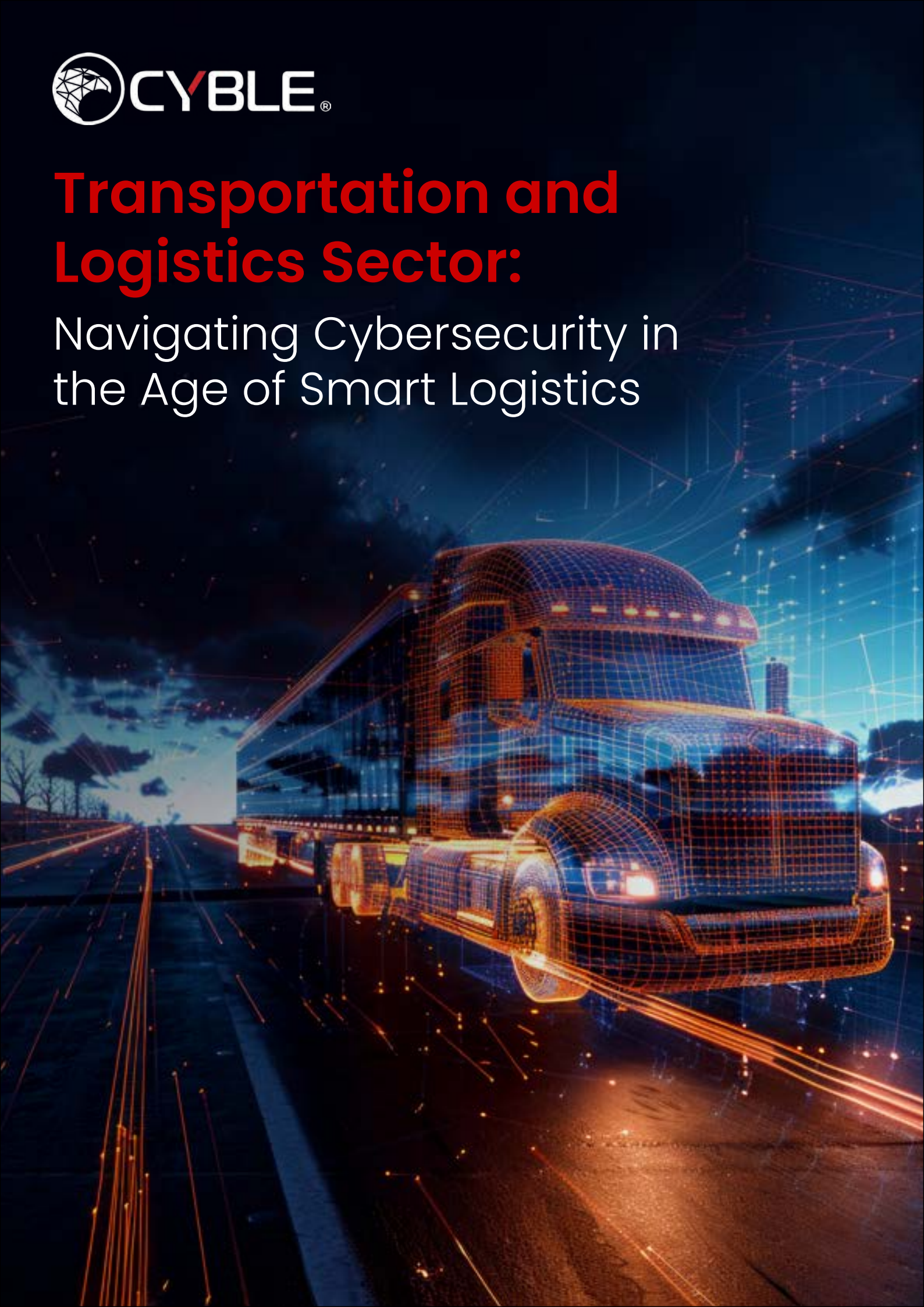
CYBLE®

Transportation and Logistics Sector:

Navigating Cybersecurity in the Age of Smart Logistics



CONTENTS

EXECUTIVE SUMMARY

The Transportation and logistics industry plays a pivotal role as the foundation of global commerce. It is the lifeblood of international trade, serving as the essential conduit for the movement of goods and services, enabling the seamless flow of products across borders and driving economic activity.

As the world becomes increasingly interconnected, the efficiency and reliability of these transport networks are more crucial than ever, underpinning the growth and stability of the global economy.

In 2024, the transportation and logistics sector faces a complex threat landscape characterized by a convergence of cybersecurity risks, economic uncertainties, geopolitical tensions, regulatory pressures, and the ongoing evolution of smart technologies.

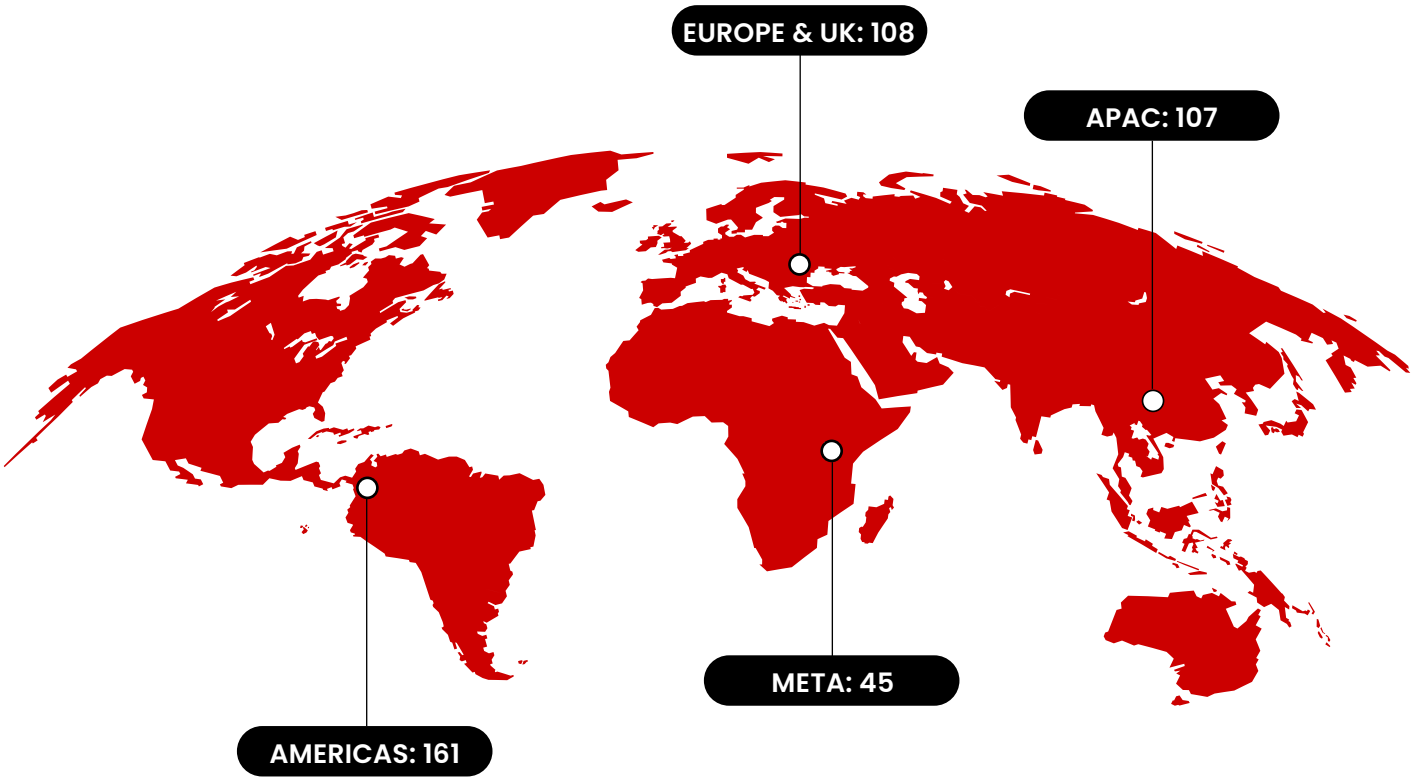
The logistics sector is undergoing rapid digital transformation, driven by advancements in technologies such as the Internet of Things (IoT), artificial intelligence (AI), and automation. These innovations promise to enhance operational efficiency and sustainability. However, they also introduce new vulnerabilities that must be managed carefully to mitigate cyber threats and operational disruptions.

