Cyberthreats in the aviation sector

Technical Analysis Report from our Global Cyber Threat Intelligence team

THALES
Building a future we can all trust

Table of Content

Table of illustration

_Summary

_This report provides an in-depth analysis of the evolving cyber threat landscape in the aviation sector, highlighting the growing influence of geopolitical tensions on the security of aviation systems. It underscores the strategic appeal of this sector to both cybercriminals and state-sponsored actors, driven by its operational complexity, the high value of its data, and the significant impact that disruptions can cause. The report also presents a detailed overview of incidents observed in 2024 and 2025, including Business Email Compromise (BEC) attacks, phishing campaigns, supply chain compromises, and ransomware threats. It emphasizes the increasing involvement of hacktivist groups and state-sponsored APTs (Russia, China, Iran, North Korea), while outlining the most used attack techniques—illustrating how adversaries continuously adapt to the sector's unique vulnerabilities.

Cyber Threat Intelligence report notice

This report serves as a strategic resource for stakeholders in the aviation industry, cybersecurity professionals, and decision-makers in both the public and private sectors. By mapping the intersection of geopolitical dynamics and cyber threats, it provides a comprehensive understanding of the current and emerging risks that could affect the aviation ecosystem. The detailed breakdown of threat actors, techniques, and recent incidents equips organizations with actionable insights to better assess their own exposure and prioritize defensive investments.
Beyond its diagnostic value, the report also supports anticipatory thinking. It can be used to inform cyber resilience strategies, shape sector-specific risk management policies, and guide collaborative efforts between industry actors and government bodies.

Additionally, it offers a foundation for scenario planning and threat modelling exercises, helping aviation stakeholders move from reactive postures to proactive threat anticipation and mitigation.

Introduction

_Securing the Skies: Cyber Threat Intelligence for the Aviation Ecosystem

In a world where the aviation sector is no longer just a symbol of mobility, but a pillar of global security and geopolitical power, cyber threats are emerging as a direct and disruptive force. Airlines, Airports, and Air Traffic Management (ATM) systems—highly connected and heavily digitized—are increasingly targeted by cybercriminals, hacktivists, and state-sponsored attackers.

At Thales, we understand that protecting the skies means securing every digital layer that keeps aircraft in the air and passengers moving safely. With more than 6,000 cybersecurity experts including cyber consultancy teams, three CERTs, one global Cyber Threat Intelligence team, and a global footprint across 30+ countries, we are at the heart of aerospace cybersecurity innovation. Our 9 Security Operations Centers (SOCs) actively monitor, detect and respond to threats 24/7, bringing together deep aeronautical know-how with cutting-edge cyber intelligence.

This report is built on our unique positioning in the aviation industry, backed by 8000+ aerospace staff, strong partnerships with 500+ operators, and our active involvement in international cyber aviation working groups. It is designed to deliver actionable CTI insights for the entire aviation ecosystem—whether you're flying the aircraft, managing the skies, or securing the gates on the ground.

_1 From the threat context to the reality of the risk

THE EFFECTS OF GEOPOLITICS ON THE AVIATION SECTOR

The interlinking of geopolitics and the aviation sector

The geopolitical interests of nations, such as territorial expansion, national security, competition for resources, among others, have motivated the research and development of recent technological advances in the field of aeronautics. Aviation has had a particularly significant impact on geopolitics, modifying international relations, security and stability. And conversely, the trend today would be to say that geopolitics and international relations have a considerable influence on the aviation sector and its security, particularly in terms of cybersecurity.

Before the advent of cyberwarfare, these concerns only materialized in the form of kinetic warfare or sabotage operations. But this is no longer the case, where non-kinetic operations aimed at compromising a government's ability to guarantee the security of critical infrastructures are unfortunately commonplace.

