The Transportation sector cyber threat overview

blog.sekoia.io/the-transportation-sector-cyber-threat-overview/

12 September 2023

Log in

Whoops! You have to login to access the Reading Center functionalities!

Forgot password?

Maxime A., Livia Tibirna and TDR (Threat Detection & Research) September 12 2023
666 0

Read it later Remove

15 minutes reading

This report aims at contextualising cyber activities targeting the transportation sector worldwide over the 2022 – 2023 period. This report is based on open source reporting and Sekoia.io observations of campaigns mostly impacting the road, air and rail transportation.

Introduction

The increasingly digitised and connected transportation sector faces a broad range of threats,
including in cyberspace. Organisations operating in the transportation sector are a prime target
The increasingly digitised and connected transportation sector faces a broad range of threats, including in cyberspace. Organisations operating in the transportation sector are a prime target for cyberattacks, due to the critical role of the transportation infrastructure for the physical connectivity and for the functioning of the economic systems within a territory. Indeed, interrupted transportation operations may have potentially significant impact on other verticals, *e.g.* **impacts on the supply chain** management. In addition, transportation operators process **personally identifiable information (PII)**, exposing them to the risk of surveillance. Additionally, some actors – national air and rail companies – are **perceived as a symbol for politically-motivated attackers** aiming at attempting the image of the originating state.

Over the past years, the transportation sector was subject to evolving cyber security regulations to improve the overall level of security, including cybersecurity. One of the latest evolutions was the adoption, in late 2022, of the NIS2 Directive aiming at strengthening the

cybersecurity level across the European Union, including the transportation and other essential sectors.

A sector highly impacted by lucrative-oriented cyber criminal threat

Lucrative-oriented cybercrime is a major threat increasingly impacting companies worldwide, including the transportation sector. Over the last two years, the sector faced an ever evolving and **progressively advanced cybercrime ecosystem**, dominated by the ransomware threat (38% of all the threats identified by ENISA within the EU). Sekoia.io assess that most financially-motivated campaigns impacting the transportation sector are **opportunistic** and are primarily intended to maximise attackers' gain by compromising victims' **data integrity**.

Ransomware and extortion campaigns

Based on Sekoia.io observations, the **ransomware-related threat steadily intensified** over the past years, both measured in the number of reported incidents and their estimated impact, and the diversification of intrusion set's nature and techniques. The **transportation sector** was **increasingly impacted** by ransomware and extortion campaigns (hitting a 186% increase between January and June 2021 according to CheckPoint and remaining in the Top 5 impacted sectors as reported by NTT Security in May 2023), reflecting similar trends observed across many sectors.

In recent years, the large majority of ransomware groups known to target corporate assets were reported conducting campaigns against the transportation sector. Reported victimology notably includes a double extortion campaign targeting Wabtec, a U.S. product and services provider for the rail and transit industry, claimed by the LockBit intrusion set in mid-2022. The same group claimed a ransomware operation against Port of Lisbon in early 2023, as well as an attack against the Romanian Association for International Road Transport (ARTRI) in April 2023. A campaign impacting Japan's biggest port, the Port of Nagoya, was also reported in July 2023. The ransomware attack, claimed by the LockBit ransomware group, targeted Nagoya Port's central container operations handling system and resulted in disrupted container operations across all terminals within the port for two days. The attack also raised concerns over its potential **impact on the local economy**, as the port handles 10% of Japan's total trade volume, and on **global supply chains** including the auto industry. Sekoia.io did not observe a specific country-level targeting and assess the geography of reported ransomware attacks against the transportation sector is mostly arbitrary.

Based on open source reporting, a significant number of successful ransomware attacks resulted in **data compromise** (encryption, theft, exposure to unauthorised users, leakage, non availability and loss). Other impacts were reported, such as financial loss, loss of operational continuity (canceled and delayed operations), reputation damage, web services unavailability.

Sekoia.io assess the **most immediate ransomware threat** impacting the transportation sector in the 2022-early 2023 period was **Ransomware-as-a-Service (RaaS) leveraging the double extortion technique.** Most of the known RaaS operators – such as LockBit, BlackCat, BlackByte and Black Basta – were reported targeting the transportation sector over the last two years. Reported lucrative campaigns implied urging the victims to pay a ransom, selling the exfiltrated data, or exploiting it for further lucrative operations such as fraud.