SHADOWS OF GEOPOLITICAL RISKS

Ongoing geopolitical conflicts have not just raised global security concerns but have stretched the trade routes and enhanced supply chain complexities in several industries. Transportation & Logistics, being the pivotal point of all sectors, is increasingly facing far more challenges in keeping up the pace with emerging uncertainties. The recent attacks on container vessels in the Red Sea exemplify the ongoing risks in Maritime logistics, which can lead to significant fluctuations in shipping rates and operational delays.

The threat of geopolitical escalations in the Middle East and the ongoing conflict are already burdening the Aviation sector and businesses due to increased freight costs. The volatile situation in the South China Sea and everyday skirmishes are compelling businesses to diversify their supply chains to mitigate the risks associated with specific regions or routes.

Thus, there is a growing emphasis on resilience and flexibility, with businesses investing in technology and infrastructure to ensure continuity in the face of disruptions. Additionally, the industry is seeing a shift towards regionalization as companies seek to shorten supply chains and reduce dependency on global trade routes.



Global Impact of Ransomware & Data Breaches on Transportation Sector

EMERGING CYBERSECURITY RISKS

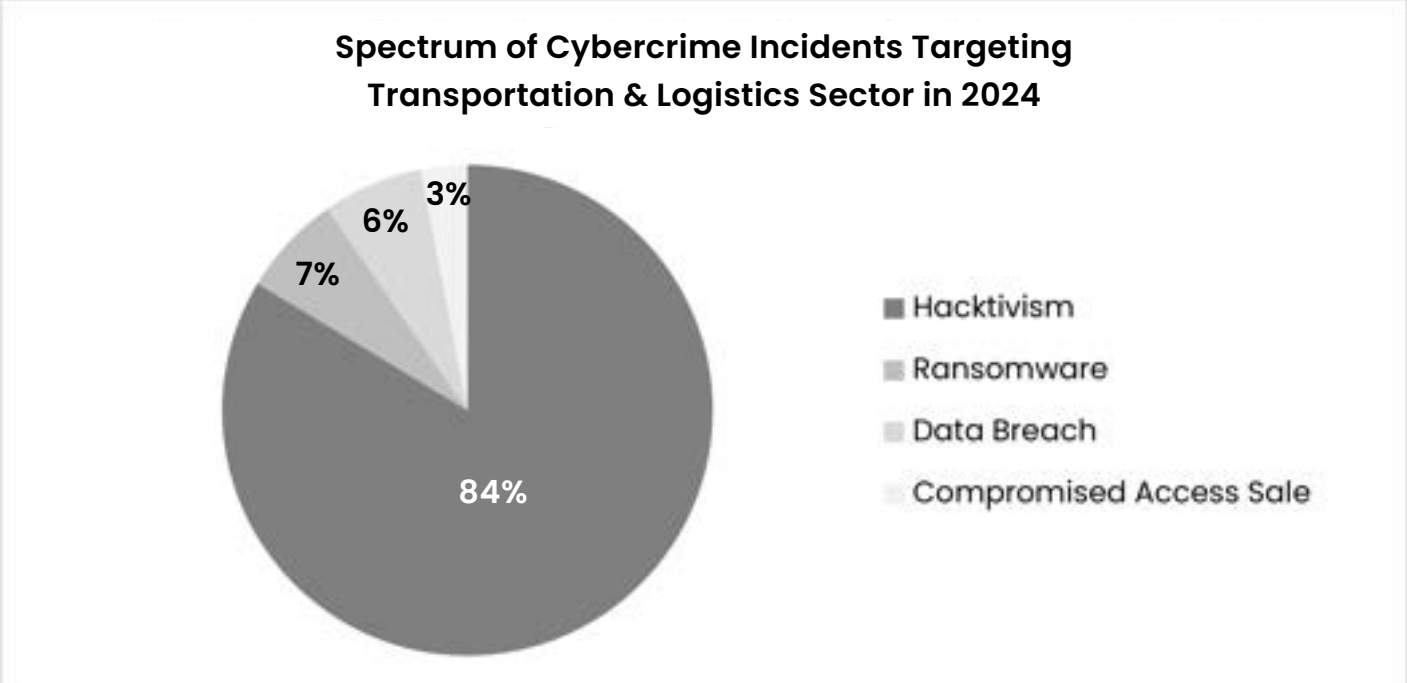
The Transportation & Logistics sector is facing myriad cybersecurity threats in 2024, driven by increased digitalization, interconnected systems, and evolving criminal tactics.

The quantum of threat posed by Ransomware operators is undeniable and remains the primary concern for the sector. Cyble Research & Intelligence Labs (CRIL) observed a marginal increase in ransomware attacks from 120 in 2023 to 122 so far in 2024.

However, due to abrupt global dynamics, a wave of cyber activism has begun to pose new challenges for the Transportation and logistics industry. The involvement of state-sponsored actors and the blending of hacktivism with organized cybercrime have raised the stakes. The hacktivism incidents targeting the sector increased phenomenally by 27 percent, from 1200 incidents captured in 2023 to 1529 incidents analyzed by CRIL in 2024.

Further, there is a significant uptick in the number of data leaks and sales of compromised data incidents. CRIL observed an alarming increase of 128 percent to 122 data breach incidents recorded from the underground forums compared to 2023.

The magnitude of the threat was further heightened in 2024; CRIL recorded a 45 percent increase in threat activities on cybercrime forums related to the sale of compromised access to IT systems widely employed by the Transportation and logistics sector.



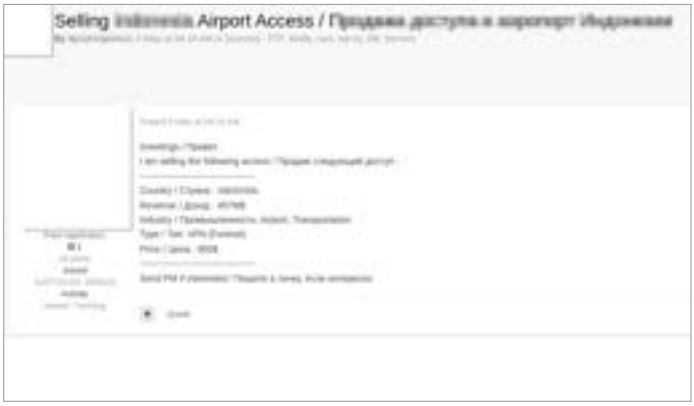
EMERGING CYBERSECURITY RISKS

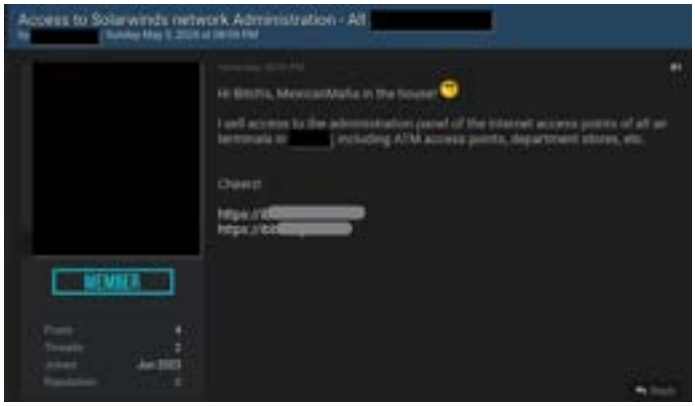
CREDENTIAL THEFT

Compromised credentials remain a major initial vector leveraged by cybercriminals for infiltrating an organization's network. In many a case, threat actors obtain these credentials from dark web repositories of stealer malwares, mostly sold in marketplaces and dumped across Telegram channels. In other cases, threat actors are able to exploit recently emerged vulnerabilities and exposed internet instances of web panels to gain illicit access and then sell them in the underground forums. These are often bought by ransomware groups and state and non-state actors to infiltrate an organization's network, escalate their privileges, maintain persistence, encrypt and steal sensitive information, or mount supply-chain attacks on associated third parties.