From a legislative point of view, there is no international standard defining "critical infrastructure". In Singapore, for example, the Cybersecurity Act defines these sectors as follows: "Critical sectors [...] include energy, water, banking and finance, health, transport (including land, sea and air), infocommunications, media, security and emergency services, and government".[1]

But in Hong Kong, the Critical Infrastructure Bill proposed in July 2024 includes air transport as a critical sector[2] on its own right, not as a sub-sector of the transport sector. If we take the case of hacktivists, who are very prolific in terms of cyberattacks against states supporting Ukraine, there have been DDoS attacks against airlines, for example. According to information dated March 13, 2025, the pro-Russian hacktivist group NoName057(16) had carried out DDoS attacks against France, targeting numerous corporate sites in various sectors. The aviation sector has been particularly hard hit, with an attack on the ASL Airlines France website.[3]

The aviation sector and current conflicts

Airspace restrictions, whether due to military conflicts, diplomatic sanctions or security concerns, are forcing airlines to make rapid operational adjustments, and are also falling victim to cyberattacks, according to current conflicts.[4]

The war between Russia and the Ukraine has considerably altered the perception of cyber-attacks targeting the aviation sector.

Firstly, there has been a change in airspace, as Western countries have banned Russian airlines from their airspace and, in retaliation, Russia has restricted access to its skies for many carriers. This led to diversions of long-haul flights between Europe and Asia, forcing airlines to fly further north or south, increasing fuel costs and journey times. Some airlines have even had to reconsider the viability of certain routes due to the additional costs involved.[5]

Secondly, the ongoing Russia-Ukraine conflict has prompted a surge of cyber-attacks against the aviation sector, with airlines based in or openly supported by nations backing Kyiv becoming prime targets.[6]

CYBERSECURITY ON THE AVIATION INDUSTRY

The aviation sector is particularly affected by cyber threats. Its strategic and critical nature for the free movement of people and the vitality of world trade it attracts a broad and evolving array of threats, particularly involving attacker groups sponsored by third countries and high-level cyber criminals.
The aviation industry is one of the most interconnected and technologically advanced sectors in the world. Airlines are at the heart of this ecosystem, managing complex operations, sensitive customer data and mission-critical systems. The role of an airline goes far beyond transporting passengers; it is essential to global trade, tourism and national security.

What Is Covered Under Aviation Cyber Security Market?

Cybersecurity in the airline industry means protecting all physical and software infrastructures, as well as sensitive data, from unauthorized access, damage or misuse. It encompasses securing digital data, networks, online platforms, IT equipment and systems for transmitting or accessing this information.

Key areas of cybersecurity include the protection of networks, wireless environments, cloud services, digital content and applications. Network security plays a central role in defending interconnected systems against cyber threats. It relies on solutions deployed locally or in the cloud, essential to the management of airlines, freight transport, airport operations and air traffic control.

The aviation cybersecurity market has grown significantly in recent years. In 2024, it is estimated to be worth $4.98 billion, rising to $5.32 billion by 2025, representing a compound annual growth rate (CAGR) of 6.8%. This dynamic can be explained by the increasing number of cyber threats in the airline industry, growing reliance on digital technologies, heightened regulatory compliance requirements, the need to protect sensitive data, as well as several high-profile cybersecurity incidents.[7]

In the medium term, this upward trend is set to continue. Growth is projected to reach $7.44 billion by 2029, with a CAGR of 8.7%. This acceleration is the result of the continuing transformation of cyber threats, the development of connectivity in aviation systems, the global expansion of the aviation sector, as well as increased international cooperation to improve cyber resilience.[8]

Key future trends include increased prioritization of internal threat detection and prevention systems, adaptation to regulatory standards and frameworks, development of specialized cybersecurity training, integration of threat hunting technologies, and improved rapid incident response capabilities. These developments reflect the sector's strong desire to better anticipate, detect and neutralize the sophisticated attacks of the future.

