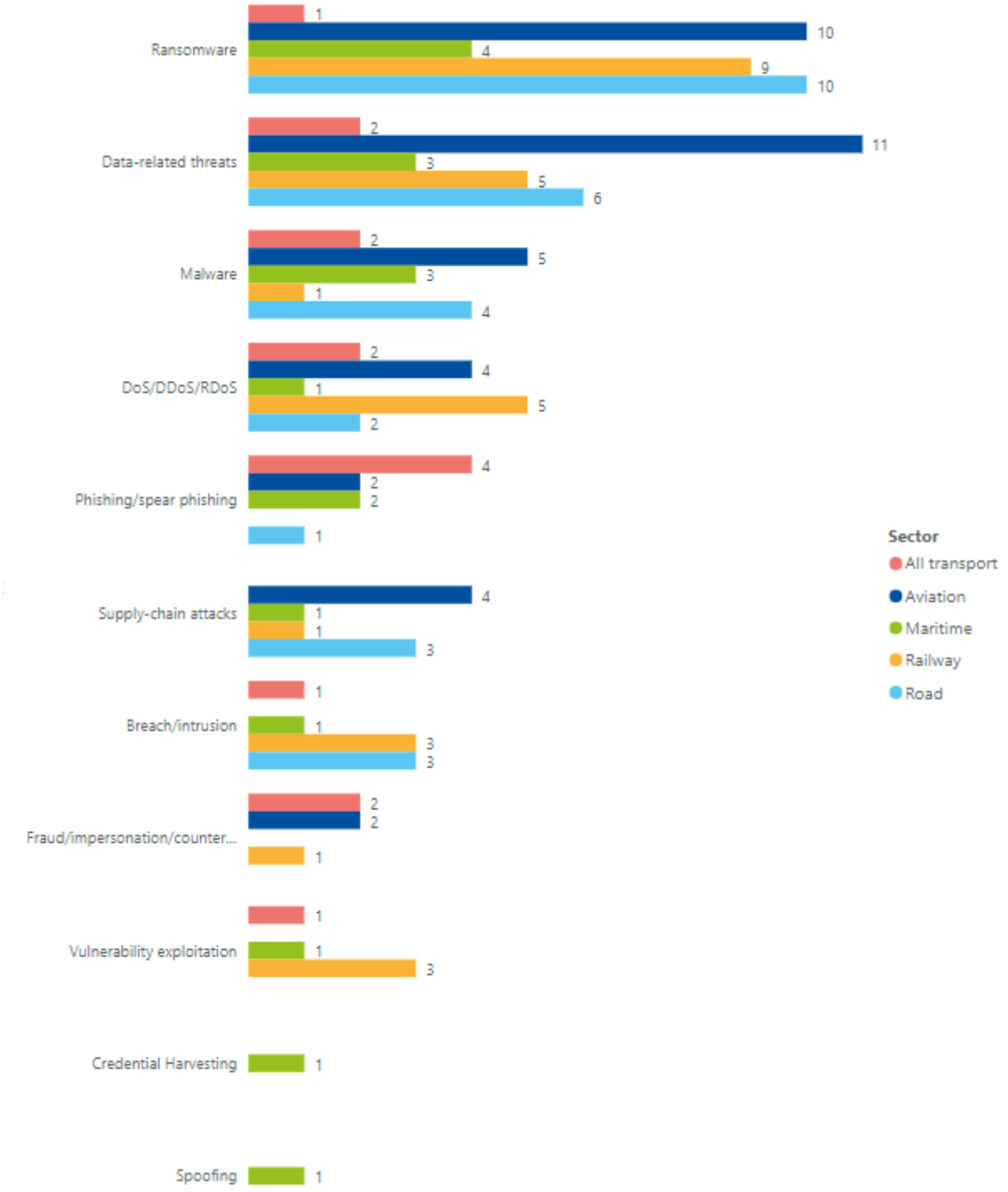
two fifths of the total number of incidents are incidents attributed to cybercriminals targeting two sectors: aviation and road transport. During the reporting period, 18% of cybercriminals targeted the aviation sector (primarily airports and airlines and their customers) and 19% targeted the road sector (primarily the automotive industry). Likewise, the motivation behind attacks on these two sectors was primarily financial gain (11% and 13% of the total number of incidents, respectively), as the aviation and automotive industries are considered to be the more lucrative ones for cybercriminals. The attacks are considered opportunistic in nature, as we have not observed known groups targeting the transport sector exclusively.

We observe that hacktivists have claimed responsibility for attacks on the railway (8%) and aviation (6%) sectors, and this has to do mainly with attacks linked to the Russia's military aggression against Ukraine. In particular, these types of attacks make up almost one tenth of the total number of incidents that aimed at operational disruption in the railway sector.

State-sponsored actors were more often attributed to targeting the maritime sector or targeting government authorities of transport ('All transport' category).

Figure 21 presents the sectorial analysis of all observed threats. We observe that there are differences in how these threats affect specific sectors. These differences are discussed in greater detail in the chapters that follow.

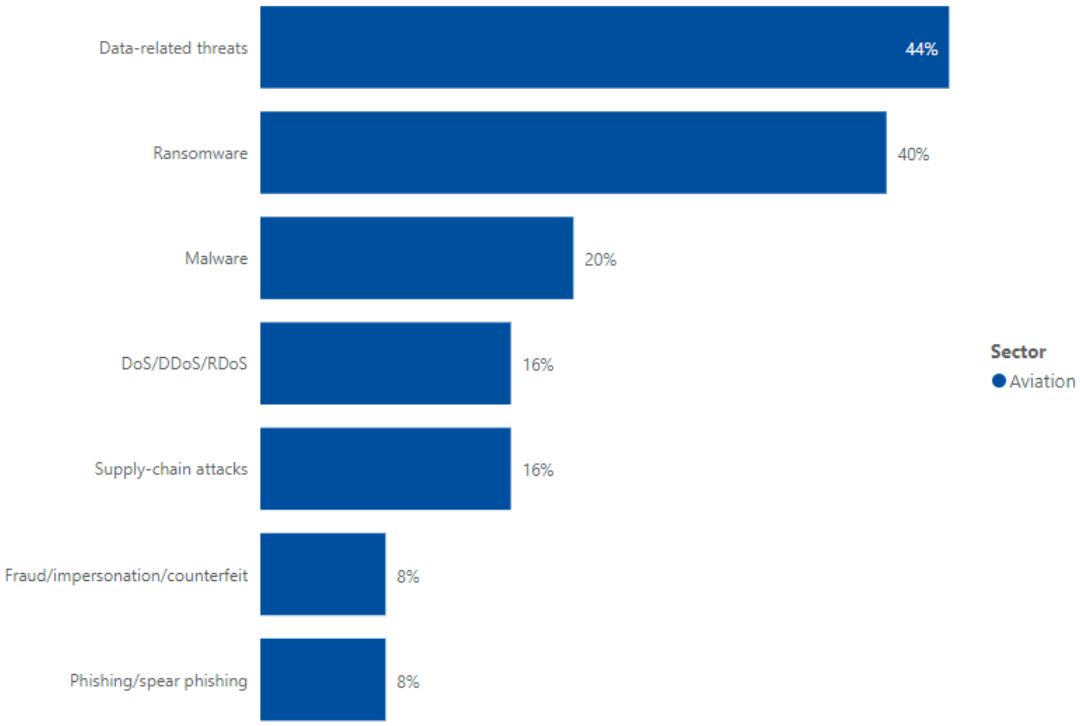
Figure 21: Prime threats in each sector (number of observed incidents)



3.1 AVIATION SECTOR

According to the data collected through OSINT by ENISA and the EU aviation safety agency (see Figure 22), prime threats for the aviation sector are data-related threats (45%), ransomware (36%) and malware (23%). In the majority of ransomware cases in the aviation sector, the attack is followed by data-related threats, such as data exfiltration and leakage, so there is significant overlap in these two categories. Customer data are one of the prime targeted assets of the sector, followed by the proprietary information of original equipment manufacturers (OEM).

Figure 22: Aviation - prime threats

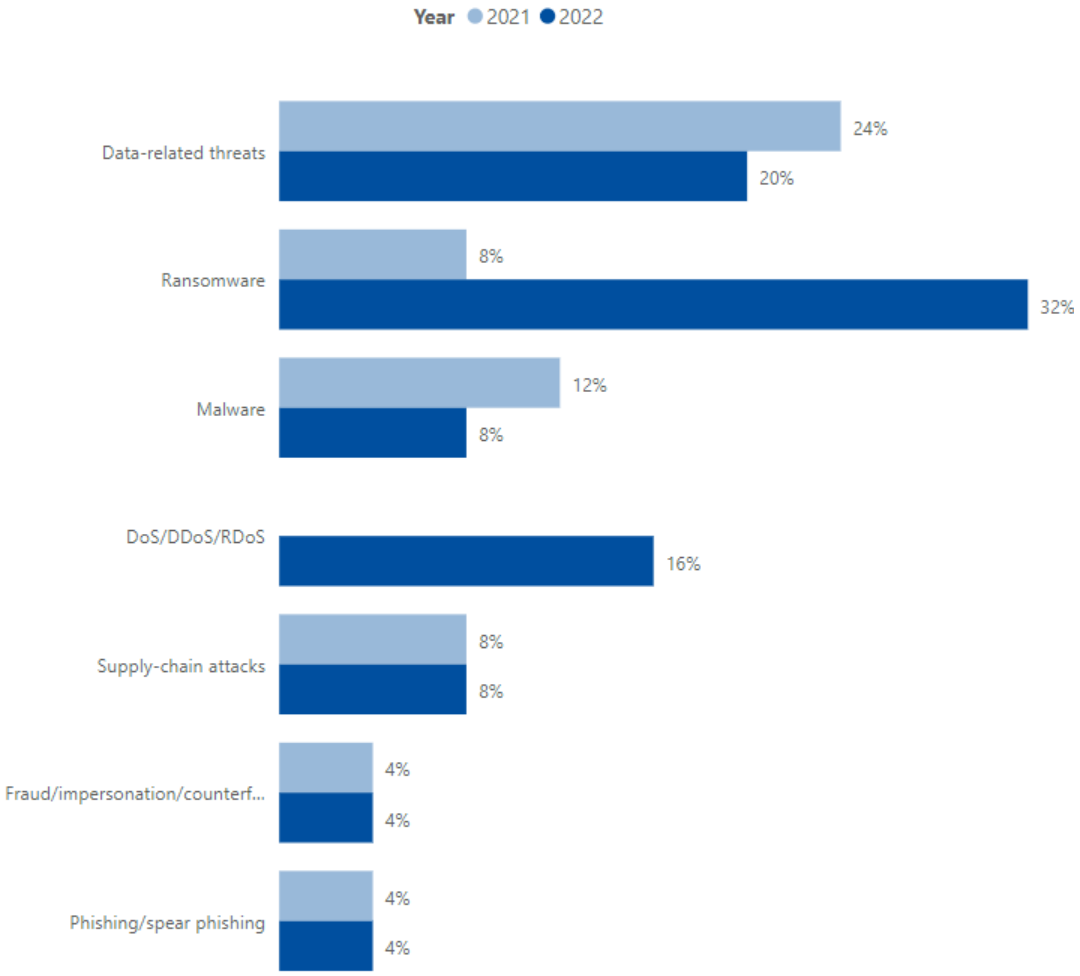


In 2022, we observed an increase in the number of ransomware attacks affecting airports (see Figure 23). Out of all operators (excluding original equipment manufacturers), airport operators are the most affected by ransomware attacks. Airports, airlines and ultimately the passengers suffer due to other incidents that have an impact on their data. The most notable events include the following.