The threat actors were observed to be manipulating and selling accesses to compromised Remote Desk Protocol (RDP) servers of Citrix Gateway, access to VPN, Firewall, Active Directories, e-commerce platforms employed by Airlines, and SolarWinds Network Performance Monitor (NPM). CRIL observed that threat actors, in some cases, were also able to gain illicit access to logistics management systems and fleet management systems.

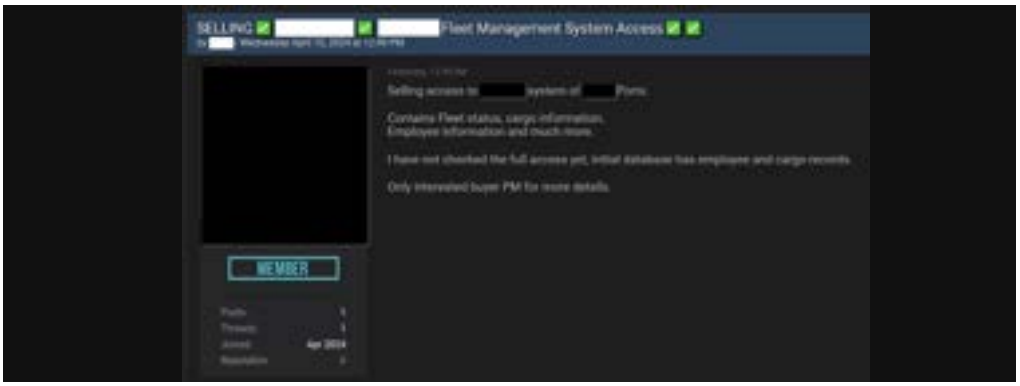
EMERGING CYBERSECURITY RISKS





In one such instance, a threat actor was observed selling unauthorized access to a Logistics Management System (LMS) for USD 50,000. The TA claimed that the compromised portal provides real-time insight and control over ships and cargo, control of ports for ships and cargo in the Danube River, view of cargo goods information, and control of customs checks between countries.

A threat actor was observed selling access to a port operator and logistics company's fleet management system (FMS). This compromised FMS allegedly contained employee and cargo records and allowed the attacker to check the fleet status and cargo movements.



EMERGING CYBERSECURITY RISKS

DATA BREACHES

The Transportation and Logistics sector faces multifaceted threats from data breaches that extend beyond immediate financial losses to long-term operational disruptions and reputational harm. Under the reverberation of global turmoil, cybercriminals were observed targeting Transportation and Logistics companies to disrupt international trade and create chaos.

Further, due to the interconnected nature of modern supply chains, data breaches can have cascading such as tracking and monitoring of goods in transit, leading to potential losses or mismanagement of shipments. This is particularly critical for sectors like healthcare and food supply chains where timely delivery is essential.

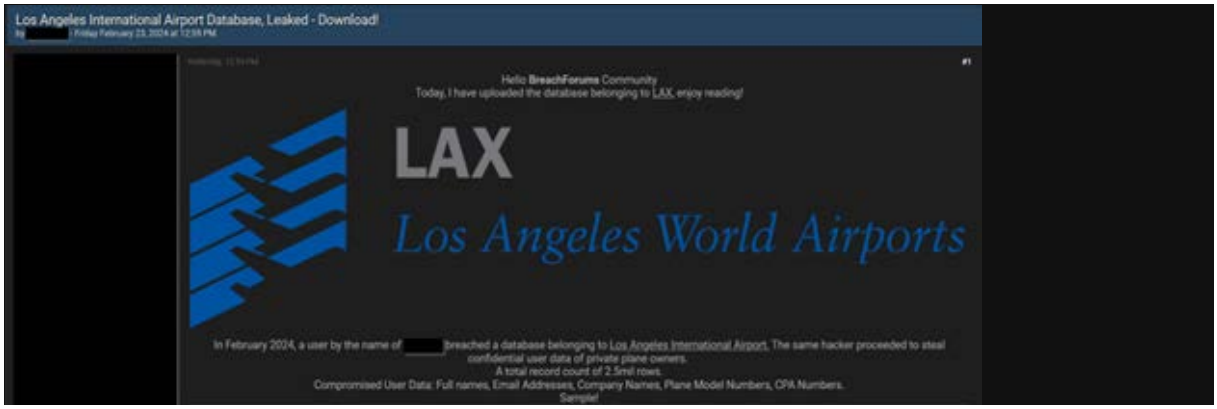
A threat actor was observed selling 846 GB (uncompressed) of compromised data of an Australian company containing information about customers, agents, freights, sales, and accounting. As proof of compromise, the TA further provided sample records that included SMS logs, trading accounts, driver details, and dispatch information for the freights.

Another incident observed on an underground forum about a data leak from an Indonesian courier service contained 1.84 million records of its users revealing their addresses, phone numbers, and recipient details. Cybercriminals can utilize such data to impersonate company officials and run smishing/phishing campaigns to deceive them into divulging additional personal information or inadvertently conducting financial fraud.

EMERGING CYBERSECURITY RISKS

An incident allegedly impacting the Florida Department of Transportation (FDOT) led to the theft of 160,000 records by a threat actor in August 2024. These records allegedly contained sensitive information about finances, contracts, and vendor details, including identifiers, names, dates, prices, and other user information.

In an alleged cyberattack on the Los Angeles International Airport network, threat actors stole and leaked 2.5 million rows containing information about private aircraft owners' full names, email addresses, company names, plane model numbers, and CPA numbers.

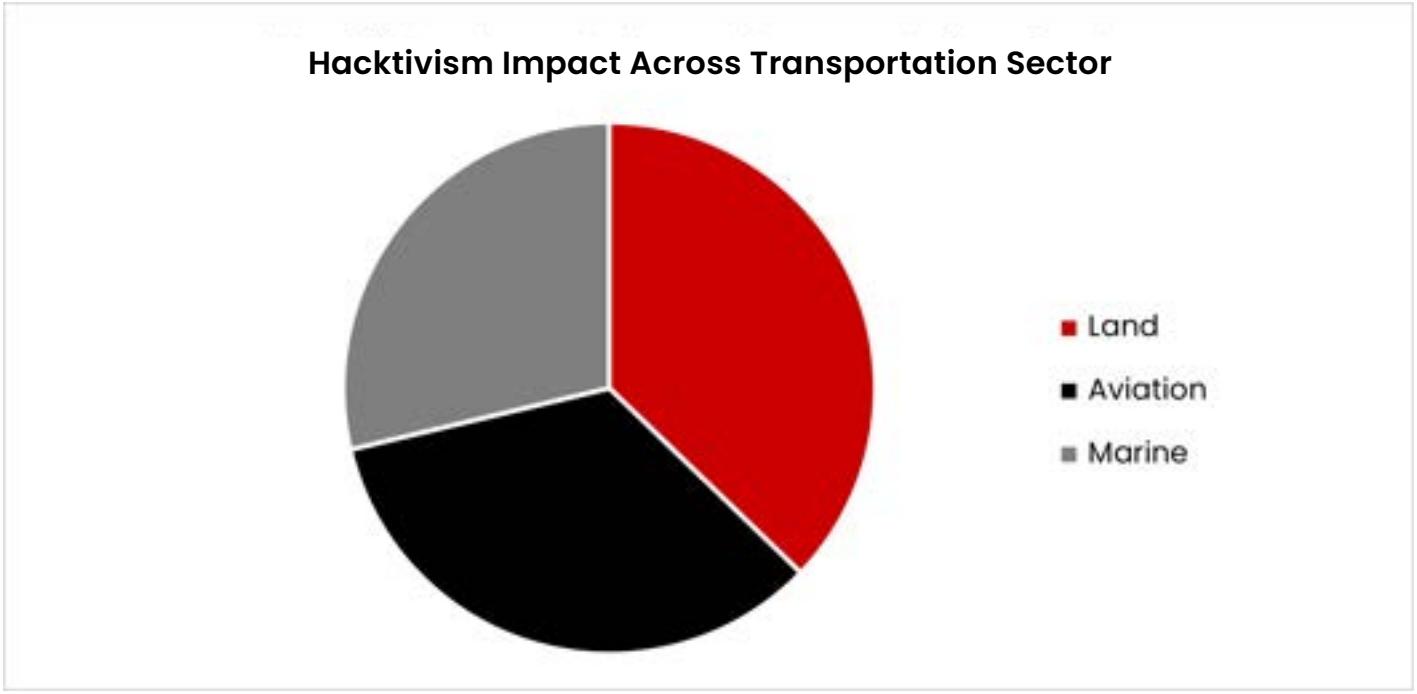


EMERGING CYBERSECURITY RISKS

HACKTIVISM

These conflicts have catalyzed a global response, with hacktivist groups from various countries joining the fray. There is a noticeable shift towards more organized and collaborative efforts among hacktivist groups. Many have adopted a quasi-recruitment approach, training individuals to act during conflicts akin to sleeper cells in traditional warfare. They have been democratizing access to hacking capabilities and promoting the use of cheap Ransomware services to maximize the impact.

