ENISA THREAT LANDSCAPE: TRANSPORT SECTOR

Marianthi Theocharidou

28 | 06 | 2023
A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community.
ENISA THREAT LANDSCAPE TRADITION

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

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

Disclaimer: The information provided in this presentation is based on publicly available data (OSINT) and on that provided by CTI contractors. It is intended to be used for Situational Awareness purposes within the scope of this presentation, and statements are limited to the reporting period of the analysis. Sources are referenced and verified to the possible extent on a best effort basis at the moment of reporting. Opinions expressed in referenced sources, if any, do not constitute an ENISA position.
• January 2021 to October 2022
• Analysis of the incidents concluded in December 2022
• 98 publicly reported incidents

MAP OF OBSERVED INCIDENTS: TRANSPORT

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

Note: the size of the circle refers to the sum of observed incidents in the country during the reporting period.
Map of Observed Incidents: Per Sector

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

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>34</td>
</tr>
<tr>
<td>Data-related threats</td>
<td>26</td>
</tr>
<tr>
<td>Malware</td>
<td>15</td>
</tr>
<tr>
<td>DoS/DDoS/RDoS</td>
<td>13</td>
</tr>
<tr>
<td>Phishing/spear phishing</td>
<td>9</td>
</tr>
<tr>
<td>Supply-chain attacks</td>
<td>9</td>
</tr>
<tr>
<td>Breach/intrusion</td>
<td>8</td>
</tr>
<tr>
<td>Fraud/impersonation/counterfeit</td>
<td>5</td>
</tr>
<tr>
<td>Vulnerability exploitation</td>
<td>5</td>
</tr>
</tbody>
</table>

The chart illustrates the percentage of threats in the transport sector. Ransomware constitutes 38% of the threats, followed by data-related threats at 30%, malware at 17%, and DoS/DDoS/RDoS at 16%. Phishing/spear phishing, supply-chain attacks, breach/intrusion, fraud/impersonation/counterfeit, and vulnerability exploitation each account for 10%, 10%, 9%, 6%, and 6% respectively.
TRANSPORT: THREATS

Findings

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

Geopolitical situation and its effect on the transport sector

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

- Cybercriminal: 47 (55%)
- Hacktivist: 20 (23%)
- State-sponsored: 13 (15%)
- Individual actor: 6 (7%)
ENISA Threat Landscape: Transport Sector
Findings

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

- State-sponsored attackers: politically motivated attacks targeting ports and vessels
  - Spoofing of the automatic identification system by a hostile state

- Cyber criminals: Ransomware, malware and phishing / spear-phishing attacks targeting:
  - port authorities,
  - port operators or
  - manufacturers (supply chain)

- Major disruptions in ports where we lack information on what type of attack took place (South Africa 2021, Northern EU oil hubs 2022).
### Findings

- **IT systems being targeted** (passenger services, ticketing systems, mobile application, display boards, etc.): disruptions due to the unavailability of IT services.

- **Notable data thefts**

- **OT systems and networks affected**:
  - Only when entire networks were down or when safety-critical IT systems were unavailable, e.g. service disruptions to the a train operator due to an attack on one of its ICT service providers (DDoS attack).

- **DDoS attacks on the rise in 2022**, reaching one fifth of the attacks on the railway sector (20%).
  - Hacktivists launching ransomware attack.
Findings

- Ransomware has targeted the automotive industry, in particular OEMs and tier-X suppliers. In some cases, the production of vehicles or parts had to stop due to an attack.
- Notable cases of proprietary information being stolen or leaked from OEMs and tier-X suppliers.
- Data-related threats primarily targeted IT systems in an effort to acquire customer or employee data and proprietary information.
The estimated median direct cost of a major security incident is EUR 225 000.
FINDINGS & ASSESSMENT

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

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

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

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

Majority of attacks to the transport sector target IT systems

- They can result in operational disruptions.

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

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

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

Agamemnonos 14, Chalandri 15231
Attiki, Greece

☎
✉ etl@enisa.europa.eu
🌐 www.enisa.europa.eu