During the first half of 2023, the transportation sector faced the growing trend of multiple opportunistic intrusion sets actively exploiting **0-day vulnerabilities** to deploy ransomware and/or exfiltrate data. One such example is the massive exploitation of the CVE-2023-34362 zero-day vulnerability found in the MOVEit file transfer solution in late May 2023. In early June 2023, British Airways, the largest airline based in the United Kingdom, and Transport for London, the London public transport operator, reported incidents involving the MOVEit vulnerability. The exploitation was subsequently attributed to intrusion sets associated with the TA505 group, resulting in **extortion campaigns** and **confidential data exposure**.

The MOVEit campaign mirrors a common trend among ransomware intrusion sets observed by Sekoia.io, which is the **mass adoption of the exfiltration-based extortion technique**, increasingly avoiding encryption. One such example is the BianLian intrusion set, reported to shift from the double-extortion model to primarily exfiltration-based extortion technique in January 2023, which continuously claims data extortion attacks impacting most verticals, including the transportation sector ([1], [2], [3]). Sekoia.io assess with high confidence that **lucrative intrusion sets will increasingly adopt the data extortion technique**, mainly resulting in reputation damage and data integrity compromise.

Credential theft campaigns

Phishing campaigns are a common attack vector for initial access in reported campaigns impacting the transportation sector. Phishing attacks are regularly followed by **further compromises** such as ransomware attacks, fraud, data theft and extortion campaigns. While **most of the observed** mass phishing **campaigns** are **opportunistic**, they are commonly **tailored** to the particular context of the **victim's activities**, as well as to major events related to the victim's industry.

For instance, based on Kaspersky observation, from early 2022, the transportation sector was subject to spam mailing campaigns leveraging the economic sanctions due to the Russo-Ukrainian conflict, highly likely to conduct fraud campaigns via spear phishing links. In May 2023, an emerging malware called FluHorse was leveraged in phishing campaigns impacting Android users of a major transportation application in Eastern Asia and of an Electronic Toll Collection (ETC) application in Taiwan. In reported campaigns, FluHorse mimics legitimate transportation applications and aims at gathering the victims' credentials, credit card data and Two-Factor Authentication (2FA) codes.

Credentials and other sensitive information obtained from phishing campaigns are either directly leveraged by the same attackers or **sold to other financially-motivated threat actors**. During our cybercrime forums monitoring routine, Sekoia.io observes a significant number of publications leaking sensitive data or selling credentials for remote access services to corporate networks within the transportation vertical. While this illicit market evolves towards specialisation and professionalisation, most threat actors observed by Sekoia.io persist in opportunistic targeting.