Aviation, a sector exposed to a present cyberthreat

Cyber threats in the aerospace sector have intensified, both in frequency and complexity. In one year, ransomware attacks targeting the aviation supply chain jumped by 600%, revealing a rapid increase in the digital risks facing the industry.[9] This upsurge can be explained by a combination of factors, including rising geopolitical tensions, the acceleration of digital transformation and the widening attack surfaces of connected systems.

Statistics reveal that 71% of cyber incidents in aviation involve the theft of credentials or illicit access to critical infrastructures, jeopardizing system security. DDoS attacks account for around a quarter of reported cases, mainly affecting online services at major airport hubs, with significant repercussions on operations and access to essential services.[10]

Furthermore, ransomware continues to hit a wide range of players: airlines, aircraft manufacturers, trade associations. Recent events, such as the Rhysida group's attack on Seattle-Tacoma airport in 2024 or the data leak suffered by Boeing in 2023, bear witness to this. Critical systems - avionics, flight management, communications - remain particularly exposed, requiring enhanced protection efforts. As artificial intelligence and emerging technologies become integrated into flight operations, the surface of vulnerability expands, heralding a likely increase in threats targeting infrastructures essential to national security by 2025.

_Analyst's observation

The financial impact of cyber-attacks in the aviation industry is now major, amounting to several billion euros a year worldwide. This cost also includes rising cybersecurity expenses, business interruption, reputational damage, legal costs associated with dealing with compromised personal data, as well as potential compensation in addition to ransomware or sophisticated attacks carried out by state-sponsored groups. In an industry as interconnected and critical as aviation, disruptions can spread very quickly, affecting not only airlines, but also airports, regulators, passengers and suppliers.
The most widespread attack vectors are well known: phishing sites imitating official platforms, DDoS attacks aimed at saturating servers, introduction of malware into on-board or ground systems, hacking into sensitive data, and of course, ransomware that paralyzes infrastructures until a ransom is paid. This range of digital tools is designed to exploit human and technical vulnerabilities at all levels, from administrative staff to critical navigation systems.
In addition to these already considerable threats, there are other forms of cybercrime specific to the airline industry, such as theft of personal or business data, usurpation of account credentials, and fraud involving loyalty programs, notably air miles. These acts, although sometimes considered secondary, undermine user confidence and are potential entry points for more serious attacks.
Taken together, these elements form what could be described as a "perfect storm": a vulnerable, highly digitized ecosystem, exposed to persistent and evolving threats, in a tense geopolitical context. This requires the aerospace industry not only to constantly modernize its cybersecurity systems, but also to develop an organizational culture focused on resilience, risk anticipation and international cooperation.

[1] "The EU Cybersecurity Act | Shaping Europe's Digital Future," accessed May 16, 2025, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

[2] "The New Cybersecurity Dawn – Hong Kong Readies for New Critical Infrastructure Legislation," accessed May 16, 2025, https://www.twobirds.com/en/insights/2024/china/the-new-cybersecurity-dawn-%E2%80%93-hong-kong-readies-for-new-critical-infrastructure-legislation.

[3] Patrice Remeur, "La France est elle vraiment ciblée par NoName057(16) ?," Solutions-Numeriques (blog), March 13, 2025, https://www.solutions-numeriques.com/?p=235931.

[4] Hub Selection Recruitment, "Geopolitical Impacts on Aviation: How Airspace Restrictions and Tensions Shape Flight Routes - Hub Selection, Aviation, Engineering, Automotive, Recruitment, Experts, Specialists, Jobs, Roles," Hub Selection (blog), March 10, 2025, https://hub-selection.com/geopolitical-impacts-on-aviation-how-airspace-restrictions-and-tensions-shape-flight-routes/.

[5] Recruitment.

[6] Recruitment.

[7] "Aviation Cyber Security Market Report 2025, Research and Analysis," accessed May 16, 2025, https://www.thebusinessresearchcompany.com/report/aviation-cyber-security-global-market-report.

[8] "Aviation Cyber Security Market Report 2025, Research and Analysis."