- In March 2021 the passenger service system provider SITA was hacked; hundreds of thousands of Star Alliance passengers' details were stolen.
- In April 2021 a malware attack on Radixx Res disrupts 20 airlines' ticket reservation systems[18]. The service disruption made it impossible for many of the airline passengers to make, change, delete or confirm bookings through the airlines' websites, although flight operations were not affected.
- In May 2021 Air India suffered a data breach. 4.5 million customers were impacted only 2 months after its passenger service system provider SITA was hacked.
- In August 2021 Bangkok Air confirmed the leak of passenger data after a ransomware attack[19]. According to the airline, some of the personal data that may have been included in the stolen files included data fields such as passenger name, family name, nationality, gender, phone number, email address, home address, contact information, passport information, historical travel information, partial credit card information and special meal information.

[18] https://www.databreaches.net/malware-attack-on-radixx-res-disrupts-20-airlines-ticket-reservation-systems/
[19] https://therecord.media/bangkok-air-confirms-passenger-pii-leak-after-ransomware-attack/

Figure 23: Aviation - prime threats (annually)



- In January 2022 Dassault Falcon Jet was hit by the Ragnar Locker ransomware gang[20]. The attack may have led to the exposure of personal information belonging to current and former employees, and their spouses and dependents.
- In February 2022 Swissport International was hit by a ransomware attack that had a severe impact on its operations, causing flights to suffer delays. Following the attack, the perpetrators (BlackCat) leaked data which included business documents, tax declarations, images of passports and ID cards of individuals. Leaked data also included personal information of job candidates[21].
- In May 2022, after a ransomware attack on SpiceJet, hundreds of passengers were stranded at airports across India, particularly those airports where restrictions on night operations were in effect[22].
- In May 2022 a Turkish airline exposed flight and crew information in a 6.5 terabyte leak[23].
- In August 2022 Accelya, a technology firm providing services to Delta, British Airways, JetBlue, United, Virgin Atlantic, American Airlines and many others, confirmed that company data was posted on a ransomware leak site[24].
- In August 2022 TAP Air Portugal was the target of a Ragnar Locker ransomware attack. The attackers leaked customers' names, addresses and telephone numbers[25].

[20] https://www.bleepingcomputer.com/news/security/dassault-falcon-jet-reports-data-breach-after-ransomware-attack/
[21] https://securityaffairs.co/wordpress/128039/cyber-crime/blackcat-swissport-ransomware-attack.html
[22] https://therecord.media/spiceject-ransomware-attack-flights-grounded/
[23] https://www.infosecurity-magazine.com/news/turkish-airline-exposes-flight/
[24] https://therecord.media/major-airline-technology-provider-accelya-attacked-by-ransomware-group/
[25] https://www.portugalresident.com/hackers-share-personal-data-of-1-5-million-tap-passengers/

- In October 2022 ransomware group LockBit 3.0 claimed to have compromised the aeronautical French defence and technology firm Thales Group[26].
- In October 2022 it was claimed on the Black Basta data leak website that the United States (US) aerospace and defence company Genesys Aerosystems, which mainly produces advanced avionics solutions and components, was a ransomware victim[27].

The data collected and analysed by Eurocontrol's EATM-CERT[28] highlight a threat that often goes underreported in open sources. 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. This discrepancy is due to the fact that this information is not often made publicly available. It is linked to the sector's victimology, which is mainly airlines and their customers being targeted. The rest of the threats reported to Eurocontrol for the first semester of 2022 were web application attacks (22%), DDoS attacks (13%), phishing attempts (12%), ransomware (6%) and malware (1%).

DDoS attacks were primarily observed by ENISA in 2022 and were linked with hacktivist activity against airports and aviation authorities, such as the following.

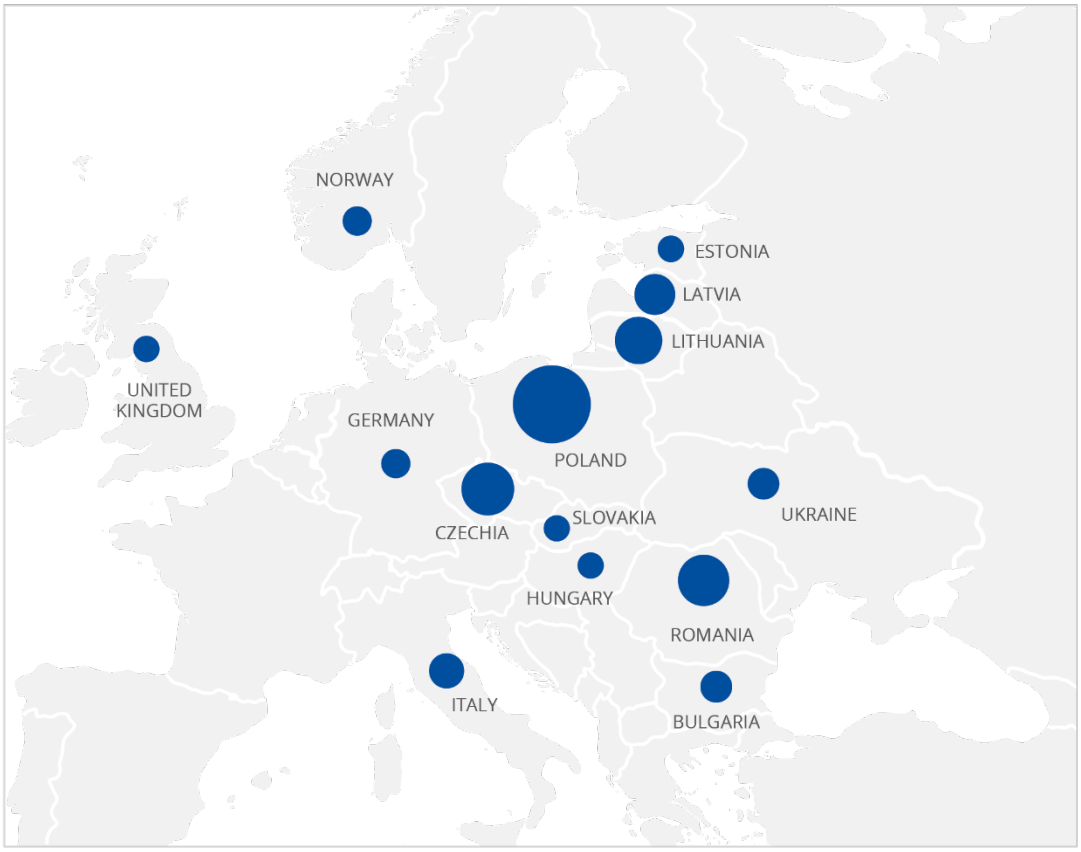
- In April 2022 the website of the Israel Airports Authority was temporarily taken offline due to a denial-of-service attack[29].
- In May 2022 a pro-Russia hacker group launched an attack on the websites of Italian ministries, including attacks targeting Italian airports[30].
- In June 2022 pro-Russia hacker group NoName057 targeted Lithuanian airports with DDoS attacks[31].
- In October 2022 Russian threat actors (e.g. Anonymous Russia) led DDoS attacks on airports in Bratislava [32], Budapest and Bulgaria[33], targeting their websites.
- In October 2022 the websites of major US airports[34] were disrupted due to a large-scale campaign of DDoS attacks, in which pro-Russian hacker group Killnet flooded servers with web traffic to take websites offline.

Eurocontrol EATM-CERT collected and shared with ENISA 97 individual cases where pro-Russian hacker group Killnet targeted airports in the EU and neighbouring countries during 2022 (proximity 'Near', Mid'). The map of this activity is depicted in Figure 24.

Data collected from ENISA and Eurocontrol indicate that airspace users/airlines are the main victims of attacks (see Figure 25). This is mainly due to the financial motivation behind these attacks, which is predominant in the sector. Airlines are being targeted directly by attacks to their systems and indirectly by attacks targeting their customers (e.g. by fraudulent websites). Eurocontrol reports airspace users (80%), airports (12%), OEMs / supply chain (6%), air navigation service providers (1%) and civil aviation authorities (1%) as the main targets for January 2022 to June 2022.

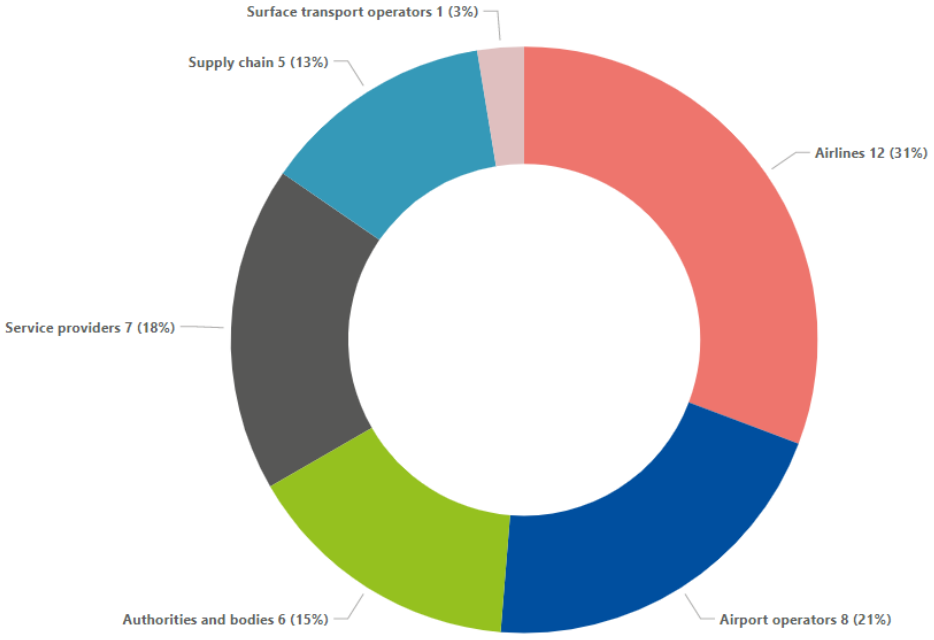
[26] https://cyware.com/news/lockbit-30-gang-allegedly-stole-thales-groups-data-aa676192/
[27] https://www.redpacketsecurity.com/black-basta-ransomware-victim-genesys-aerosystems/
[28] The incidents which served as a basis for the analyses (January 2021 to June 2022) were: (a) publicly reported incidents/events which EATM-CERT collected, (b) findings of EATM-CERT (c) non-publicly reported cyber incidents or events, shared with EATM-CERT by aviation stakeholders (air navigation service providers, airport operators, original equipment manufacturers, civil aviation authorities, airspace users) and the Aviation Information Sharing and Analysis Centre.
[29] https://www.timesofisrael.com/liveblog_entry/airport-websites-hit-by-denial-of-service-attack/
[30] https://www.wired.it/article/attacco-cyber-russia-italia-legion-ministero-polizia/
[31] https://www.lrt.lt/en/news-in-english/19/1728365/major-incidents-contained-after-lithuania-gets-hit-with-massive-cyber-attacks
[32] https://www.cyberthreat.report/ddos-attack-against-slovakia-by-russian-hackers/
[33] https://sofiaglobe.com/2022/10/16/official-cyber-attack-on-bulgarian-government-websites-traced-to-russia/
[34] https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/

Figure 24: Airports targeted by Killnet in Europe and neighbouring countries during 2022



Note: the size of the circle refers to the sum of observed incidents in the country during the reporting period.
Country (sum of attacks to airports): Poland (25), Czechia (13), Romania (13), Lithuania (11), Latvia (8), Italy (6), Bulgaria (4), Ukraine (4), Germany (3), Norway (3), Estonia (2), Slovakia (2), United Kingdom (2), Hungary (1).