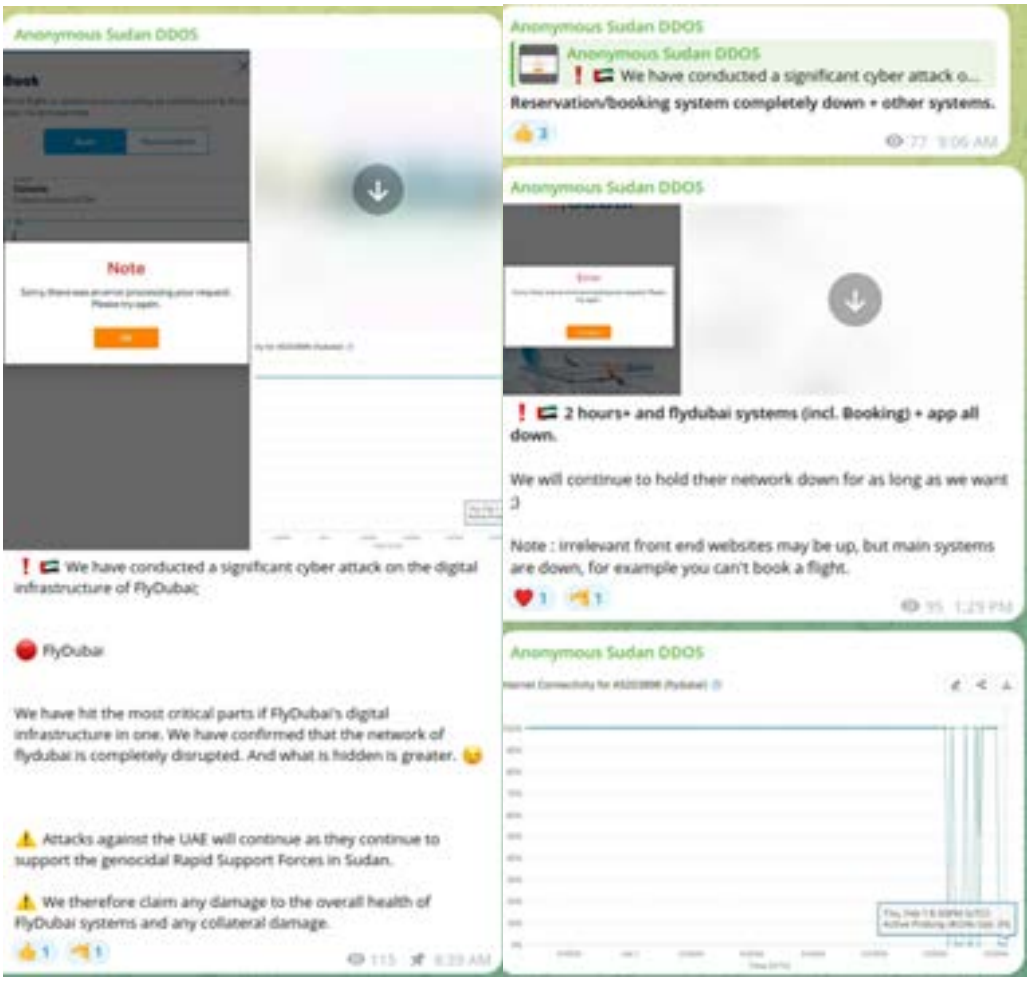
The hacktivist attacks observed by CRIL, as indicated below, indicate the distribution across the three major categories of the Transportation & Logistics Sector.



EMERGING CYBERSECURITY RISKS

Distributed Denial-of-Service (DDoS) attacks have long been a favored cyber-activist tactic employed by hacktivist groups. However, in recent times, these attacks have become increasingly overwhelming, often disrupting online booking systems, shipment tracking applications, and communication channels between various stakeholders in the supply chain. The financial implications of DDoS attacks can be staggering. Companies may incur costs related to downtime, recovery efforts, and potential loss of business due to customer dissatisfaction.

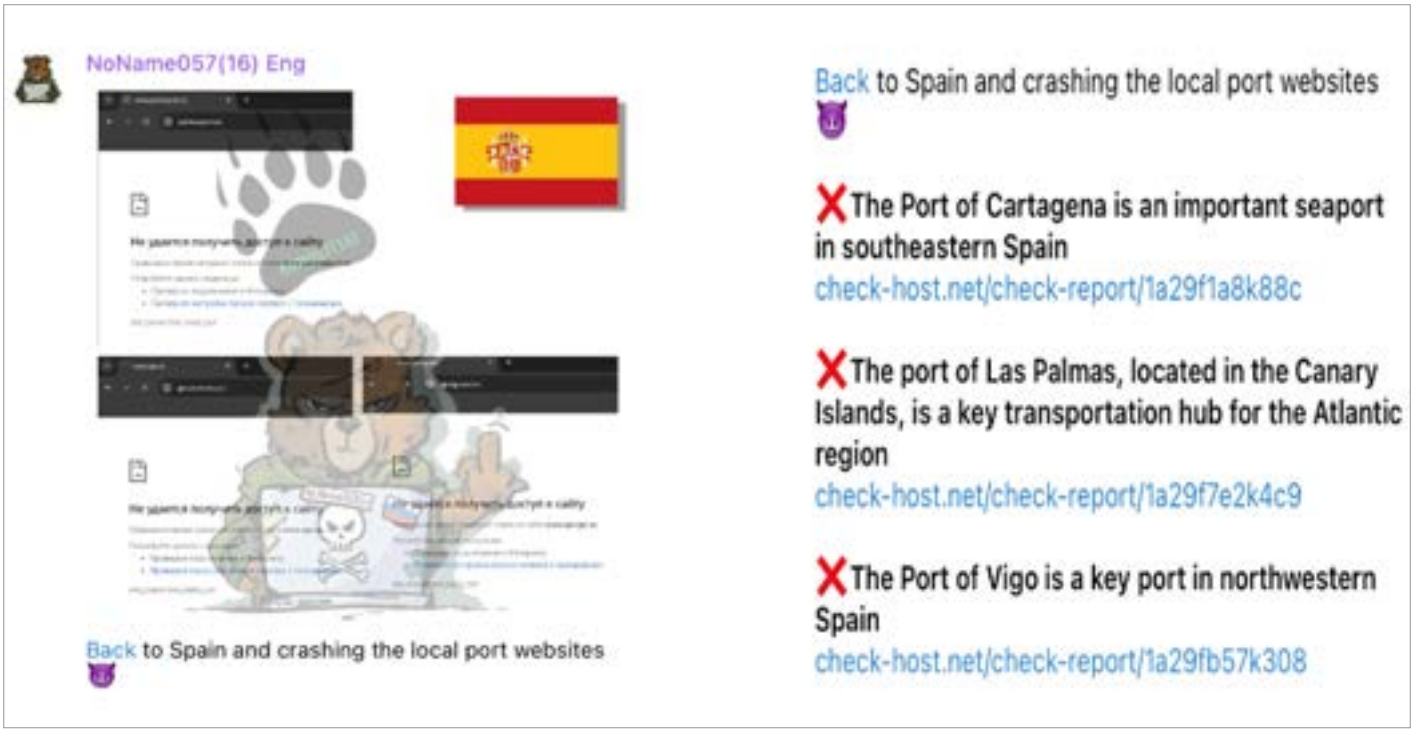
A notable example is the hacktivist group Anonymous Sudan, which launched an extensive and sustained attack on the networks of UAE-state-owned carriers Flydubai. The group claimed to target the entire digital infrastructure, including reservation systems and their mobile application. The group claimed to have been executing the attack for over six hours and continued to overwhelm their servers. Anonymous Sudan alleged these attacks due to their perception of UAE supporting the rebel Rapid Support Forces in Sudan.