[9] "Together Against Threats: Advancing Aviation Cybersecurity Through Collective Action," Technology Advancement Center, February 11, 2025, https://thetac.tech/together-against-threats-advancing-aviation-cybersecurity-through-collective-action/.

[10] "Together Against Threats."

WHY DO CYBER ATTACKERS TARGET THE AVIATION SECTOR?

The entire air-transport ecosystem, such as airlines, airports, air-traffic management (ATM), aircraft manufacturers, maintenance organizations, drones, and global distribution systems, presents a uniquely attractive target due to several factors, among which we can find the following.

Operational complexity

Aviation operations are inherently complex, due to the stringent regulatory requirements of the sector and the airline's dependence on extensive, interdependent systems. A single flight relies on several critical systems: flight-planning software, baggage-handling PLCs, passenger-service apps, satellite links, weather feeds, payment gateways, and dozens of third-party vendors. A compromise in a seemingly minor node can propagate across partners in minutes, forcing flight delays, closing runways or halting an assembly line in a distant factory.

High data value

The sector holds a rich mix of sensitive data. Beyond passenger names and payment cards, airlines and airports accumulate travel histories, frequent-flyer preferences, biometric templates collected at seamless-border gates, and detailed cargo manifests that may reveal intellectual-property shipments or military logistics. If a data breach occurs and threat actors get this kind of data, it can be directly monetized, used for cyberespionage, for targeted phishing campaigns or other frauds.

Operational disruption

No other industry feels the pain of downtime so quickly and so publicly. If the departure-control system at a big airport suffers an attack, tens of thousands of passengers are stuck within minutes. A ransomware attack on air-traffic control services can force large parts of the airspace to close. Malware in a factory's digital model can stop an entire aircraft line from being built. Hackers know these interruptions cost huge amounts of money, so they bet airlines and airspace companies or regulators will pay a ransom fast rather than suffer days of cancelled flights, delayed cargo, and stalled production.

Geopolitical reasons

The focus on geopolitical motives in airline cybersecurity reveals a major issue that is often underestimated: the role played by civil aviation in the strategic balance of states. Airlines, although commercial entities, operate within critical national infrastructures (transport networks, border management, economic and tourism flows) and are therefore perceived as prime targets for hostile nation-states. Cyberattacks sponsored by foreign governments are not necessarily aimed at direct financial gain, but rather at gathering sensitive information (diplomatic itineraries, passenger profiles, biometric data, etc.), destabilizing the economy, or demonstrating power in a context of political or military tension.

Intellectual-property theft and industrial espionage

Aircraft and engine manufacturers store proprietary design files, performance logs and certification documents worth billions in R&D. Compromising a Tier-2 composites supplier, an engine test cell or an avionics software repository can deliver blueprints, material tolerances and firmware that shorten a competitor's development cycle or enhance a nation's military capabilities.

_Analyst's observation

The airline industry is ultra-regulated, operating with a global, digitized supply chain. The slightest flaw can cause major cascading effects, from delays to flight cancellations. This increases the pressure on IT systems, which must not only be robust, but also resilient and accessible at any time. This technological dependence creates fertile ground for targeted attacks, exploiting the imperative need for airlines to maintain operational continuity.
Beyond the technical challenges, there are more strategic dimensions. Indeed, there is the high commercial value of passenger data, the geopolitical motivations behind certain attacks, and above all, the central issue of trust.

_2 Cyber events on the Aviation sector in 2024 and 2025

The aviation sector has faced a turbulent threat landscape over the past years, marked by a notable increase in both the frequency and complexity of cyber incidents. From financially motivated cybercriminals to politically driven hacktivist groups and state-sponsored actors, aviation has remained a high-value target.

This section provides an overview of the most significant cyber events impacting the industry in 2024 and 2025, categorized by type and vector of attack. The analysis includes business email compromise (BEC), supply chain breaches, ransomware campaigns, hacktivist operations, and cyber-espionage activities, highlighting key incidents and their implications for operational continuity and sector resilience.