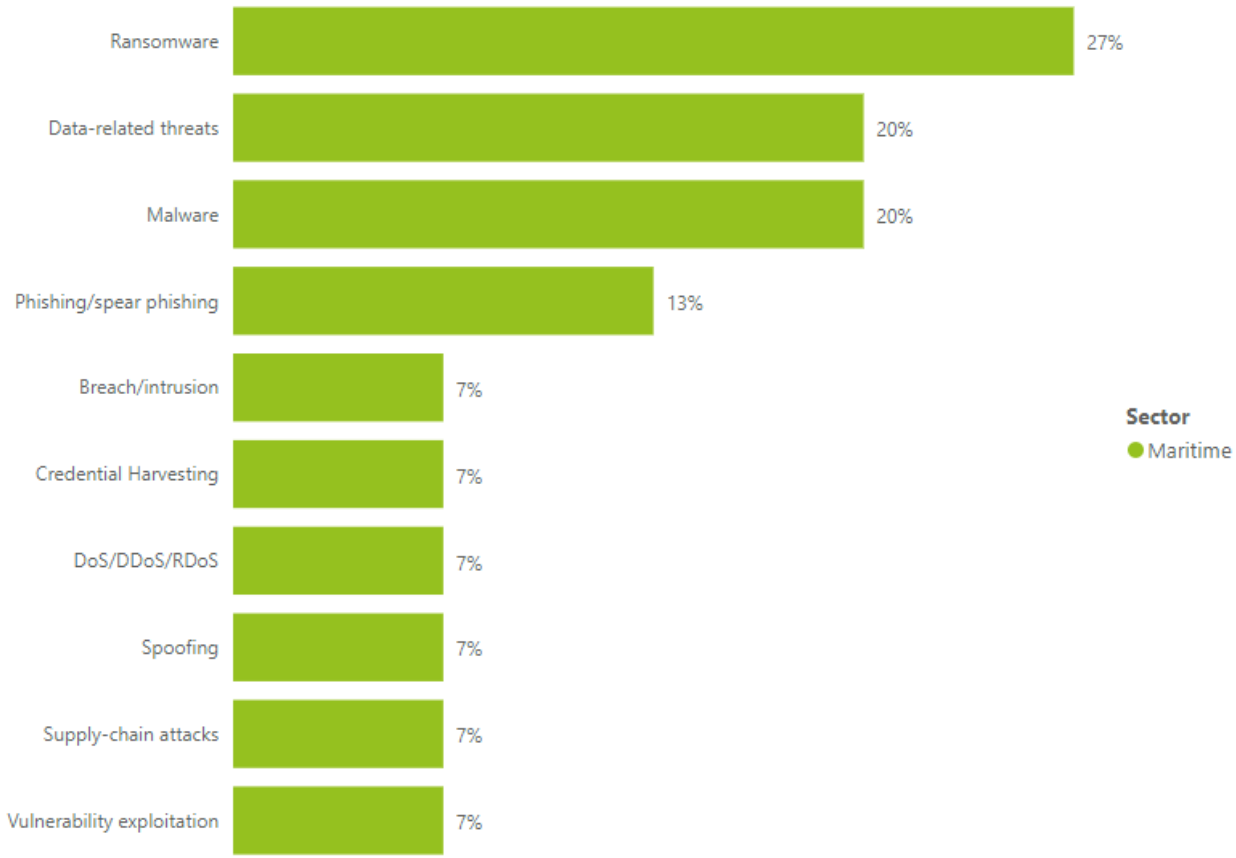
Figure 25: Aviation - targets



3.2 MARITIME SECTOR

The proliferation of cybersecurity incidents[35] in ports over the last few years, such as the cyberattack on Antwerp port[36], the NotPetya ransomware incident and its impact on Maersk[37] and the wave of ransomware attacks on the Port of Barcelona [38] and San Diego[39], has led to a change in the sector's cyber risk profile. Figures 26 and 27 show the threats targeting the maritime sector overall and on an annual basis.

Figure 26: Maritime - prime threats



Attacks in the maritime domain are often politically motivated and perpetrated by state-sponsored attackers. During 2021 and 2022, a few notable cases of activities linked to state actors were reported. These attacks indicate the interest of state sponsored actors to cause operational disruption by targeting ports and vessels.

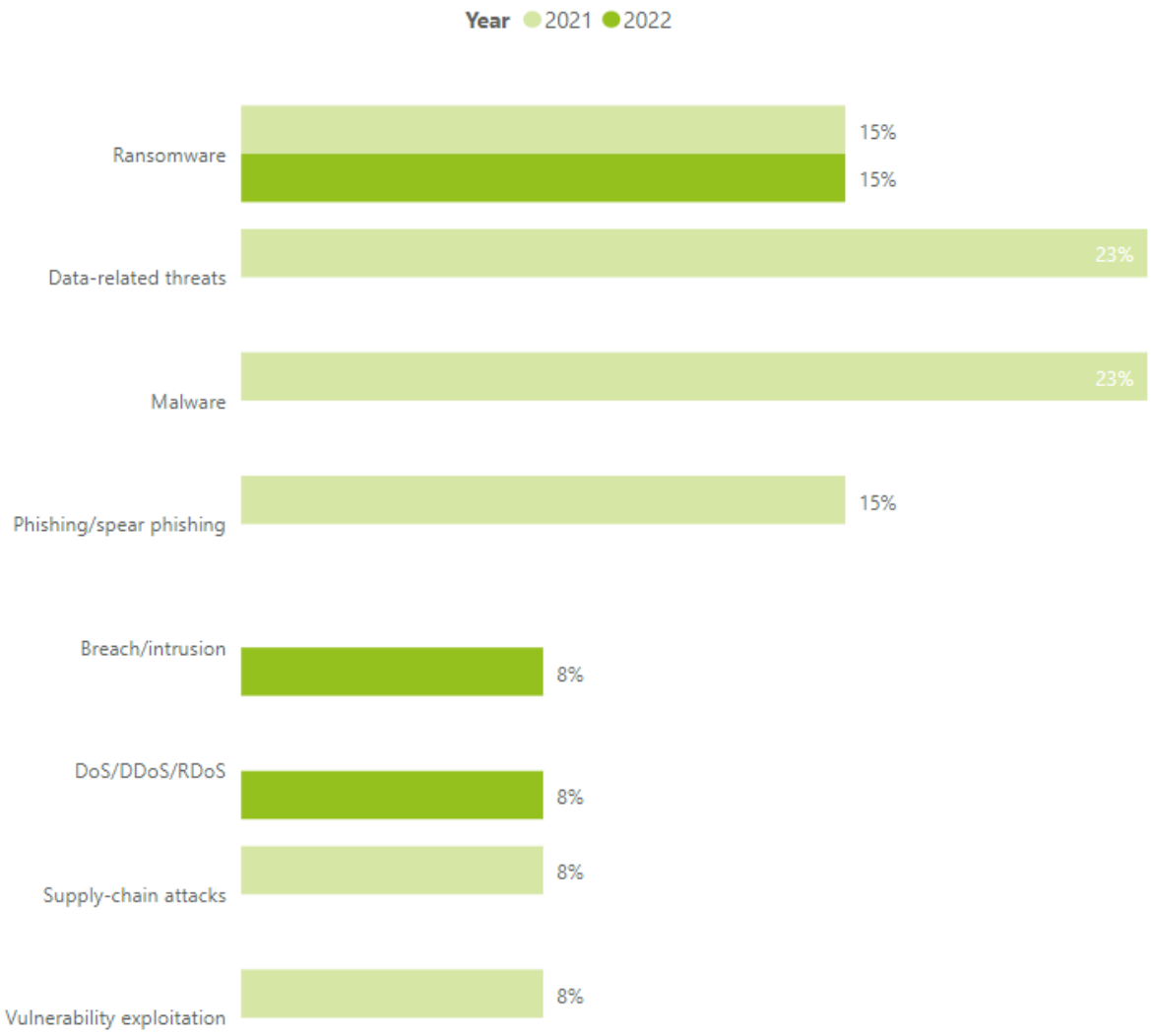
In early 2021, it was reported that two Indian sea ports were targeted by Chinese hackers amid geopolitical tensions[40]. In August 2021 the Port of Houston Authority was targeted by a cybersecurity attack which is believed to have originated from a nation-state actor. In October 2021 Microsoft reported that 'Iran-linked' hackers targeted US, EU and Israeli defence and maritime sectors with password spray attacks[41]. May 2022 Israel was linked to a disruptive cyberattack on an Iranian port facility[42]. Computers that regulate the flow of vessels, trucks and goods all crashed at once, creating massive congestions on waterways and roads leading to the facility. In May 2022 the Port of London Authority was hit by a DDoS attack, which temporarily took the Port of London's website offline. The attack is believed to have been carried out by the Iran-affiliated Altahrea group and politically rather than financially

[35] https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/@@download/fullReport
[36] https://www.bbc.com/news/world-europe-24539417
[37] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[38] https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/
[39] https://www.darktrace.com/en/blog/troubled-waters-cyber-attacks-on-san-diego-and-barcelonas-ports/
[40] https://www.recordedfuture.com/redecho-targeting-indian-power-sector
[41] https://www.microsoft.com/en-us/security/blog/2021/10/11/iran-linked-dev-0343-targeting-defense-gis-and-maritime-sectors/
[42] https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

motivated[43]. This group is known for having made multiple DDoS attacks on Israeli targets, including the Israel Ports Authority, in the past.

Finally, an interesting threat that may affect vessels is the spoofing of the automatic identification system[44] by a hostile state, although we have not seen many occurrences of this threat in the past.

Figure 27: Maritime - prime threats (annually)



When it comes to activity by cybercriminals or individual actors, we primarily observe ransomware, malware and phishing / spear-phishing attacks targeting the port authorities, port operators or manufacturers (supply chain) (see Figure 28).

Examples include the following.

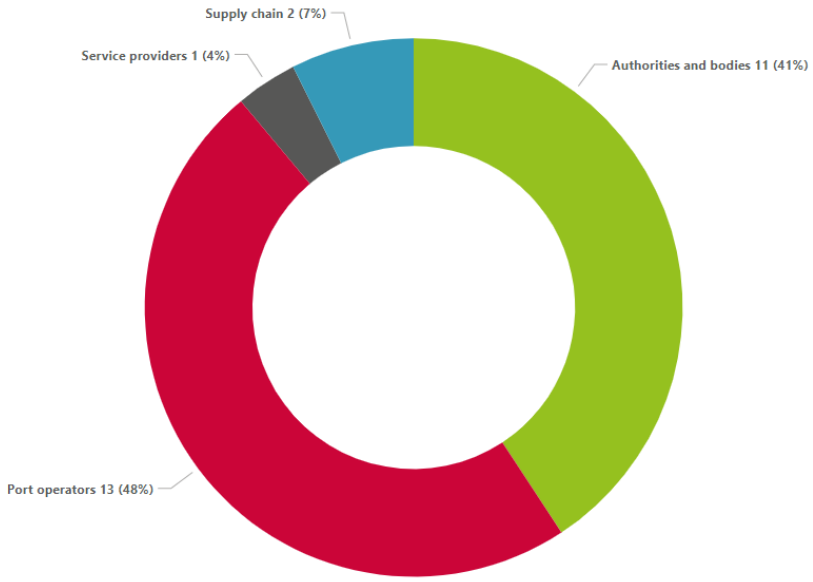
- In February 2021 French boat building giant Beneteau announced that it had suffered a malware intrusion on some of its servers and that it had decided to disconnect all 'information systems' to prevent the malware from spreading. Several production units, notably in France, had to slow down or stop their production activities for a few days[45].