EMERGING CYBERSECURITY RISKS

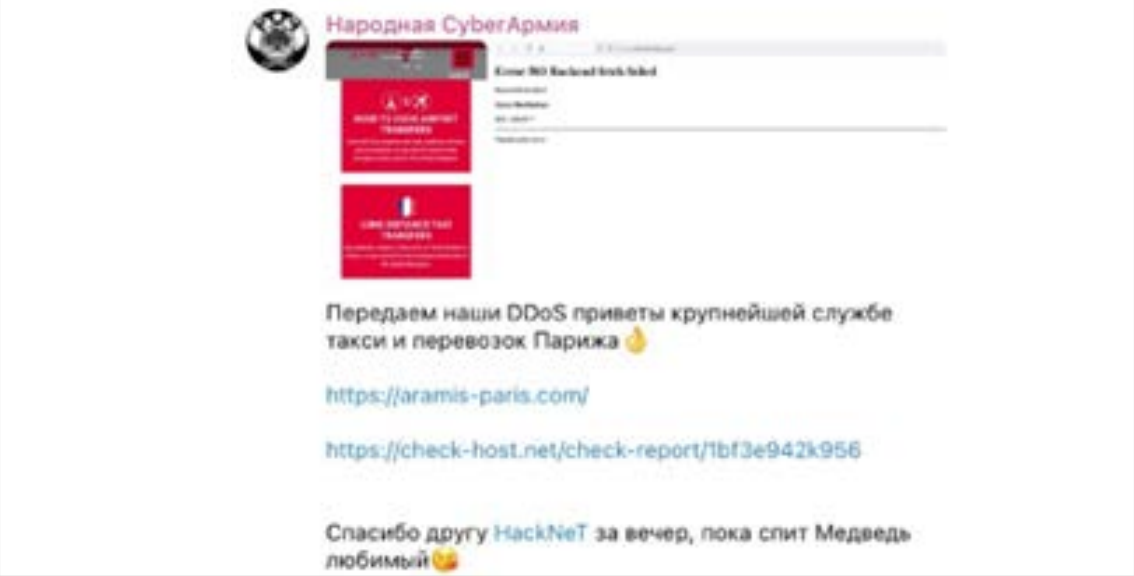
Amongst some of the unsettling hacktivism incidents impacting critical infrastructures associated with the Transportation & Logistics sector due to the ongoing Russia-Ukraine conflict, pro-Russian hacktivist groups such as NoName057(16), People's Cyber Army, HackNett, CyberDragon, and others have continuously launched coordinated attacks on airports, marine ports, and other public transportation systems.

In one such incident in May 2024, NoName057(16) targeted major Spanish ports, including the Port of Cartagena, the Port of Las Palmas, and the Port of Vigo.



Correspondingly, events of international significance, like the Paris Olympics 2024 and the European Elections, have also sparked a row of cyber protests. In a coordinated cyber offensive, the pro-Russian hacktivist group People's Cyber Army launched DDoS attacks on French taxi services Aramis in retaliation to the International Olympic Committee's (IOC) sanctions barring Russian athletes from participating in the Olympics under their national flag.

EMERGING CYBERSECURITY RISKS



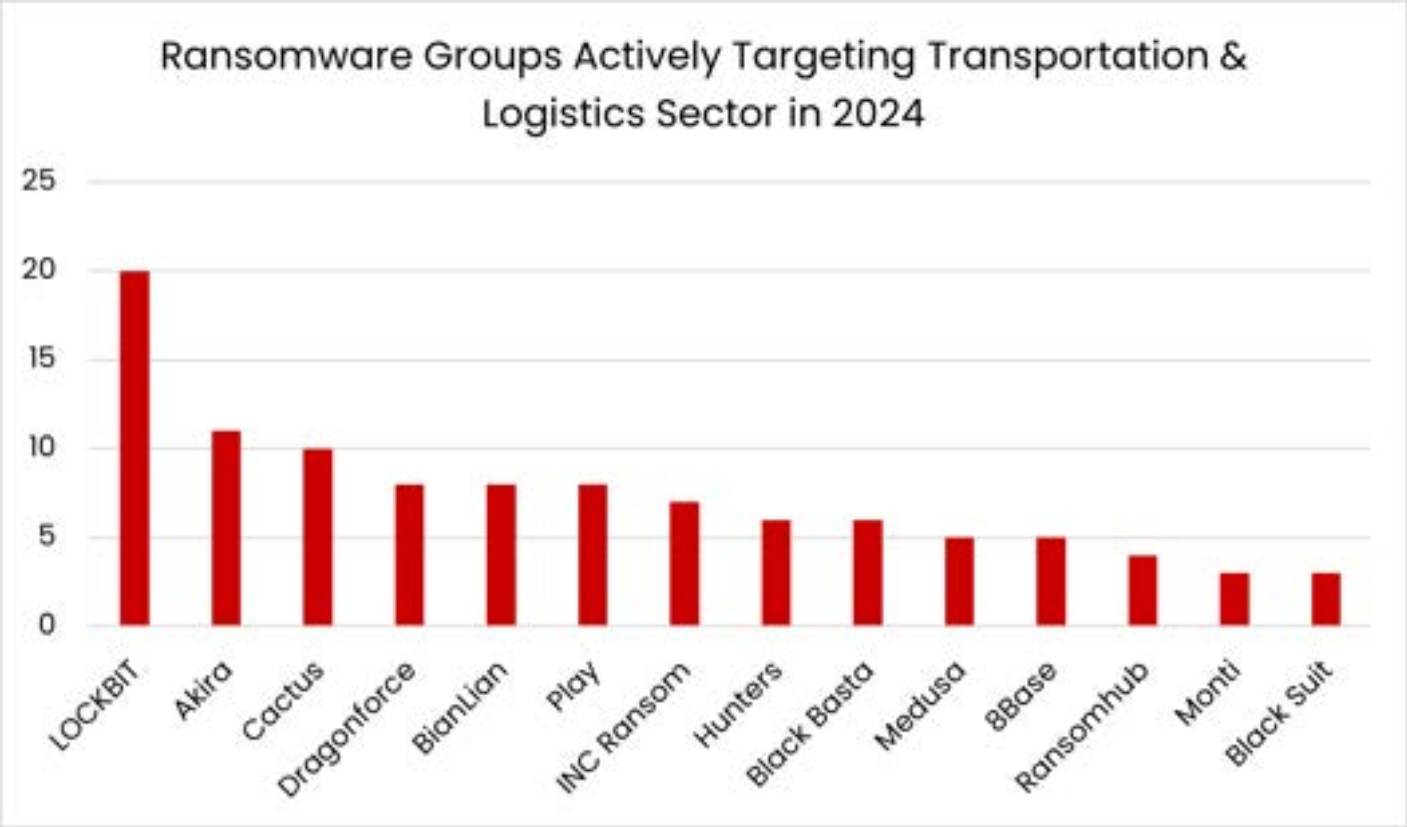
Hacktivists have been stepping up their game to launch sophisticated cyber-attacks on vulnerable IT and Industrial Control Systems (ICS), including mobile applications, exposed Human-Machine Interface (HMI), Programmable Logic Controllers (PLCs), and SCADA systems to disrupt the operations and inflict chaos. Moreover, hacktivists, to gain notoriety amongst the media, are attempting to infiltrate the networks, steal data, and leak them on their Telegram channels.

Another infamous hacktivist, SiegedSec, claimed to have compromised Malaysian carrier AirAsia Berhad and leaked 2.2 GB of data from the airline's mobile application, including source codes and internal files. The leaked data contained supplier and vendor details, statements of accounts for certain periods, bank account details for the airline in different countries, customer records, and invoices related to their ground operations.