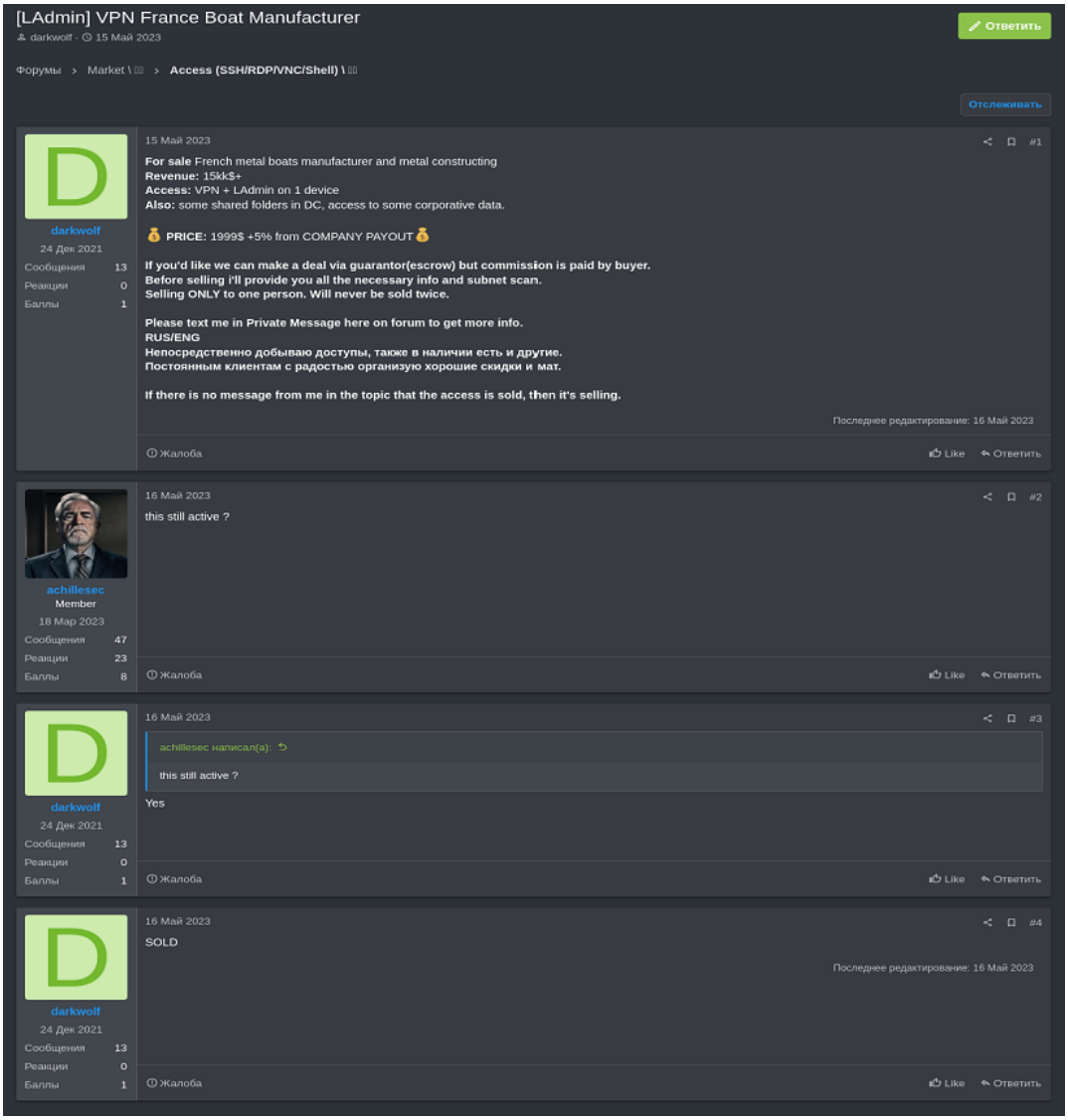

Figure 1. A threat actor selling an unauthorized VPN access to a French boat manufacturer's internal networks (Source: RAMP cybercrime forum)

Opportunistic disruption operations led by nationalist hacktivist groups

Since the beginning of the Russian invasion of Ukraine in February 2022, Sekoia.io observed a **significant increase regarding the activity of nationalist hacktivist groups.** Those groups usually use cybercriminal techniques, tactics and procedures (TTPs) but differ from cybercrime activities regarding their motivations, responding to geopolitical rather than lucrative goals. Hacktivist groups are known to carry out Distributed denial of service (DDoS) attacks and DDoS-related activities, defacement, hack-and-leak operations and extortion campaigns that hide a disruption goal. Such targeting often impacts the transportation sector, as many entities such as **airlines or national rail services** represent an **opportunistic and symbolic objective** to undermine foreign states. Since February 2022, multiple NHG claimed cyber operations which aimed at contributing to the narrative of the side they belong. On the Russian side, mainly targeting Ukraine and NATO entities, **Killnet**, **NoName057**, **Anonymous Sudan** – an assessed false flag hacktivist group directly related to Killnet – were the most active.

Cyber and kinetic disruption

In the 2022-2023 period, the transportation sector was particularly impacted by **DDoS operations** claimed by the aforementioned groups. In March 2023, Sekoia.io observed Anonymous Sudan carrying out successive DDoS campaigns over French entities, including airports and French airlines AirFrance, Transavia and FlyingBlue. Over the same period, NoName057 leveraged their participative DDoS tool named DDOSIA to impact websites from entities in NATO countries, among them French rail transportation companies were particularly targeted (Paris transports RATP, national rail service SNCF). In June 2023, shortly after French president Macron announced the incoming delivery of an air defense system to Kiev, Sekoia.io detected multiple targets related to the French transport group RATP. Sekoia.io assess with high confidence **those targets represent an opportunistic way for the attackers to mediatise cyber operations impacting countries supporting Ukraine** against the Russian invasion.