[43] https://safety4sea.com/cyber-attack-targets-port-of-london-authority/
[44] https://www.theregister.com/2021/06/24/russia_ais_spoofing/
[45] https://www.securityweek.com/boat-building-giant-beneteau-says-cyberattack-disrupted-production

- In June 2021 the Massachusetts Steamship Authority was targeted by a ransomware attack which brought down its website and caused delays for ferry passengers.
- In August 2021 the Compagnie générale de navigation sur le Lac Léman fell victim to a cyberattack on its website, targeting the ticketing system. The hackers managed to steal the bank details of some customers[46].
- In September 2021 French carrier CMA CGM confirmed a data leak, which involved customer information, including names, employers, positions, email and phone details[47].
- In November 2021 a ransomware attack on the maritime IT company Danaos (ICT service provider) affected several Greek shipping companies who used the Danaos' communication systems[48]. Reportedly, the cyberattack blocked their communication with ships, suppliers, agents, charterers and suppliers, while at the same time the files with their correspondence were lost.
- In February 2022 a suspected ransomware attack knocked out the management information system at the Jawaharlal Nehru Port Container Terminal, one of five container terminals in India's top container gateway, the Jawaharlal Nehru Port Trust (Nhava Sheva). The Jawaharlal Nehru Port Container Terminal had one of its scheduled vessels divert to a nearby terminal after it abruptly stopped accepting vessels. At the same time, the system breakdown left port users no choice but to revert to paper-based cargo processing. This caused major traffic problems at the gates of the port, also disrupting traffic at the gates of other terminals[49].

Moreover, there were major disruptions in other ports where we lack information on what type of attack took place. For example, in July 2021 four major ports in South Africa (Cape Town, Ngqura, Port Elizabeth and Durban) were paralysed following a massive attack on the Transnet National Port Authority, the country's main freight manager[50]. In January 2022, several northern European oil hubs in major ports were the target of cyberattacks[51]. IT systems have been disrupted at Oiltanking in Germany, SEA-Invest in Belgium and Evos in the Netherlands.

Figure 28: Maritime - targets

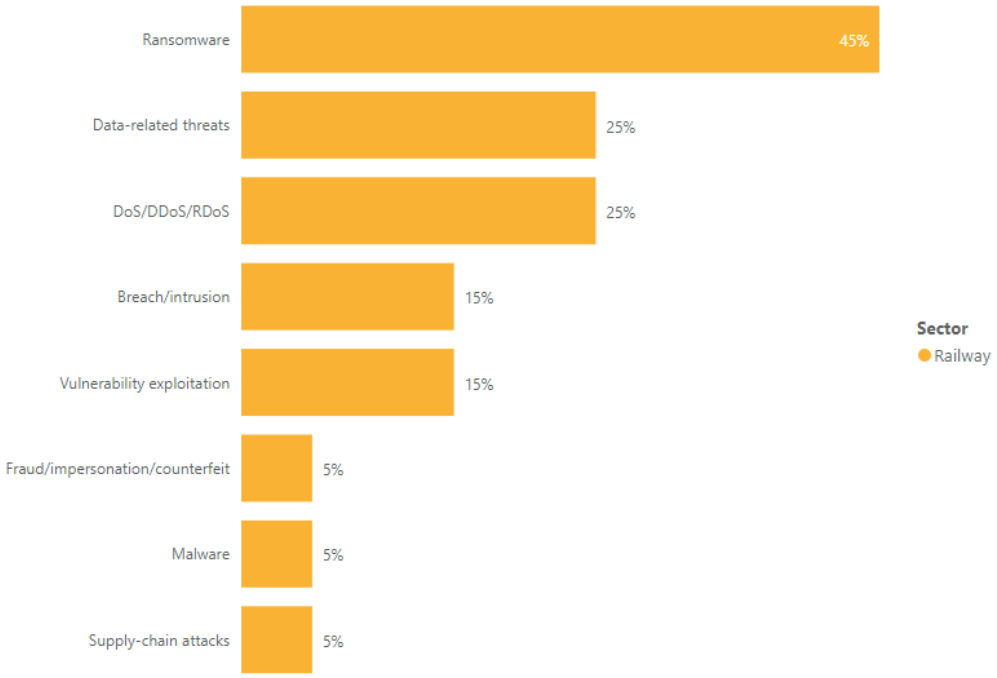


[46] https://www.radiolac.ch/actualite/la-cgn-victime-dune-cyberattaque-sur-son-site-internet/
[47] https://lloydslist.maritimeintelligence.informa.com/LL1138249/CMA-CGM-confirms-data-leak-after-cyber-attack
[48] https://icsstrive.com/incident/ransomware-attack-at-maritime-it-company-danaos-propagated-to-greek-shipping-companies/
[49] https://theloadstar.com/truck-queues-lengthen-as-nhava-sheva-tries-to-restore-it-after-cyber-attack/
[50] https://maritime.direct/en/2021/07/23/port-operations-disrupted-by-cyber-attack; https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/; https://www.fas.usda.gov/data/south-africa-cyber-attack-cripples-operations-port-durban-second-time-month; https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/
[51] https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/; https://www.bbc.com/news/technology-60250956 https://www.techzine.eu/news/security/72268/belgian-port-giant-sea-invest-hit-by-hacking-attack/; https://www.reuters.com/article/belgium-cyber-idUSL1N2UE0PS

3.3 RAILWAY SECTOR

Figure 29 and Figure 30 show the threats targeting the railway sector overall and on an annual basis. Ransomware and data-related threats are the two main threats targeting the railway sector (45% and 25%, respectively), followed by DDoS attacks with an increasing rate. Ransomware and Data-related threats are closely interlinked, as a ransomware attack is often followed by data leakage or exfiltration.

Figure 29: Railway - prime threats



The majority of the attacks observed targeted the IT systems of railways (passenger services, ticketing systems, mobile application, display boards, etc.) and caused disruptions due to the unavailability of these services. Examples include the ransomware attacks targeting Skånetrafiken (August 2021) and Ferrovie dello Stato Italiane (March 2022), which resulted in customers not being able to buy tickets following infections to IT systems. The only cases were OT systems and networks were affected were either when entire networks were affected or when safety-critical IT systems were unavailable.

Notable data thefts include the cases of OmniTRAX, MTA, Norfolk Southern Railroads and Lokaltog A/S, where personnel and medical records were stolen. The case of OmniTRAX represents the first publicly known case of a double-extortion ransomware attack against a US freight rail operator.

Another interesting case includes the service disruptions to the Danish train operator DSB's network (October 2022) due to an attack on one of its ICT service providers after an alleged DDoS attack. The incident reportedly affected the accessibility of a key safety-critical IT system, thereby disrupting DSB operations for several hours that day.

Finally, an interesting case is the one of hacktivists launching a ransomware attack on the Belarusian state-run train company in a bid to disrupt Russian troop movements (January 2022). To achieve this, the group deployed modified ransomware to bring down the railway system and encrypted servers, databases and workstations belonging to the Belarusian railway service.

Figure 30: Railway - prime threats (annually)

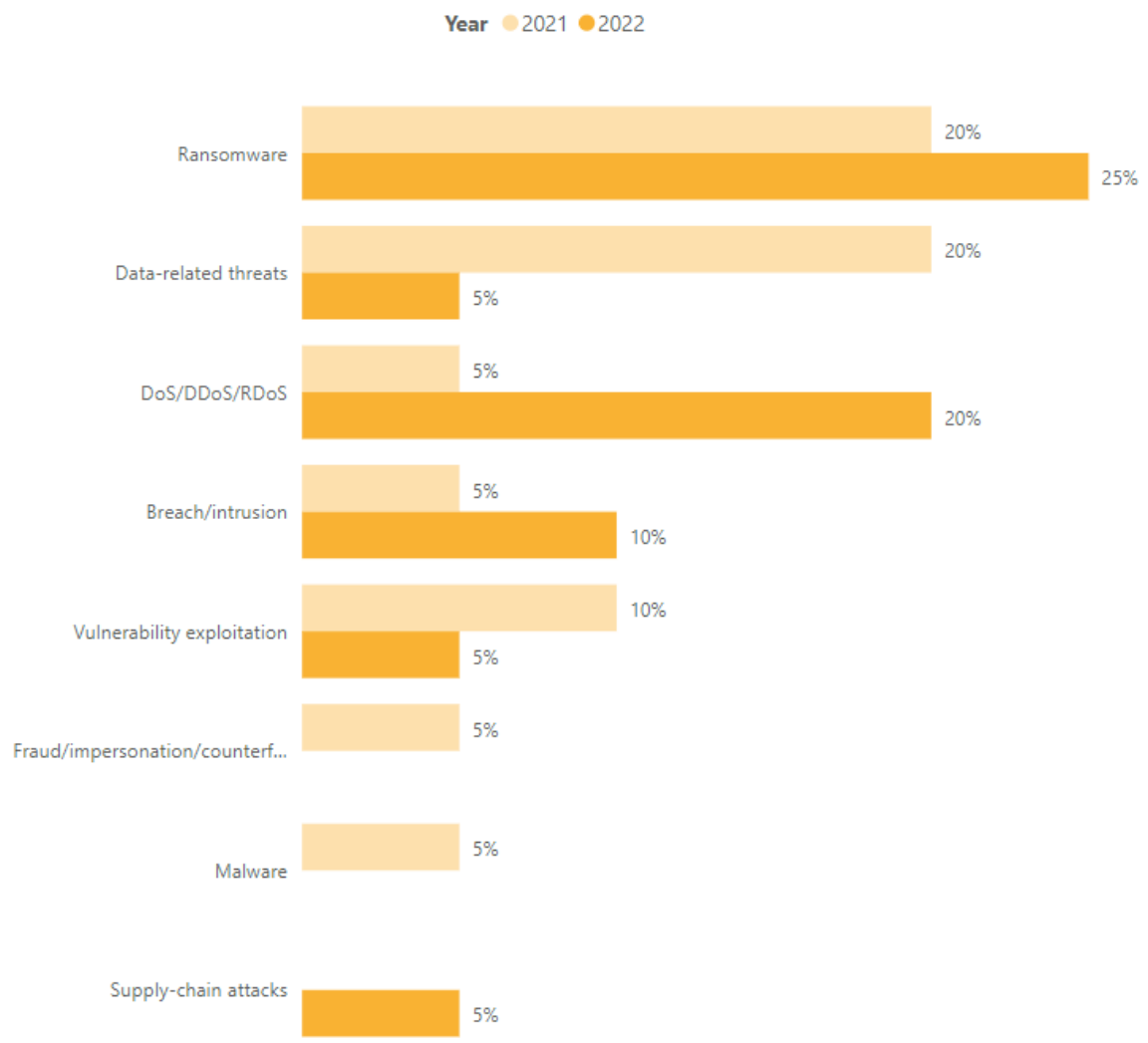
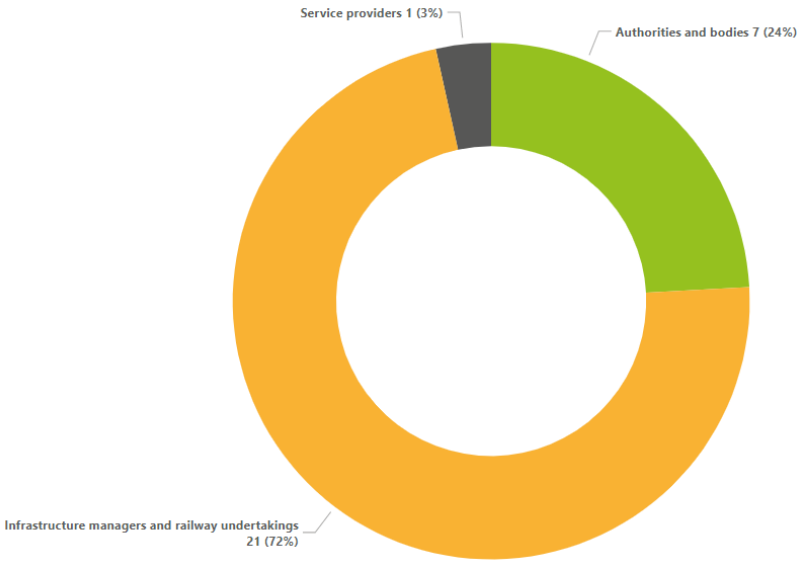