EMERGING CYBERSECURITY RISKS

RANSOMWARE

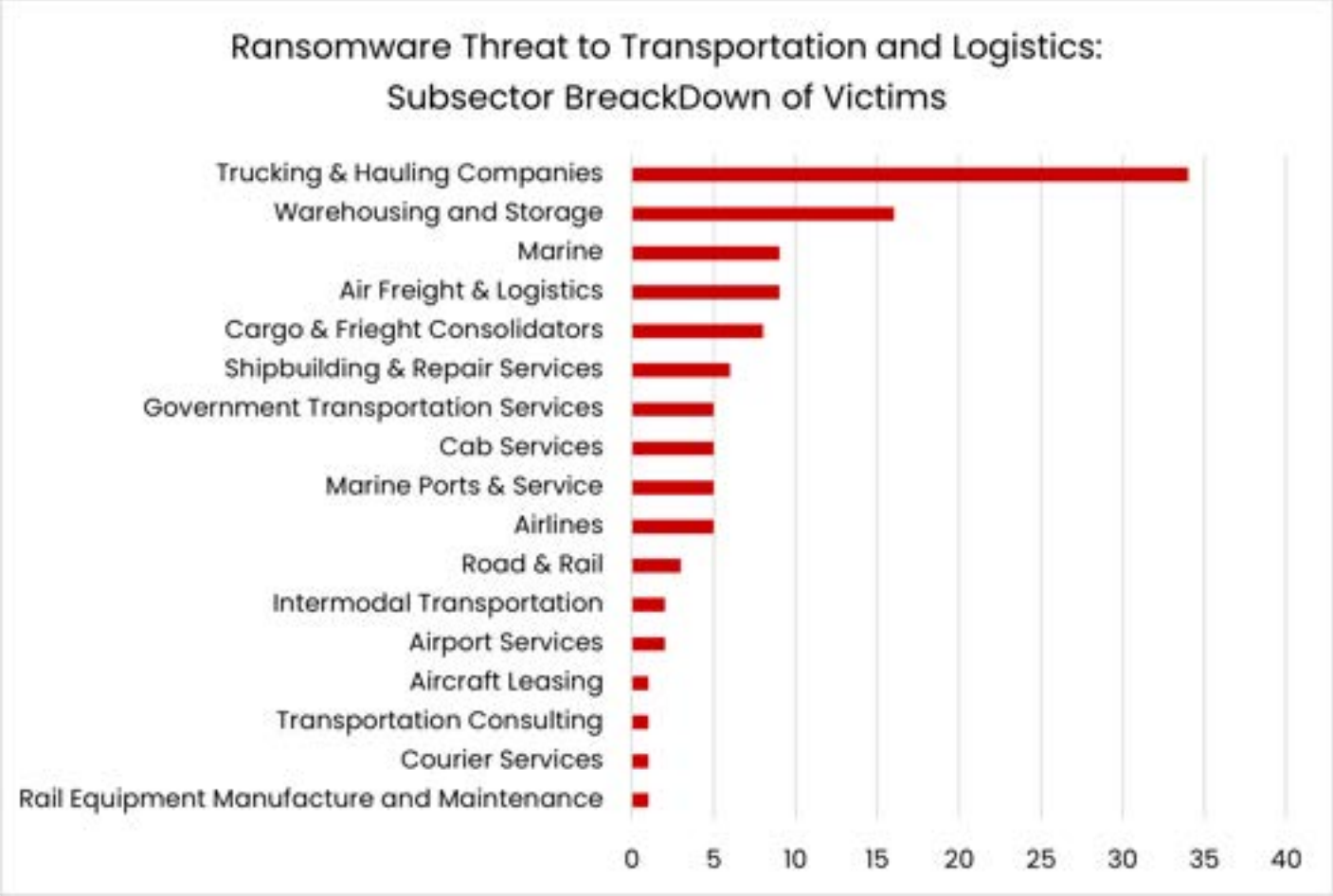
LOCKBIT continued to be the most notorious ransomware group, with 20 victims claimed from the Transportation and Logistics Sector. It was followed by Akira and Cactus.



EMERGING CYBERSECURITY RISKS

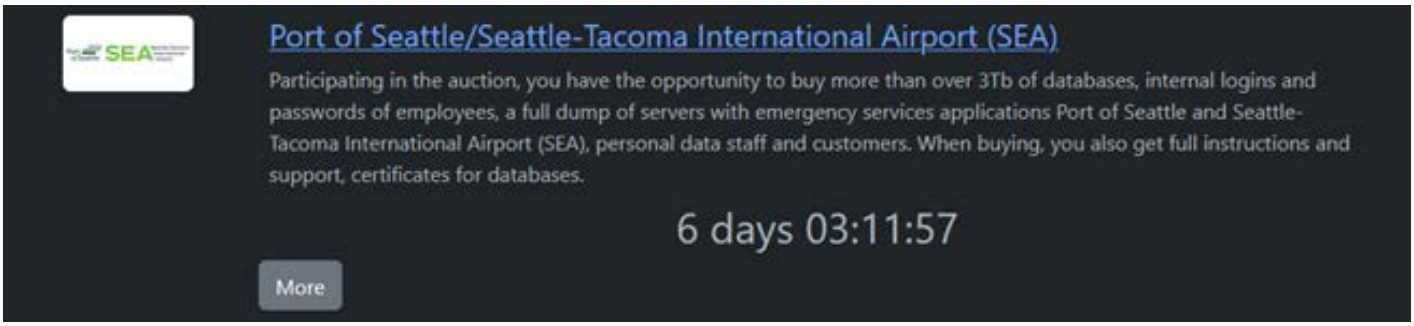
CRIL further dissected these ransomware attacks in 2024 to highlight the following ransomware threat landscape and understand the underlying motive of ransomware groups:

- The Trucking and Hauling sub-sector is the most targeted sector, reflecting the industry's reliance on technology and the critical nature of logistics operations, making it a prime target.
- Warehousing and storage facilities also faced a considerable number of attacks, highlighting vulnerabilities in inventory management and supply chain operations.
- The Air Freight and Marine sectors, which are crucial for international trade, emerged as the third most targeted subsectors due to ongoing geopolitical tensions.



EMERGING CYBERSECURITY RISKS

The Rhysida ransomware group attacked the Port of Seattle, leading to severe disruptions at Seattle-Tacoma International Airport. The attack encrypted critical systems, affecting baggage sorting, flight information displays, and check-in processes. This incident forced the use of handwritten boarding passes and manual bag searches, significantly impacting passenger experience and operational efficiency.

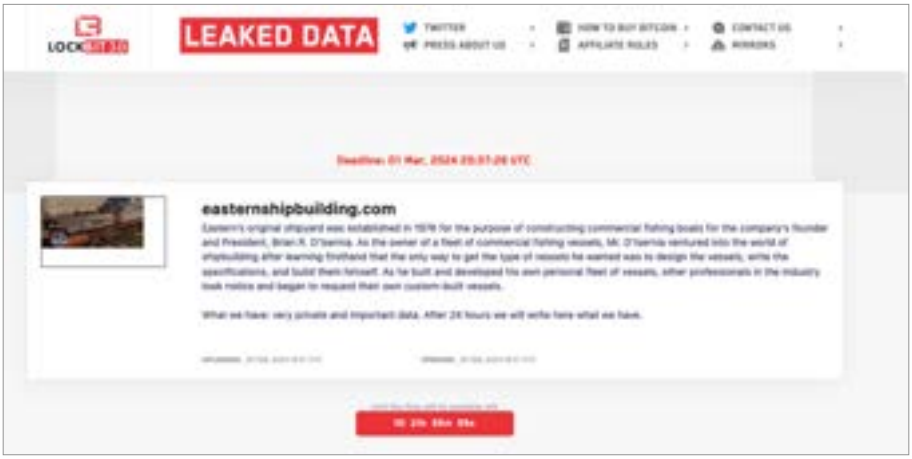


The newly emerged DragonForce ransomware group, in June 2024, took responsibility for an attack on Oahu Transit Services, Inc., widely known as 'TheBus'. The ransomware group claimed to have exfiltrated over 390 GB of data from the victim's network, among which they highlighted access to 800,000 transients' data. Following the attack, Oahu Transit Services experienced a multiple-day outage affecting its operations. This disruption hindered public transportation services, impacting daily commuters and travelers reliant on TheBus.

EMERGING CYBERSECURITY RISKS

Ransomhub ransomware targeted the Brazilian Port of São Francisco do Sul in May this year and leaked samples containing PII of Port officials, passport copies, financial documents, and engineering drawings. The ransomware group further claimed to exfiltrate 880,000 documents among the total 548 GB of compromised data. It is noteworthy that the access to the said organization was sold on an underground forum just a week back before the incident.