BUSINESS EMAIL COMPROMISE (BEC)

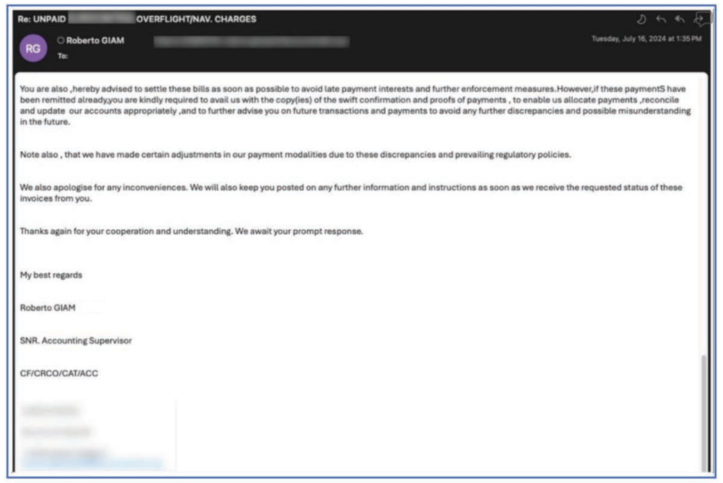
Business Email Compromise (BEC) attacks have become an increasingly sophisticated tool for financial fraud, as threat actors exploit compromised legitimate business email accounts to steal funds through unauthorized transactions. These types of attacks have been on the rise across various industries, including the aviation sector, where threat actors often target accounting and finance departments to initiate fraudulent payment requests.

Incident Example: EMEA-based Aviation Company BEC Attack

In a notable incident within the aviation industry, a threat actor spoofed an aviation company based in the EMEA region (Europe, the Middle East, and Africa) to deceive its clients, which included both global and U.S.-based aviation companies[11].

The attacker sent fraudulent emails to the customers' accounting departments, requesting payment for overdue invoices, with the goal of misleading these departments into making unauthorized payments to the attacker's accounts. While the attack was eventually detected by an advanced email security solution, another well-known secure email gateway provider failed to identify the threat.

Throughout July 2024, the threat actors continued to target aviation companies by sending emails requesting payment for overdue invoices. By mid-August, new intelligence revealed that the attackers had altered the domains used in their campaign multiple times—at least five different changes were made to typo-squatted domains, a tactic where malicious actors register domains that closely resemble legitimate ones to deceive recipients into believing they are authentic.



Re: UNPAID [redacted] OVERFLIGHT/NAV. CHARGES

RG ○ Roberto GIAM [redacted]
To:
Tuesday, July 16, 2024 at 1:35 PM

You are also ,hereby advised to settle these bills as soon as possible to avoid late payment interests and further enforcement measures.However,if these paymentS have been remitted already,you are kindly required to avail us with the copy(ies) of the swift confirmation and proofs of payments , to enable us allocate payments ,reconcile and update our accounts appropriately ,and to further advise you on future transactions and payments to avoid any further discrepancies and possible misunderstanding in the future.

Note also , that we have made certain adjustments in our payment modalities due to these discrepancies and prevailing regulatory policies.

We also apologise for any inconveniences. We will also keep you posted on any further information and instructions as soon as we receive the requested status of these invoices from you.

Thanks again for your cooperation and understanding. We await your prompt response.

My best regards

Roberto GIAM

SNR. Accounting Supervisor

CF/CRCO/CAT/ACC

[redacted]

FIGURE 1: AN EMAIL SPOOFING THE EMEA-BASED AVIATION COMPANY (PROOFPOINT)

[11] Cybersecurity Stop of the Month: Preventing Vendor Impersonation Scams,» Proofpoint, September 16, 2024, https://www.proofpoint.com/uk/blog/email-and-cloud-threats/preventing-vendor-compromise-attacks.