Figure 31: Railway - targets



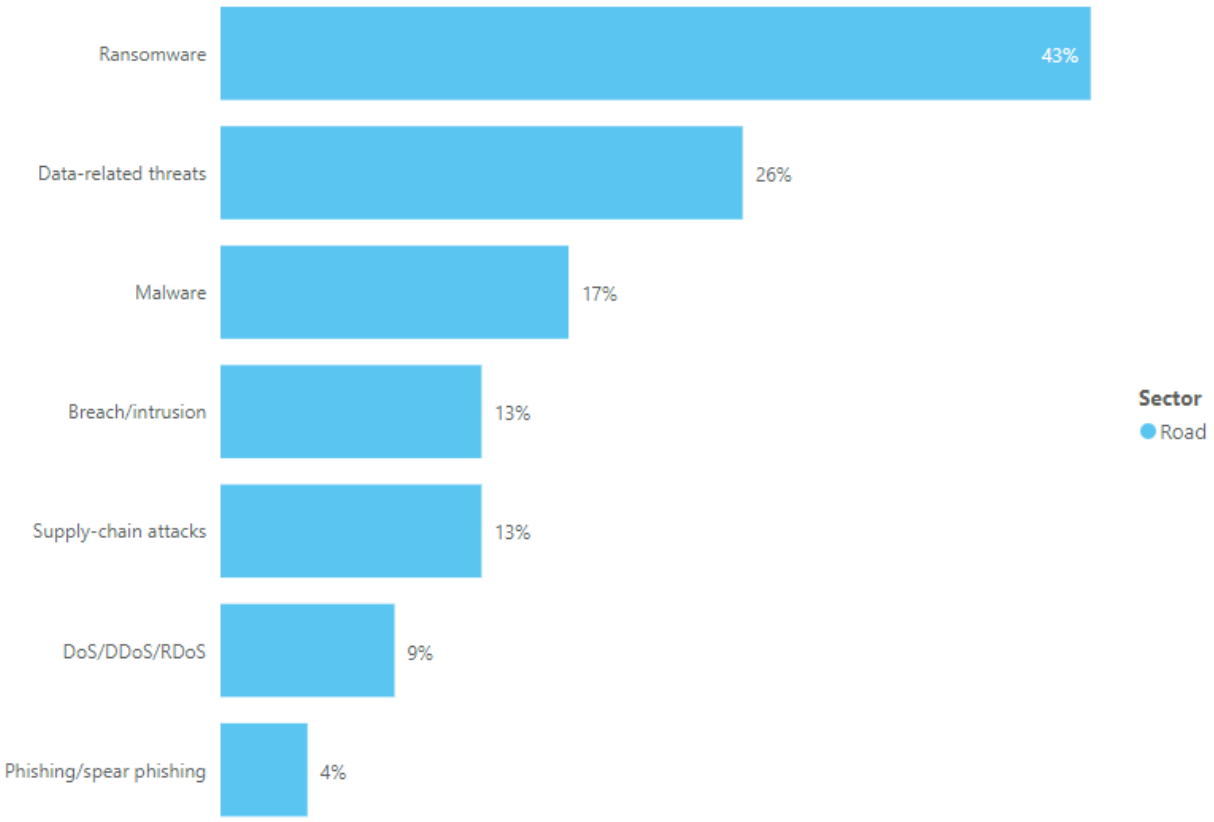
DDoS attacks were on the rise in 2022, reaching one fifth of the attacks on the railway sector (20%). This is primarily due to the increased hacktivist activity which followed Russia's unprovoked invasion of Ukraine. Hacktivist elements with pro-Russian/anti-NATO sentiments have been conducting DDoS attacks against railway companies. Examples include pro-Russia hacker groups claiming responsibility for attacks on railway transport operator CFR Calatori (April 2022), Lithuanian Railways (June 2022), Latvian passenger train company SJSC (June 2022) and Estonian Railways (August 2022).

When it comes to vulnerabilities (15%), two cases stand out. In December 2021 Canadian transportation agency Metrolinx temporarily took down their website as a precautionary measure, after being informed by the federal government about a cyber vulnerability. In January 2022, an anonymous hacker reported a vulnerability impacting the Swiss national railway system and potentially allowing access to customers' personal data.

3.4 ROAD SECTOR

Figure 32 and Figure 33 show the threats targeting the road sector overall and on annual basis. Ransomware is the predominant threat (43%) for the road transport sector, followed by data-related threats (26%) and malware (17%).

Figure 32: Road - prime threats

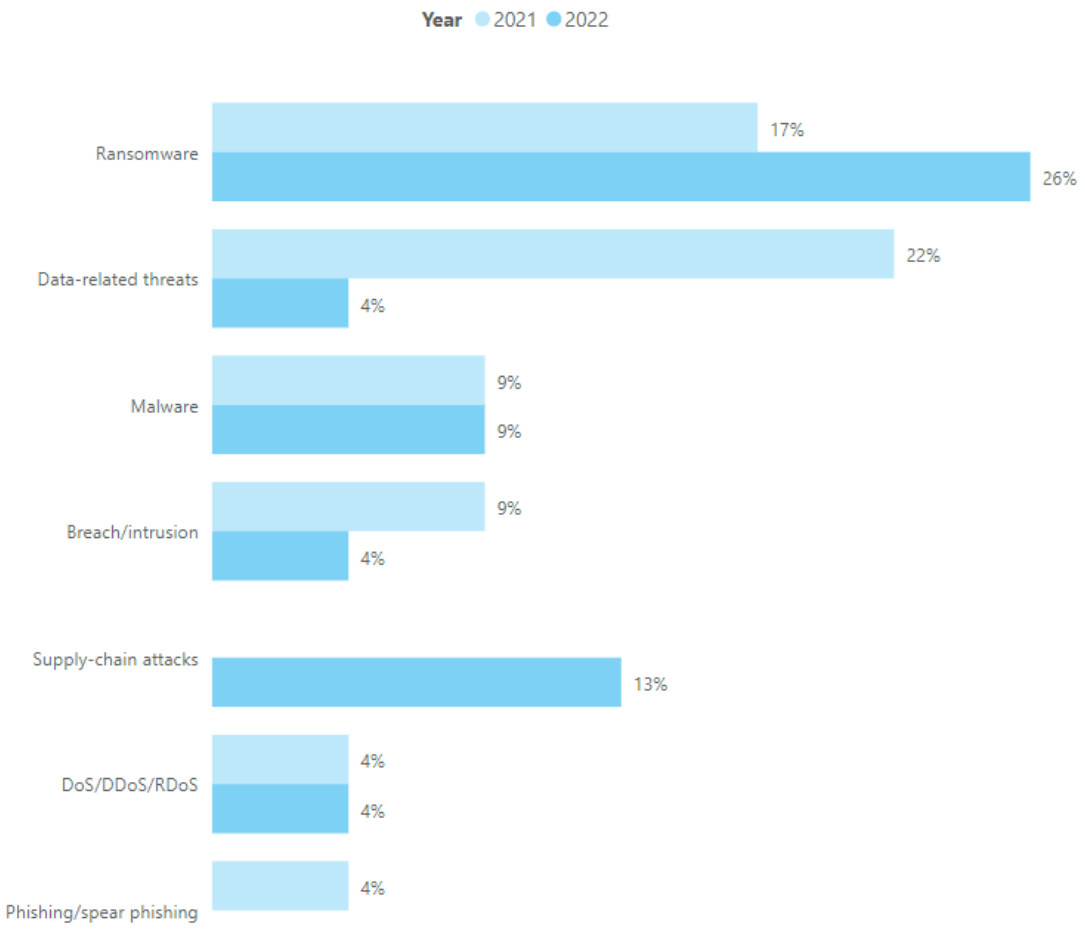


Ransomware has targeted the automotive industry, in particular OEMs and tier-X suppliers. In some cases, the production of vehicles or parts had to stop due to an attack. Notable cases include the following.

- In September 2021 Dutch car company Bochane fell victim to a ransomware attack. According to the report, which was published on the company website, a lot of their computers were blocked for a day[52].
- In February 2022 Toyota Motor Corporation suspended factory operations for a day, losing around 13 000 cars of output, after a supplier of plastic parts and electronic components was hit by a suspected cyberattack[53].
- In February 2022 Kia Motors America suffered a ransomware attack by the DoppelPaymer gang, demanding USD 20 million for a decrypter and to not leak stolen data. The attack was acknowledged in the public domain after Kia Motors America portals faced major outages and internal disruptions to its customer-facing systems across the country[54].
- In March 2022 Japanese car parts giant Denso[55] shut down the network connections of compromised devices after detecting a breach. The incident has not led to the disruption of production activities, with plants continuing to operate normally. However, the hacker group Pandora has taken credit for the attack, claiming to have stolen 1.4 terabytes of data.

[52] https://www.omroepflevoland.nl/nieuws/254573/autobedrijf-bochane-gehackt
[53] https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/
[54] https://aithority.com/security/doppelpaymer-ransomware-attack-sinks-a-global-motor-companys-20-million/
[55] https://www.securityweek.com/car-parts-giant-denso-targeted-ransomware-group

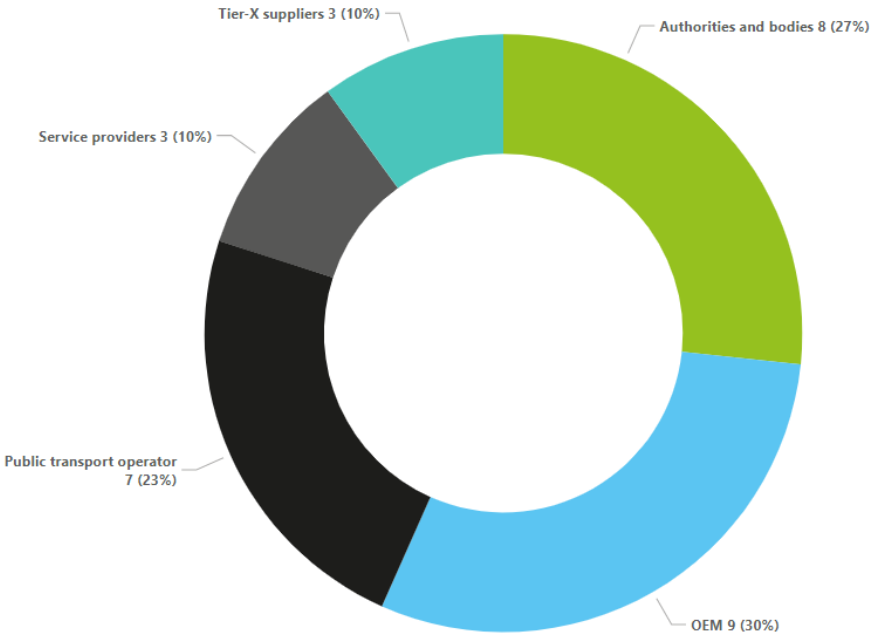
Figure 33: Road - prime threats (annually)



- In April 2022 Germany's car rental giant Sixt was hit by cyberattack[56]. All non-essential services were shut down. It was assumed that ransomware groups are focusing on an organisation like Sixt because of the upcoming tourist season.
- In May 2022 AGCO Corporation sites in China, France, Germany and the US suffered a ransomware attack, making servers inaccessible and halting production for 2 days[57].
- In June 2022 a US subsidiary of Nichirin[58], a Japanese company that makes hoses for the automotive industry, was hit by ransomware. The incident forced the company to shut down some production control systems and switch to manual processes.