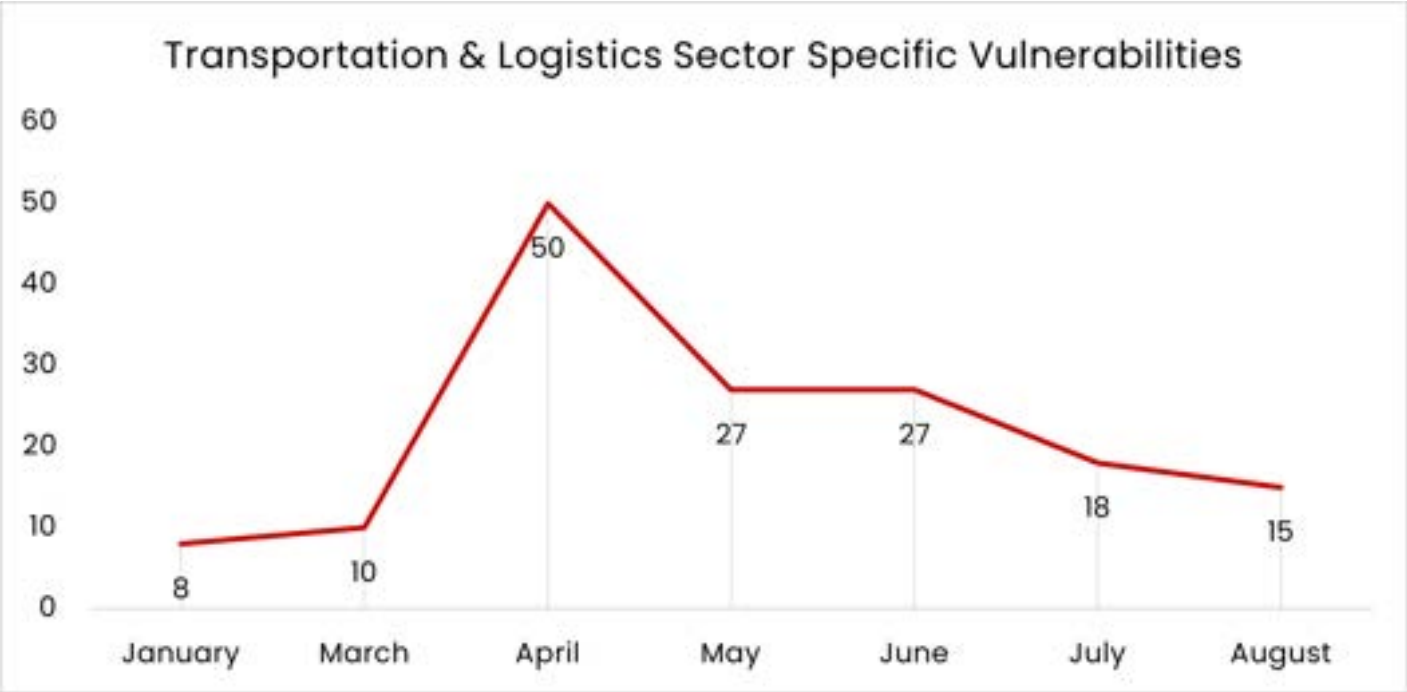
LOCKBIT had added US-based Eastern Shipbuilding Group to its list of victims in February 2024. Eastern Shipbuilding is responsible for building the Heritage-class OPCs, and a disruption to their operations may have further delayed the delivery of these critical vessels to the US Coast Guard. The breach may have exacerbated an already precarious position for Eastern Shipbuilding, which was already facing significant delays due to a devastating hurricane.



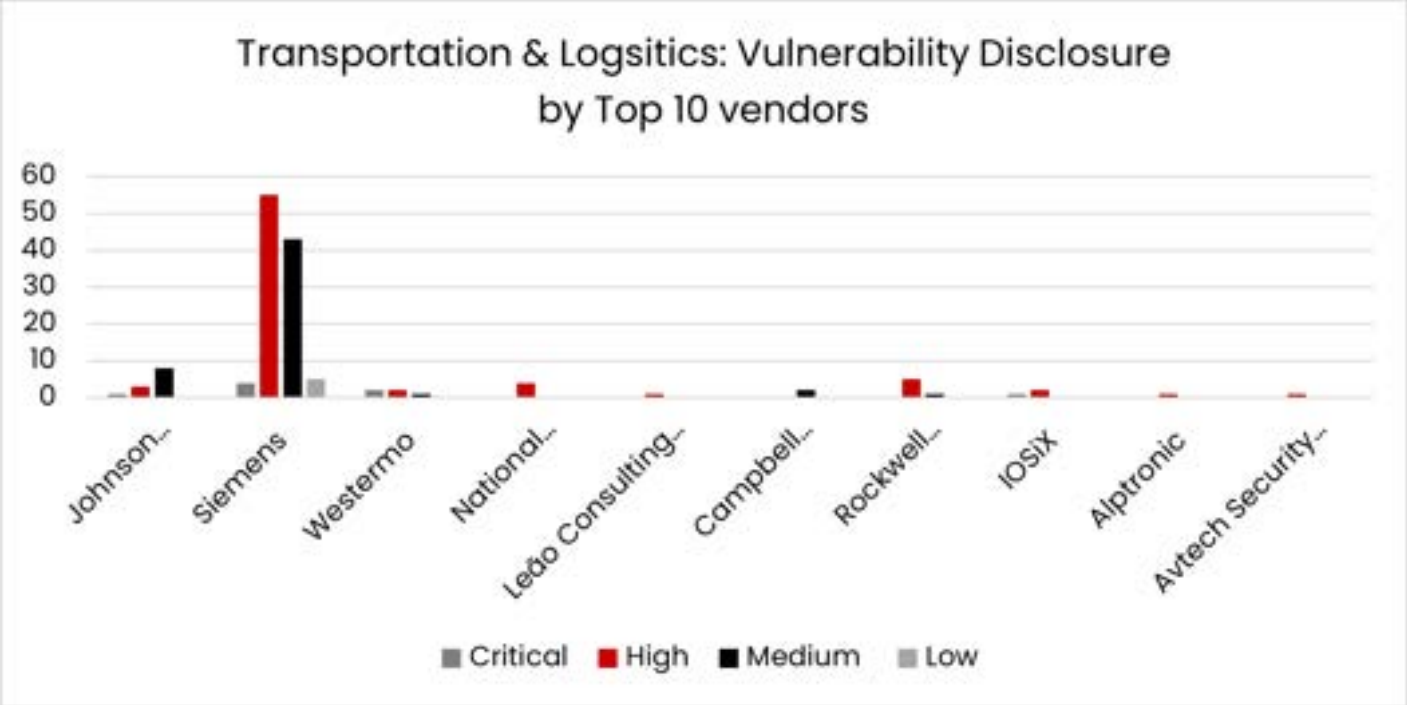
VULNERABILITY LANDSCAPE

CRIL closely monitored security advisories released by the Cybersecurity and Infrastructure Security Agency (CISA) specific to Operational Technology (OT) products used in the Transportation & Logistics sector from January 2024 to highlight the following:

- For the timeline of January 2024 to August 2024, a total of 37 security advisories were published by CISA, highlighting vulnerable ICS assets used in the Transportation & Logistics sector.
- The security advisories published covered 155 vulnerabilities in various vendors' products. The graph below underlines the months when the number of vulnerability disclosures increased.



VULNERABILITY LANDSCAPE



- Johnson Controls Inc. and Siemens have disclosed the majority of vulnerabilities (as shown in the graph above) in their product range, including:

  1. **Telecontrol:** A product of Siemens designed for a variety of transportation applications, providing essential monitoring and control capabilities. These solutions facilitate the oversight of mobile stations, including local public transport systems and ships operating on rivers and coastal areas. Additionally, they enable the control and monitoring of critical traffic management systems, such as traffic lights, tunnel projects, and lighthouses. Note: During the time of investigation, Cyble's ODIN scanner indicated 42 instances, with the majority of instances from Croatia.
  2. **ExacqVision:** ExacqVision, a video management system by Johnson Controls, is extensively used in the Transportation and logistics sector for monitoring tank farms, loading racks, rail yards, and commercial sites. It enhances security by providing reviewable video capable of recognizing license plates and driver faces. Further, airport warehouses help identify people and track specific goods, ensuring accurate inventory management and safety.