Similar operations were observed to be conducted by pro-Russia hacktivist groups supporting Ukraine. For instance, in January 2022, the Belarusian Cyber Partisans, a group opposed to the Moscow-aligned Belarus government, conducted a ransomware attack on Belarusian Railway information systems. The campaign aimed at **denouncing** the involvement of the Belarusian President in the Russian military operation against Ukraine, and **delaying the deployment** of the Russian **military troops** near Ukraine using the Belarusian Railways' system. The ransom asked by the Belarusian Cyber Partisans was the release of 50 political prisoners and the withdrawal of Russian troops, instead of money. No open source information is available whether that operation impacted Belarusian military troop transportation.

Ransom DDoS attacks (RDDoS)

Ransom Distributed Denial of Service (RDDoS) attacks are a form of cyber malicious campaign aiming at performing distributed denial of service until a ransom fee is paid. This **extortion-based** technique is mostly leveraged to escalate the impact of an ongoing campaign and force the victim to pay the ransom.

While the transportation sector was impacted by denial of service attacks over the last years, a less widespread RDDoS attack was reported targeting the Swedish aviation industry in early 2023. In February 2023, the Russia-aligned hacktivist group Anonymous Sudan announced a massive **politically-motivated DDoS campaign** against the Swedish airport infrastructure, an initiative joined later by the UserSec group. Later, Anonymous Sudan expanded this DDoS campaign to other Scandinavian air transportation entities, leveraging the **RDDoS** technique against Scandinavian Airlines and Northern Europe's leading airline, asking for a $3,500, then $3M and later $10M ransom. Impacts such as website and application unavailability, as well as passengers' data exposure were reported by the victim, which is a relatively unusual behaviour for a hacktivist group usually focused on website accessibility disruption.

Sekoia.io assess it is likely Anonymous Sudan, alongside with other Russia-aligned hacktivist nationalist groups operations, conducted a **fake extortion campaign** with an overstated ransom demand to amplify their operation aiming at undermining Sweden, currently awaiting NATO integration.

Anonymous Sudan ties with Russia-aligned hacktivist groups

Anonymous Sudan emerged in January 2023 with the "OpSweden", a DDoS campaign against Sweden in reaction of an mediatised anti-muslim act conducted by a swedish right-wing activist. However, evidence shows a strong possibility that Anonymous Sudan is a sub-group of the pro-Russian hacktivist group Killnet, a group with which Anonymous Sudan has publicly aligned itself since March 2023.

A bit of context is needed to understand the self designated Anonymous Sudan group. In May 2022, following the Russian invasion of Ukraine, Finland and Sweden applied to join NATO. Turkey, as a NATO member, voiced its opposition to include Sweden arguing Stockholm was helpling Kurdish organizations Ankara considers terrorist. Diplomatic negotiation went by to find a consensus.

Sekoia.io assess with confidence that in January 2023, when the swedish right-wing activist committed the mediatised anti-muslim act, Russian nationalist hacktivist groups such as **Killnet** identified an **opportunity to undermine Swedish-Turkish negotiation** on an islamophobic pretext, as Turkish president Erdogan often reacts on this subject. Killnet either created Anonymous Sudan or helped a preexisting unskilled group, to conduct and mediatise proxy DDoS operations on Sweden and later other NATO countries, to impact states that support Ukraine.