[56] https://www.infosecurity-magazine.com/news/car-rental-giant-sixt-hit-by/
[57] https://france3-regions.francetvinfo.fr/hauts-de-france/oise/beauvais/piratage-informatique-le-site-d-assemblage-de-tracteurs-massey-fergusson-agco-beauvais-victime-d-une-cyber-attaque-2537316.html
[58] https://www.securityweek.com/us-subsidiary-automotive-hose-maker-nichirin-hit-ransomware

Figure 34: Road - targets



Data-related threats primarily targeted IT systems in an effort to acquire customer or employee data and proprietary information. In February 2021, hackers published the data of more than 3.2 million users of DriveSure (US car dealership service provider focused on employee training programmes and customer retention)[59]. According to the sources, hackers published leaked folders with over 22 GB of MySQL databases with not only personal information, but also 93 063 hashed passwords and emails with clients. In August 2021, Skånetrafiken (Sweden's regional public transportation authority and operator) was, for the second time, the subject of cyberattacks. The target was ticketing machines and the website for buying tickets[60]. Strætó[61] (public transport company which operates city buses in the Icelandic capital) also fell victim to cyberattacks, where the personal data of employees was stolen.

Notable cases of proprietary information being stolen or leaked include the attacks on Tesla and Volvo. In September 2021 Tesla's 'top-secret full self-driving AI car software'[62], which enables Tesla cars to drive autonomously, was leaked, enabling hackers outside the US to use this functionality. In December 2021 Volvo disclosed in a press release[63] that unknown attackers had stolen R & D information by hacking some of their servers, but did not confirm the nature of the attack, which was allegedly a ransomware attack.

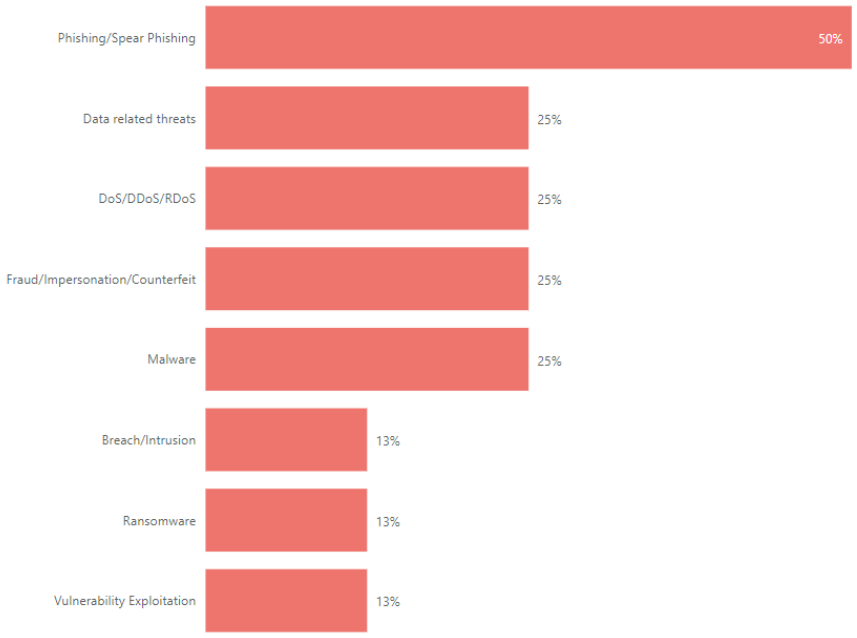
[59] https://www.riskbasedsecurity.com/2021/02/01/personal-data-of-3-million-people-exposed-in-drivesure-hack/
[60] https://www.svt.se/nyheter/lokalt/skane/skanetrafikens-sajt-och-app-ur-funktion
[61] https://straeto.is/en/user-information/cyber-attack-against-straeto
[62] https://www.dailystar.co.uk/tech/news/elon-musks-top-secret-full-24929177
[63] https://www.media.volvocars.com/global/en-gb/media/pressreleases/292817/notice-of-cyber-security-breach-by-third-party-1

3.5 CROSS SECTOR ATTACKS

Finally, there is a limited number of cyber incidents that cannot be placed in one specific subsector. These include general campaigns targeting the whole transportation sector in particular countries. These campaigns are often attributed to hacktivists and state-sponsored actors and are linked to geopolitical tensions.

Moreover, there are also incidents where attackers directly target transport agencies. Examples include incidents of impersonation, such as in the case of the US Department of Transport, which was the target of phishing attacks both in September 2021[64] and in September 2022[65]. For more examples of these types of attacks, please refer to the Annex.

Figure 35: Threats targeting the transport sector as a whole



The report did not analyse the effect of cyber-attacks which target sectors that transport depends on. Such an analysis would include energy and telecommunication. This is an interesting aspect to examine in future threat landscapes.

[64] https://threatpost.com/attackers-impersonate-dot-phishing-scam/169484/?web_view=true
[65] https://www.bleepingcomputer.com/news/security/microsoft-365-phishing-attacks-impersonate-us-govt-agencies/; https://cofense.com/blog/credential-phishing-targeting-government-contractors-evolves-over-time

4. CONCLUSIONS

In this report, we have performed a deep dive into the threat landscape of a particular sector, namely the transport sector. While the annual ENISA threat landscapes include sectorial analysis, the documents do not analyse the context of each sector in depth. In this report, we have tried to shed more light in the types of incidents, the actor motivations, the affected assets, the victims and the potential impacts to the transport sector. This information is often sector specific and can provide more valuable information for risk management to the cybersecurity professionals in the transport sector.

Ransomware attacks became the most significant threat against the sector during 2022, surpassing data-related threats, which were the most significant threat in 2021

. However, it is still assessed that ransomware groups remain opportunistic and relatively indiscriminate in their targeting. Recent months do not indicate that there has been any particular focus on the transport sector relative to other sectors. Ransomware has been steadily increasing[66] and the transport sector has been affected similarly to the other sectors.

Our assessment is that **threat actors will increasingly conduct ransomware attacks with not only monetary motivations[66]**. An example is the ransomware attack by Belarusian hacktivists against the Belarusian state railway in January 2022[67]. Hacktivists will likely be attracted by the effectiveness and the impact that ransomware attacks can have and the media attention they attract. The scale and sophistication of hacktivists' ransomware operations are not expected to be as high as the ones conducted by cybercriminals. Finally, governmental organisations are very likely the primary targets of hacktivists' ransomware operations.

The significant increase in hacktivist activity, which followed Russia's unprovoked invasion of Ukraine, and the increasing rate of DDoS attacks are highly likely to continue. Hacktivist elements with pro-Russian/anti-NATO sentiments have been conducting DDoS attacks. These attacks targeted several European nations, perceived by the groups to be assisting Ukraine in its war effort. This increasing volume of DDoS attacks against the European transport sector was primarily observed in Q2 and Q3 2022. The main targets were European airports, railways and transport authorities. Several examples are listed below (see Annex for further information).

- In April 2022 pro-Russia hacker group Killnet claimed to be behind attacks on Romanian government websites, including railway transport operator CFR Calatori[68].
- In May 2022 Czechia's Directorate of Roads and Highways was targeted with DDoS attacks by Killnet, resulting in disruption to web-based services[69].
- In May 2022 Several Italian transport organisations were targeted with DDoS attacks by Legion - Cyber Spetsnaz RF[70].
- In June 2022 Killnet claimed to have disrupted the website of Lithuanian Railways, preventing passengers from purchasing train tickets online[71].
- In June 2022 Latvian passenger train company SJSC was targeted with DDoS attacks, likely by pro-Russian hacktivists[72].
- In July 2022 NoName057 targeted two Lithuanian airports with DDoS attacks[73].

[66] ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[67] https://www.infosecurity-magazine.com/news/belarus-activists-fire-ransomware/; https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/; https://www.railway-technology.com/news/belarusian-railway-cyber-breach/
[68] https://www.romania-insider.com/romania-state-websites-cyberattack-2022
[69] https://english.radio.cz/cyber-agency-says-attack-czech-states-road-and-motorway-directorate-encoded-data-8751033
[70] https://www.wired.it/article/attacco-cyber-russia-italia-legion-ministero-polizia/
[71] https://www.lrt.lt/en/news-in-english/19/1728365/major-incidents-contained-after-lithuania-gets-hit-with-massive-cyber-attacks
[72] https://www.apollo.lv/7535816/ddos-uzbrukumu-del-trauceta-pasazieru-vilciena-bilesu-tirdznieciba-uznemuma-majaslapa
[73] https://www.lrt.lt/en/news-in-english/19/1728365/major-incidents-contained-after-lithuania-gets-hit-with-massive-cyber-attacks

- In August 2022 Killnet claimed responsibility for attacks to more than 200 state and private Estonian institutions, including Estonia Railways[74].
- In August 2022 a pro-Russia hacker group known as the Cyber Army of Russia targeted the Ukrainian government's Department of Transport Safety.

Even though pro-Russian hacktivists continue to target transport organisations in Ukraine and neighbouring countries, the capabilities of most pro-Russian hacktivists remain low and are largely limited to DDoS and defacement attacks. On the other hand, hacktivists supporting Ukraine have been conducting DDoS and 'hack and leak' operations. Some examples include the following.

- In March 2022 hacktivist collective Anonymous (presumably) carried out an attack on the Russian Federal Air Transport Agency, deleting approximately 65 terabytes of data[75].
- In April 2022 Anonymous-linked group GhostSec claimed to have accessed an IT system of Metrospetstekhnika[76].
- In August 2022 Anonymous claimed to have hacked Yandex Taxi, causing a massive traffic jam in Moscow[77].
- In September 2022 transport in Novosibirsk was affected as hacker security group Team Onefist disrupted traffic[78].

The **majority of attacks to the transport sector target IT systems** and can result in operational disruptions. However, **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[66]. The factors contributing to this assessment are:

- the ongoing digital transformation in the transport sector and the increased connectivity between IT and OT networks;
- the increased urgency to pay ransom to avoid any critical business and social impact;
- the ongoing rebranding of ransomware groups, which increases the chances of malware blending and the development of capabilities to target and disrupt OT networks;
- Russia's military aggression against Ukraine, as ransomware groups are taking sides and are likely to conduct retaliatory attacks against critical western infrastructure;
- the increase in the number of newly identified vulnerabilities in OT environments.

The analysis of the ransomware threat landscape from May 2021 to June 2022 resulted in some conclusions that can be regarded as lessons for the community.