INTERNET EXPOSURES OF CRITICAL ASSETS IN THE TRANSPORTATION & LOGISTICS SECTOR

After a comprehensive investigation into cyberattacks launched by ransomware groups, hacktivist groups, and other threat actors targeting the Transportation & Logistics sector, CRIL identified the following categories of assets widely used in the sector have been and are likely to remain under threat:

1. **TELEMATICS AND GPS FLEET TRACKING**:
Systems that monitor vehicle locations and fleet performance are essential for ensuring efficient transport operations and optimizing routes.

2. **EV CHARGING AND ELECTRIC VEHICLE INFRASTRUCTURE**:
Critical infrastructure supporting the electrification of transport is vulnerable to disruptions in charging stations and management systems.

3. **ASSET TRACKING AND MANAGEMENT SOFTWARE**:
Tools used to track and manage transportation assets like vehicles and cargo, crucial for maintaining operational oversight and preventing loss.

4. **TRANSPORT LOGISTICS AND VISIBILITY SOLUTIONS**:
Platforms providing end-to-end visibility of shipments are vital for supply chain efficiency and minimizing delays.

5. **AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)**:
Systems that identify vehicles using license plates are important for traffic control, toll collection, and vehicle access management.

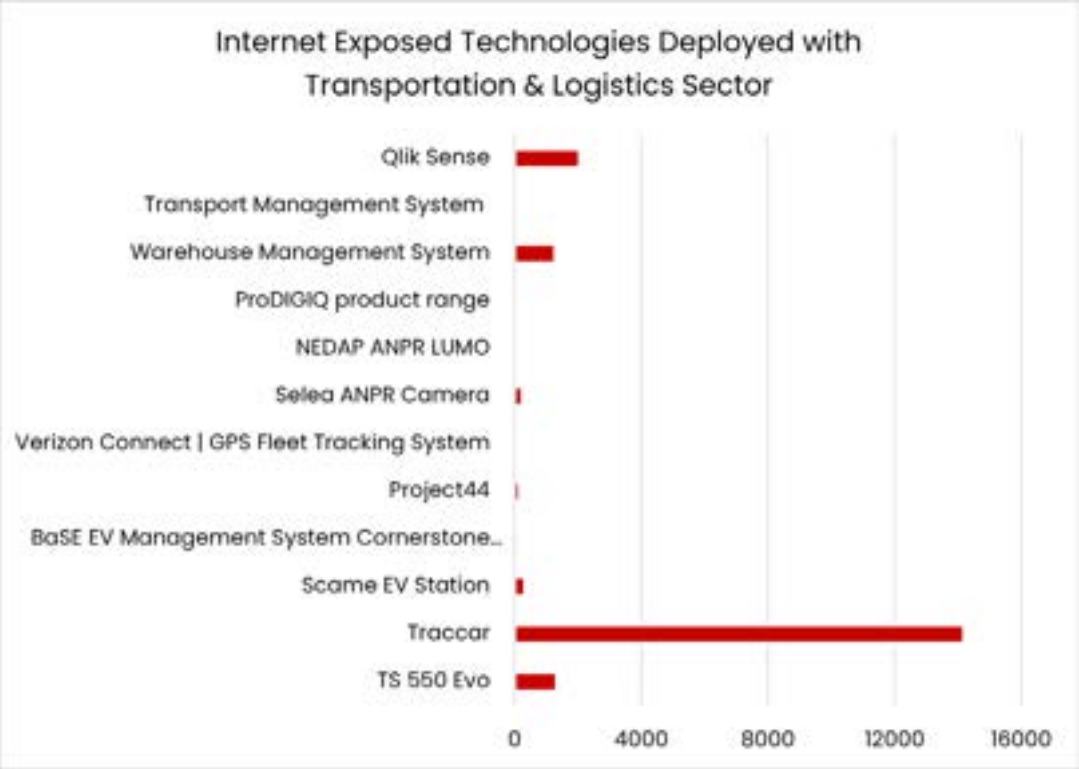
6. **AIRPORT AND AVIATION SOLUTIONS**:
Software and systems managing airport operations, flight schedules, and security are integral to the smooth functioning of air transport.

7. **WAREHOUSE AND INVENTORY MANAGEMENT**:
Software used to control inventory and streamline the flow of goods, which is key to maintaining transportation supply chains.

8. **DATA ANALYTICS AND BUSINESS INTELLIGENCE**:
Analytics platforms that support decision-making in transportation by providing insights into performance, efficiency, and optimization strategies.

INTERNET EXPOSURES OF CRITICAL ASSETS IN THE TRANSPORTATION & LOGISTICS SECTOR

Building on the identified categories, researchers further analyzed the products used within these sectors for potential internet exposure using Cyble's ODIN scanner. In several instances, exposed assets were linked to both public and private organizations operating in the transportation sector. The graph below illustrates these findings.



It is important to highlight that among the products observed, Franklin Fueling Systems has identified two critical assets with potential vulnerabilities: Traccar and the Automatic Tank Gauges EVO 550.

Traccar, an open-source GPS tracking platform, was found to have several remote code execution vulnerabilities, as reported by Horizon3.ai. These vulnerabilities could allow attackers to gain unauthorized access, manipulate fleet tracking data, or disrupt transportation operations.

Similarly, the EVO 550 Automatic Tank Gauge, which plays a vital role in fuel management systems, was the subject of a recent advisory from CISA due to security weaknesses that could expose critical fuel infrastructure to cyber threats. Cyble is actively monitoring cyberattacks targeting these gauges, which are widely used in the oil and gas industry.

CONCLUSION

The transportation sector is a critical pillar of global economies, facilitating the movement of goods, services, and people. A cyberattack targeting this sector not only impacts the victim organization financially and operationally but also disrupts the supply chain as a domino effect, affecting the delivery of essential goods and services vital for other national sectors. Strategically aimed attacks have the potential to cripple a nation's economy, creating widespread disruption. Recently, there has been a significant surge in attacks on airports and port authorities, indicating that threat actors are becoming increasingly sophisticated, with the capability to conduct large-scale cyber espionage and disruptive operations.

Cyble Research and Intelligence Labs believes that in the near future, threat actors may expand their focus beyond the externally facing vulnerable assets of organizations within the transportation sector. A more targeted campaign strategy is expected to emerge, where attackers will increasingly aim at IoT and OT (Operational Technology) devices used in this industry. These devices, which play critical roles in managing infrastructure, logistics, and real-time operations, present unique vulnerabilities that, if exploited, could lead to severe disruptions. As transportation systems become more digitized and interconnected, the risk of these attacks grows, making IoT and OT devices prime targets for sophisticated cyber campaigns.

Industry Recognition

Gartner

Cyble Named a Sample Vendor in Three Gartner® Hype Cycles for Managed IT Services, 2024, Cyber Risk Management, 2024 and Security Operations, 2024

FORRESTER®

Cyble Recognized in Forrester's Attack Surface Management Solutions Landscape Q2-2024 Report

FROST & SULLIVAN

Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

Gartner Peer Insights.

4.6/5

Ranked among top 5 cyber threat intelligence providers

Named a leader in the G2 Grid for Dark Web Monitoring

Named Editor's Choice for Threat Intelligence by Cyber Defense Magazine

Earned nine awards at the Global InfoSec Awards during RSA

Ranked in Y Combinator's Top 100 AI Startups for 2024

Recognized as one of America's Best Startup Employers by Forbes

CYBLE.

Cyble provides one of the fastest and most comprehensive coverages across adversaries, infrastructure, exposure, weaknesses, and targets by leveraging cutting-edge AI technology and real-time threat intelligence and detection. Through advanced data analysis, expert insights, and automated processes, Cyble facilitates swift detection, prioritization, and remediation of security threats, and enables governments and enterprises to protect their citizens and infrastructure by delivering crucial intelligence promptly. Headquartered in Atlanta, GA, and with employees across 12 countries, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com

11175 Cicero Drive Suite, 100 Alpharetta GA 30022, US. | contact@cyble.com | +1 888 673 2067