Figure 2. Anonymous Sudan announcement of DDoS campaign targeting the Swedish aviation industry (Source: Anonymous Sudan Telegram channel) – 07/02/2023

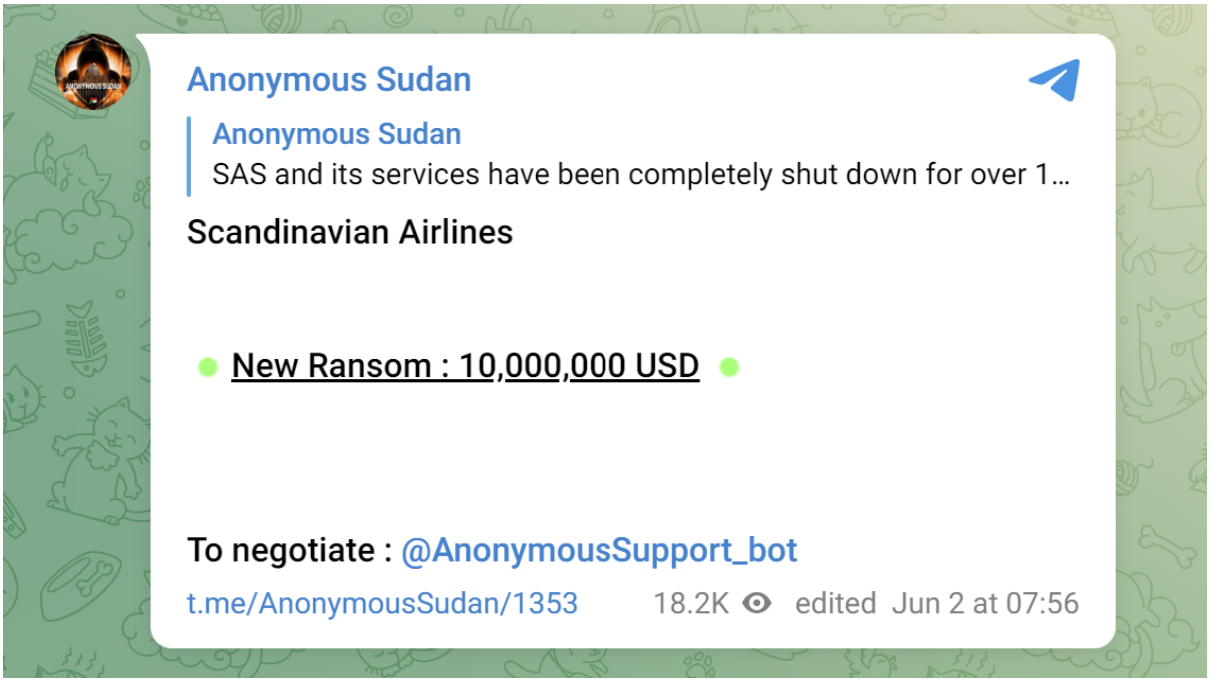

Figure 3. Anonymous Sudan announcement of RDDoS campaign targeting Scandinavian Airlines (Source: Anonymous Sudan Telegram channel) – 02/06/2023

A transportation sector less reported as impacted by State-nexus intrusion sets

Transportation sector is also a target for state-aligned cyber offensive operations both **as a final target for industrial espionage**, and **as a medium** to conduct **espionage operations and kinetic disruption**. However, as few details (detailed victimology, assessed impact) are usually available in open-source reporting state-nexus cyber operations on the transportation sector, it is difficult to be exhaustive on this aspect of the cyber threat.

Given the criticality of the transportation sector, as the energy, in high intensity conflicts, most exemple in this section are related to the Russia-Ukraine war. Is it due to the overrepresentation of cyber operations related to the conflict reported in open source. Off note, transportation entities unrelated to the Russia-Ukraine conflict can still be targeted by state-nexus cyber threats.

Road and rail logistics disruption

Various entities, private companies, operators, NGOs and state administrations operating in the transportation vertical can be targeted by cyber operations in order to **disrupt the provided service**, and potentially, conduct **strategic espionage on the transported assets.**

Since the beginning of the Russian invasion of Ukraine in February 2022, multiple Russian-nexus intrusion sets (Calisto, Gamaredon, Sandworm) were reported to target Ukraine-based and NATO transportation and logistic companies. For instance in March 2023, Russian military GRU-associated **Sandworm** was observed by Microsoft conducting a destructive attack on the network of an undisclosed logistic provider headquartered in Western Ukraine. Technical investigation allowed Sekoia.io to detect similar targeting conducted by FSB-associated **Calisto** intrusion set, which carried out phishing campaigns aiming at credential theft on logistics companies such as *DTGruelle* and *Emcompass*, both involved in support to Ukraine war support.