While 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. Jamming and spoofing of geolocation data could affect their availability and integrity, affecting transport sector operations. This type of attack requires further analysis in the future.

When it comes to mitigating threats which target the transport sector, readers may consult the recommendations and security measures included in Annex D of the *ENISA Threat Landscape 2022*[79]. For each threat type, specific recommendations are provided and mapped to security measures that are part of international standards used by entities under the NIS Directive, including transport organizations[80].

[74] https://www.ohtuleht.ee/1068880/kuberrunnakus-sai-pihta-ka-eesti-raudtee
[75] https://www.aviacionline.com/2022/03/cyber-attack-on-russias-aviation-authority-this-is-what-we-know/
[76] https://securityaffairs.co/wordpress/130409/hacktivism/anonymous-hacked-other-russian-organizations.html
[77] https://securityaffairs.co/wordpress/135280/hacktivism/anonyomus-hacked-yandex-taxi.html
[78] https://www.ibtimes.com/russians-novosibirsk-forced-pound-pavements-team-onefist-paralyzes-traffic-exclusive-3611628
[79] ENISA Threat Landscape 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[80] Minimum Security Measures for Operators of Essentials Services https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

In general, cyberattacks are rarely reported, especially those with non-significant impact or near misses. Most organisations prefer to deal with the problem internally and avoid bad publicity. Some countries have laws regulating the mandatory reporting of incidents, but in most cases a security attack is first disclosed by the attacker. In the EU, the arrival of the revised NIS2 directive[81] and the enhanced notification provisions for security incidents is expected to support a better understanding of relevant incidents.

The lack of reliable data from targeted organisations makes it very hard to fully understand the problem or even know how many cyberattacks on the transport sector actually occur. Even using the data from the web pages of threat actors (an undeniably unreliable source), it is very hard to keep track of the actual number of attacks. The most important information that is missing is the technical explanation as to how the attackers obtained access to the targets. This is usually private data that describes the security posture of the target, so it is never shared with the public. As a consequence, our learning as a community of the problems to be solved remains fragmented and isolated.

Moreover, the effects of cross sector dependencies could be of particular interest to the transport sector. We would require a more detailed analysis of how cyberattacks targeting the energy and telecommunications sectors could affect transport or how an attack on one means of transport could cause a disruption to another means of transport.

[81] https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-new-rules-cybersecurity-network-and-information-systems

ANNEX: MAJOR INCIDENTS

Table 1: Aviation

Date	Proximity	Country	Incident
January 2021	Near	France	Dassault Falcon Jet were hit by the Ragnar Locker ransomware gang[82].
January 2021	Far	Global	A Chinese hacking group stole airline passenger details[83].
March 2021	Near	Switzerland	The passenger service system provider SITA was hacked; hundreds of thousands of Star Alliance passengers' details were stolen[84].
April 2021	Global	Global	Malware attack on Radixx Res disrupts 20 airlines' ticket reservation systems[85].
May 2021	Global	Global	RevengeRAT and AysncRAT target aerospace and aviation [86].
May 2021	Global	India	Air India suffered a data breach, 4.5 million customers impacted, two months SITA was hacked[87].
May 2021	Near	Cyprus	Hacker unsuccessfully tried to attack Larnaca airport server[88].
August 2021	Far	Guatemala	The website of the Dirección General de Aeronáutica Civil suffered a cyberattack.
August 2021	Far	Thailand	Bangkok Air confirmed that a passenger information leak had occurred after a ransomware attack[89].
October 2021	Far	Russia	New APT ChamelGang targeted Russian energy and aviation organisation[90].
February 2022	Mid	Switzerland	BlackCat claimed responsibility for an attack on Swissport[91].
February 2022	Far	Mauritius	The computer network of Air Mauritius fell victim to a cyberattack[92].
February 2022	Near	Poland	An attack on the Polish Medical Air Rescue collapsed virtually all their systems[93].
March 2022	Far	Russia	An unidentified group (presumed to be the hacking group Anonymous) carried out an extremely effective attack on the Russian Federal Air Transport Agency[94].
April 2022	Far	Canada	Canadian low-cost airline Sunwing Airlines faced 4 days of extensive flight delays after the third-party software system was breached by hackers[95].
April 2022	Mid	Israel	The website of the Israel Airports Authority was knocked offline due to a denial-of-service attack[96].

[82] https://securityaffairs.co/wordpress/113216/data-breach/dassault-falcon-data-breach.html
[83] https://www.zdnet.com/article/a-chinese-hacking-group-is-stealing-airline-passenger-details/
[84] https://www.theguardian.com/world/2021/mar/05/airline-data-hack-hundreds-of-thousands-of-star-alliance-passengers-details-stolen
[85] https://www.databreaches.net/malware-attack-on-radixx-res-disrupts-20-airlines-ticket-reservation-systems/
[86] https://www.zdnet.com/article/cyberattacks-against-the-aviation-industry-that-flew-under-the-radar-linked-to-nigerian-threat-actor/
[87] https://securityaffairs.co/wordpress/118162/data-breach/air-india-data-breach.html
[88] https://cyprus-mail.com/2021/05/30/state-bracing-for-more-cyberattacks/
[89] https://www.soy502.com/articulo/toque-queda-rehabilitan-pagina-salvoconductos-viaje-32419
[90] https://therecord.media/bangkok-air-confirms-passenger-pii-leak-after-ransomware-attack/
[91] https://securityaffairs.co/wordpress/128039/cyber-crime/blackcat-swissport-ransomware-attack.htm
[92] https://www.lemauricien.com/le-mauricien/de-lundi-a-mardi-le-reseau-informatique-de-mk-victime-dune-cyberattaque/474407/
[93] https://niebezpiecznik.pl/post/atak-na-lotnicze-pogotwie-ratunkowe/
[94] https://www.aviacionline.com/2022/03/cyber-attack-on-russias-aviation-authority-this-is-what-we-know/
[95] https://cyware.com/news/canadian-low-cost-airline-sunwing-suffers-flight-delays-due-to-third-party-breach-516d93ae/
[96] https://www.timesofisrael.com/liveblog_entry/airport-websites-hit-by-denial-of-service-attack/

Date	Proximity	Country	Incident
May 2022	Far	India	SpiceJet fell victim to a massive ransomware attack[97].
May 2022	Mid	Turkey	A Turkish airline exposed flight and crew information in 6.5 terabyte leak[98].
May 2022	Near	Italy	A pro-Russia hacker group launched a new attack on the websites of Italian ministries (Italian airports were targeted)[99].
June 2022	Near	Lithuania	NoName057 targeted Lithuanian airports with DDoS attacks[100].
August 2022	Near	Montenegro	An unprecedented cyberattack hit the state infrastructure of Montenegro[101].
August 2022	Near	Spain	Major airline technology provider Accelya was attacked by a ransomware group[102].
August 2022	Near	Portugal	TAP Air Portugal fell victim to a Ragnar Locker ransomware attack[103].
September 2022	Far	United States	Breached American Airlines email accounts were abused for phishing purposes[104].
October 2022	Near	France	LockBit 3.0 claimed to have compromised Thales Group[105].
October 2022	Far	United States	The websites of major US airports were disrupted due to a large-scale campaign of DDoS attacks by Killnet[106].

Table 2: Maritime

Date	Proximity	Country	Incident
February 2021	Near	France	Boat Building Giant Beneteau Says Cyberattack Disrupted Production[107].
March 2021	Far	India	10 Indian power generation and transmission[108] entities, and two Indian sea ports were targeted by Chinese hackers amid geopolitical tensions.
April 2021	Near	France	Bourbon confirmed that a cyberattack had occurred[109].
June 2021	Far	United States	Massachusetts Steamship Authority targeted in a cyberattack[110].
June 2021	Far	South Korea	South Korean container line HMM suffered a security breach and a cyberattack on its email systems[111].
June 2021	Near	Ukraine	Automatic identification system signals were spoofed[112].

97 https://therecord.media/spiceject-ransomware-attack-flights-grounded/
98 https://www.infosecurity-magazine.com/news/turkish-airline-exposes-flight/
99 https://www.wired.it/article/attacco-cyber-russia-italia-legion-ministero-polizia/
100 https://www.lrt.lt/en/news-in-english/19/1728365/major-incidents-contained-after-lithuania-gets-hit-with-massive-cyber-attacks
101 Unprecedented cyber attack hit State Infrastructure of MontenegroSecurity Affairs
102 https://therecord.media/major-airline-technology-provider-accelya-attacked-by-ransomware-group/
103 https://www.portugalresident.com/hackers-share-personal-data-of-1-5-million-tap-passengers
104 https://www.securityweek.com/breached-american-airlines-email-accounts-abused-phishing
105 https://cyware.com/news/lockbit-30-gang-allegedly-stole-thales-groups-data-aa676192/
106 https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/
107 https://www.securityweek.com/boat-building-giant-beneteau-says-cyberattack-disrupted-production
108 https://thehackernews.com/2021/03/chinese-hackers-targeted-indias-power.html
109 https://splash247.com/bourbon-confirms-cyber-attack/
110 https://www.bizjournals.com/boston/news/2021/06/02/ma-steamship-authority-targeted-in-cyberattack.html
111 https://www.tradewindsnews.com/containerships/hmm-confirms-cyber-attack-on-email-servers-with-system-still-largely-down/2-1-1025365
112 https://www.theregister.com/2021/06/24/russia_ais_spoofing/

Date	Proximity	Country	Incident
July 2021	Far	South Africa	Four major ports in South Africa (Cape Town, Ngqura, Port Elizabeth and Durban) were paralysed following a massive attack on the Transnet National Port Authority[113].
September 2021	Far	United States	Port Houston was targeted by a suspected nation-state actor in cyberattack[114].
September 2021	Near	Switzerland	CGN victim of a cyberattack on its website[115].
September 2021	Near	France	CMA CGM confirmed that a data leak had occurred after a cyberattack[116].
October 2021	Global	World	Microsoft says 'Iran-Linked' hackers targeted US, EU and Israeli defence and maritime sectors[117].
November 2021	Near	Greece	Danaos and Greek shipping companies fell victim to a ransomware attack[118].
November 2021	Mid	United Kingdom	Maritime giant Swire Pacific Offshore suffered a data breach following a cyberattack[119].
January 22	Near	Belgium, Germany, the Netherlands	A cyberattack disrupted northern European oil hubs in major ports[120].
February 2022	Far	India	A ransomware attack hit the Nhava Sheva container terminal[121].
May 2022	Far	Iran	Israel was linked to a disruptive cyberattack on an Iranian port facility[122].
May 2022	Mid	United Kingdom	The Port of London Authority was hit by 'politically motivated' cyberattack[123].
October 2022	Near	France	Lockbit 3.0 targeted French seaport administrator and economic interest group Dragages-Ports[124].