Other operations were reported in open-source, impacting national transportation sectors. In July 2021, Iranian authorities reported cyber attacks impacting Iranian Railways and the Ministry of Roads and Urban Development information systems. The operation was claimed by the anti-Iranian regime hacktivist group Indra, a group that Tehran accuses of being helped by Israel, likely to undermine the government and favor a popular uprising.

Plausible prepositioning operations

Other state-nexus operations were reported impacting transportation and logistics companies, such as Israeli maritime and road shipping firms targeted by Iran-associated **TortoiseShell**, anintrusion set observed by ClearSky setting up watering hole attacks on at least eight Israeli companies in May 2023. Although it is difficult to assess the intention of such operations due to the absence of intrusion details in open source reporting, the **transportation sector, as a strategic asset for a state security and economic stability**,

is likely a target for prepositioning operations where the intrusion is conducted to be the more covert possible, allowing future actions on objective (espionage, sabotage or both). Another example is the China-associated TIANWU intrusion set, observed in december 2021 by TeamT5 leveraging the malware Pangolin8Rat to target a **Taiwanese rail-transportation company**, an operation we can assess as plausibly linked to Chinese efforts to preposition in the event of Taiwan annexion conflict. **Aerospace companies can be targeted** as wellfor alleged prepositioning operations. In February 2022 the KA-SAT satellite communication modems, operated by VIA-SAT company, were impacted by Russia-nexus **Sandworm**, launching a destructive command on a likely prepositioned compromise, to disrupt Ukrainian army communications.

Technology and industrial espionage

The transportation sector, involving high technology, is a target for industrial cyber espionage. The threat is particularly relevant pertaining to the civil aerospace industry, especially **airliner manufacturers** due to the research and development investments. China-associated intrusion sets such as LanceFly, APT41, Winnti and Mustang Panda are often reported by different cybersecurity vendors as groups involved in industrial cyber espionage, notably focusing on aerospace companies. APT41, an intrusion set associated to the Chinese Ministry of State Security, was indeed observed by TrendMicro in March 2022 using a custom Cobalt Strike loader to target a Taiwanese aviation company, a focus coherent with Symantec and Recorded Future analysis on LanceFly victimology, an intrusion set which technically overlaps [1] APT41.

Surveillance and individuals espionage

When operated by intelligence services, State-nexus intrusion sets can **target transportation companies to gather information about individuals**. A similar operation was observed by IBM Security in March 2021 documenting the Iran-nexus MuddyWater group, associated with the Ministry of Intelligence of the Islamic Republic of Iran (MOIS), conducting an espionage operation against an Asian airline. The files found on the MuddyWater command and control (C2) server suggested possible access to reservation data. Similar indirect targeting for individual espionage was later used by another Iran-nexus intrusion set, Cuboid Sandstorm. The group, assessed to be associated with the intelligence service of the Islamic Revolutionary Guard Corps (IRGC), was observed by Microsoft in May 2023 impacting Albania hotels, likely to gather information on individuals linked to an Iranian dissident organization.

Conclusion

The transportation sector is a regular target for financially-motivated actors, notably ransomware groups conducting double extortion campaigns. While cybercrime intrusion sets can leverage the criticality of the transportation infrastructure to extort victims, Sekoia.io assess with high confidence that **most lucrative campaigns impacting the transportation sector are opportunistic**.

Sekoia.io assess **Russia-aligned hacktivist threat impacting transportation entities located in Europe will likely pursue**, exploiting political opportunity to conduct mainly **DDoS operations** to impact any countries involved in Ukraine support. To a lesser extent, targeting airline companies could be interpreted as a retaliation for abandoning their operations in Russia in response to the Russo-Ukrainian war.

Sekoia.io assess is it likely that entities associated with **the transportation sector will continue to be a target for State-nexus intrusion sets** aiming at disrupting logistics —especially those implied in Ukraine war support —, performing industrial espionage and individuals' surveillance.

External references :

[1] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor, accessed September 12, 2023

Thank you for reading this blogpost. We welcome any reaction, feedback or critics about this analysis. Please contact us on tdr[at]sekoia.io

Feel free to read other TDR analysis here :

Comments are closed.