[113] https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22
[114] https://www.porttechnology.org/news/port-houston-targeted-by-nation-state-actor-in-cyber-attack/
[115] https://www.radiolac.ch/actualite/la-cgn-victime-dune-cyberattaque-sur-son-site-internet/
[116] https://lloydslist.maritimeintelligence.informa.com/LL1138249/CMA-CGM-confirms-data-leak-after-cyber-attack
[117] https://www.microsoft.com/en-us/security/blog/2021/10/11/iran-linked-dev-0343-targeting-defense-gis-and-maritime-sectors/
[118] https://icsstrive.com/incident/ransomware-attack-at-maritime-it-company-danaos-propagated-to-greek-shipping-companies/
[119] https://www.databreaches.net/swire-pacific-offshore-reports-cyberattack/
[120] https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/
[121] https://theloadstar.com/ransomware-attack-hits-nhava-sheva-container-terminal/
[122] https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/
[123] https://safety4sea.com/cyber-attack-targets-port-of-london-authority/
[124] https://www.redpacketsecurity.com/lockbit-3-0-ransomware-victim-dragages-ports-fr/

Table 3: Railway

Date	Proximity	Country	Incident
January 2021	Far	United States	A ransomware attack hit the short line rail operator OmniTRAX[125].
March 2021	Near	Czechia	A cyberattack hit railways in Czechia[126].
April 2021	Far	United States	Suspected Chinese hackers breached the New York City Transit Authority's computers[127].
May 2021	Mid	United Kingdom	United Kingdom rail network Merseyrail likely hit by Lockbit 3.0 ransomware[128].
July 2021	Far	Iran	Hackers breached Iranian rail network, disrupting service[129].
July 2021	Mid	United Kingdom	Northern's ticket machines were hit by a ransomware cyberattack[130].
August 2021	Near	Sweden	Skånetrafiken was exposed to a cyber attack[131].
October 2021	Near	France	French transport giant exposed 57 000 employees' information and source code[132].
November 2021	Far	Canada	After Montreal and Vancouver, Toronto's subway was also hacked[133].
December 2021	Far	Canada	The GO Transit website came back online after being down due to a worldwide cyber threat (vulnerability)[134].
January 22	Mid	Switzerland	A hacker flagged a flaw in Switzerland's national railway system[135].
January 22	Mid	Belarus	Belarusian activists fired ransomware at the country's state-run railway service[136].
February 2022	Near	Italy	The EAV suffered a cyberattack[137].
March 2022	Near	Italy	Italy's state railway may have been the target of a cyberattack[138].
April 2022	Far	Russia	Anonymous-linked group GhostSec claimed to have accessed an IT system of Metrospetstekhnika[139].
April 2022	Near	Romania	Russian hackers temporarily brought down Romanian government websites, including railway transport operator CFR Calatori[140].
June 2022	Near	Latvia	Latvian passenger train company SJSC targeted with DDoS attacks, likely by pro-Russian hacktivists[141].
June 2022	Near	Lithuania	Attackers disrupted the website of the Lithuanian Railways, preventing passengers from purchasing train tickets online[142].
July 2022	Near	Denmark	Danish regional railway company hit by a ransomware attack[143].
August 2022	Near	Estonia	Estonia was hit by cyberattacks in which Estonia Railways was targeted[144].
October 2022	Near	Denmark	Denmark's train network was stalled by a cyberattack on a subcontractor[145].

125 https://www.databreaches.net/ransomware-attack-hits-short-line-rail-operator-omnitrax
126 https://www.denik.cz/z_domova/zeleznice-hackeri-utok-vlak-20210322.html
127 https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html
128 https://www.bleepingcomputer.com/news/security/uk-rail-network-merseyrail-likely-hit-by-lockbit-ransomware/
129 https://www.reuters.com/world/Middle-east/hackers-breach-iran-rail-network-disrupt-service-2021-07-09/
130 https://www.bbc.com/news/uk-england-57892711
131 https://www.svt.se/nyheter/lokalt/skane/skanetrafikens-sajt-och-app-ur-funktion
132 https://www.infosecurity-magazine.com/news/french-transport-giant-exposes/
133 https://www.20minutes.fr/monde/3164079-20211103-canada-apres-montreal-vancouver-metro-toronto-aussi-pirate
134 https://toronto.ctvnews.ca/go-transit-website-taken-offline-due-to-worldwide-cyber-threat-1.5703584
135 https://www.infosecurity-magazine.com/news/hacker-flags-flaw-in-swiss-railway/
136 https://www.infosecurity-magazine.com/news/belarus-activists-fire-ransomware/
137 https://www.napolitoday.it/attualita/eav-attacco-informatico.html
138 https://www.reuters.com/world/us/italys-state-railway-may-have-been-target-cyber-attack-2022-03-23/?rpc=401&
139 https://securityaffairs.co/wordpress/130409/hacktivism/anonymous-hacked-other-russian-organizations.html
140 https://www.romania-insider.com/romania-state-websites-cyberattack-2022
141 https://www.apollo.lv/7535816/ddos-uzbrukumu-del-trauceta-pasazieru-vilciena-bilesu-tirdznieciba-uznemuma-majaslapa
142 https://www.lrt.lt/en/news-in-english/19/1728365/major-incidents-contained-after-lithuania-gets-hit-with-massive-cyber-attacks
143 https://www.version2.dk/artikel/lokaltog-taler-ud-om-ransomwareangreb-blev-ogsaa-ramt-sidste-aar
144 https://www.ohtuleht.ee/1068880/kuberrunnakus-sai-pihta-ka-eesti-raudtee
145 https://www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/

Table 4: Road

Date	Proximity	Country	Incident
April 2021	Near	Malta	Toyota Malta warned the public of a WhatsApp scam using its brand name [146].
June 2021	Far	United States	Cape Cod Regional Transit Authority was hit by ransomware attack [147].
June 2021	Far	India	After their attacks on India's power assets, Chinese hackers targeted the transport sector [148].
July 2021	Far	Iran	Websites of Iran's Ministry of Roads and Urban Development reportedly went out of service after another 'cyber-disruption' [149].
August 2021	Near	Sweden	Skånetrafiken was exposed to a cyberattack [150].
September 2021	Far	United States	Elon Musk's top-secret 'full self-driving' AI car software was leaked to hackers [151]
September 2021	Near	Netherlands	The car company Bochane was hit by a ransomware attack [152].
October 2021	Near	France	French transport giant exposed 57 000 employees' information and source code [153].
October 2021	Near	Germany	A threat actor leaked the Mercedes-Benz platform's source code [154].
November 2021	Near	Sweden	Volvo Cars Corporation disclosed that they had been targeted in a cybersecurity breach [155].
December 2021	Near	Iceland	Strætó suffered a cyberattack [156].
December 2021	Far	United States	Kia Motors America was hit by a DoppelPaymer ransomware attack [157].
April 2022	Near	Germany	Car rental giant Sixt was hit by a cyberattack [158].
May 2022	Far	Australia	Transport for NSW was struck by a cyberattack [159].
May 2022	Near	France	The Massey Ferguson tractor assembly site, AGCO Beauvais, was the victim of a cyberattack [160].
May 2022	Near	Czechia	Czechia's Directorate of Roads and Highways was targeted with a DDoS attack by Killnet, resulting in web-based services being disrupted [161].
June 2022	Far	United States	American subsidiary of automotive hose maker Nichirin was hit by a ransomware attack [162].
August 2022	Far	Russia	Anonymous hacked Yandex Taxi, causing a massive traffic jam in Moscow [163].
February 2022	Global	World	For Toyota, the hacking-into of a key supplier's systems led to a production halt in 14 of its Japanese plants [164].
August 2022	Far	Indonesia	Jasa Marga subsidiary clarified alleged hacking [165].
September 2022	Mid	United Kingdom	The transport company Go-Ahead suffered a cyberattack [166].

[146] https://timesofmalta.com/articles/view/toyota-malta-warns-of-whatsapp-scam-using-its-brand-name.866376
[147] https://eu.capecodtimes.com/story/news/2022/06/04/cape-cod-regional-transit-authority-ransomware-cyber-attack-fbi-investigating/7501982001/
[148] https://www.thehindubusinessline.com/news/national/after-power-chinese-hackers-target-transport-sector/article34125502.ece
[149] https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/
[150] https://www.svt.se/nyheter/lokalt/skane/skanetrafikens-sajt-och-app-ur-funktion
[151] https://www.dailystar.co.uk/tech/news/elon-musks-top-secret-full-24929177
[152] https://www.omroepflevoland.nl/nieuws/254573/autobedrijf-bochane-gehackt
[153] https://www.infosecurity-magazine.com/news/french-transport-giant-exposes/
[154] https://cybernews.com/news/threat-actors-leak-mercedes-benzs-platform-source-code/
[155] https://autosec.se/volvo-cars-corporation-disclose/
[156] https://straeto.is/en/user-information/cyber-attack-against-straeto
[157] https://aithority.com/security/doppelpaymer-ransomware-attack-sinks-a-global-motor-companys-20-million/
[158] https://www.techzine.eu/news/security/78131/car-rental-giant-sixt-shut-down-following-cyberattack/
[159] https://www.zdnet.com/article/transport-for-nsw-struck-by-cyber-attack/
[160] https://france3-regions.francetvinfo.fr/hauts-de-france/oise/beauvais/piratage-informatique-le-site-d-assemblage-de-tracteurs-massey-fergusson-agco-beauvais-victime-d-une-cyber-attaque-2537316.html
[161] https://english.radio.cz/cyber-agency-says-attack-czech-states-road-and-motorway-directorate-encoded-data-8751033
[162] https://www.securityweek.com/us-subsidiary-automotive-hose-maker-nichirin-hit-ransomware
[163] https://securityaffairs.co/wordpress/135280/hacktivism/anonyomus-hacked-yandex-taxi.html
[164] https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/
[165] https://en.tempo.co/read/1626771/jasa-marga-subsidiary-clarifies-alleged-hacking-data-leak
[166] https://www.theguardian.com/business/2022/sep/06/go-ahead-cyberattack-bus-services-thameslink-rail

Date	Proximity	Country	Incident
September 2022	Near	Global	Uber was hacked, its internal systems breached and vulnerability reports stolen[167].
September 2022	Far	Russia	Transport in Novosibirsk was affected as team Onefist disrupted traffic[168].
October 2022	Near	Germany	An info-stealer campaign targeted German car dealerships and manufacturers[169].

Table 5: Transport sector as a whole ('All transport')

Date	Proximity	Country	Incident
March 2021	Far	India	Chinese hackers targeted the transport sector[170].
September 2021	Far	United States	Attackers impersonated the US Department of Transportation in a two-day phishing scam[171].
December 2021	Far	Taiwan, Philippines, Hong Kong	Chinese hackers were spotted targeting the transport sector[172].
February 2022	Global	Global	Advanced persistent threat (APT) activity from hacker group TA2541 targeted the transport sector globally[173].
August 2022	Near	Latvia	Latvia experiences perhaps the most powerful cyberattack in its history[174].
September 2022	Far	United states	Microsoft365 phishing attacks impersonate US government agencies, including the Department of Transportation[175].
October 2022	Near	Poland, Ukraine	Cyberattacks hit Polish and Ukrainian logistics and transport companies[176].

[167] https://www.bleepingcomputer.com/news/security/uber-links-breach-to-lapsus-group-blames-contractor-for-hack/
[168] https://www.ibtimes.com/russians-novosibirsk-forced-pound-pavements-team-onefist-paralyzes-traffic-exclusive-3611628
[169] https://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/
[170] https://www.thehindubusinessline.com/news/national/after-power-chinese-hackers-target-transport-sector/article34125502.ece
[171] https://threatpost.com/attackers-impersonate-dot-phishing-scam/169484/?web_view=true
[172] https://www.securityweek.com/trend-micro-spots-chinese-hackers-targeting-transportation-sector
[173] https://industrialcyber.co/threats-attacks/ta2541-attackers-target-surface-transportation-manufacturing-defense-enterprises/
[174] https://cybershafarat.com/2022/07/31/latvia-is-experiencing-perhaps-the-most-powerful-cyber-attack-in-its-history/
[175] https://www.bleepingcomputer.com/news/security/microsoft-365-phishing-attacks-impersonate-us-govt-agencies/
[176] https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

TP-04-23-081-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-624-8
doi:10.2824/553997