To further bolster the credibility of their fraudulent messages, the attackers created a fake LinkedIn profile, which they used to lend legitimacy to their communications. This tactic, commonly seen in social engineering attacks, is designed to make fraudulent emails appear more convincing and persuasive.

Over the course of several months, the attackers specifically targeted individuals within the accounts payable and finance departments, as well as distribution lists associated with finance and accounting.

Key indicators that raised suspicion included the fact that the recipient had no prior relationship with the sender, a red flag for potential fraud. Additionally, the sender's domain was newly registered, a common trait in fraudulent campaigns as attackers often create fresh domains to evade detection. The domain had low traffic and was not recognized by the organization, further suggesting malicious intent. To mask their identity, the attackers used a domain that closely resembled an existing supplier's domain, with a slight variation (an additional letter «l»). Such small changes are often employed in BEC attacks to impersonate trusted entities. The emails themselves requested either payment for the overdue invoices or proof of payment, which is highly unusual for legitimate senders who typically already have access to payment details.

Incident Example: Phishing Campaign by ATK300 (UNK_CraftyCamel)

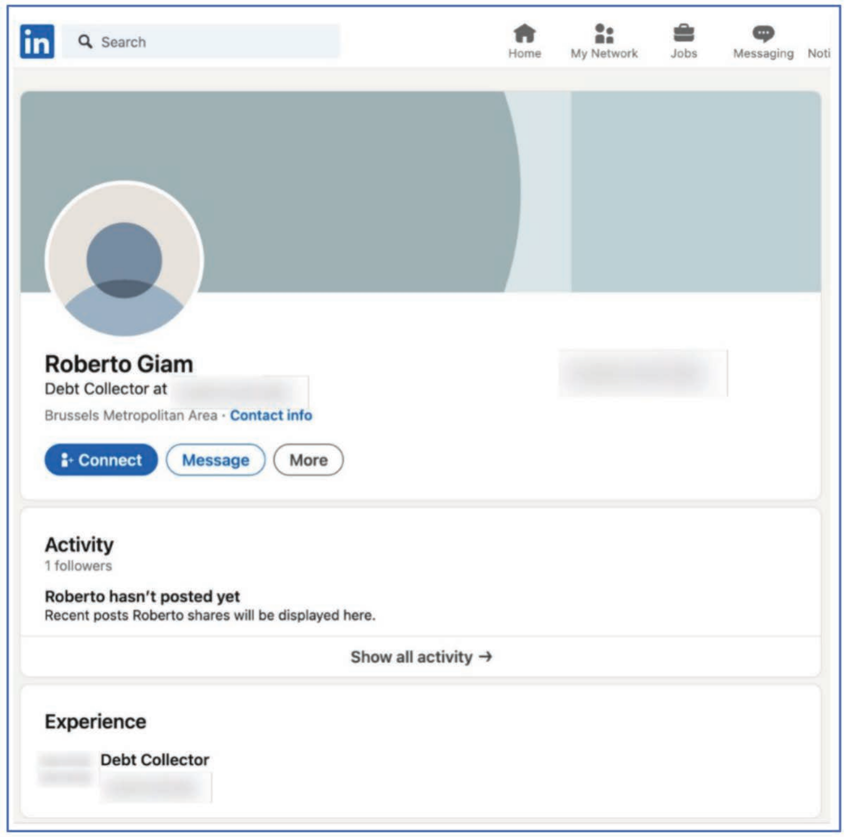
In late October 2024, another highly targeted email-based attack was attributed to the Iranian-linked threat actor group, UNK_CraftyCamel. This group launched a phishing campaign targeting five aviation and satellite communications organizations in the United Arab Emirates[12].

To execute the attack, the threat group used a compromised email account from INDIC Electronic, an Indian electronics company that maintains business ties with all the targeted organizations. The attackers tailored the emails specifically for each organization, leveraging the established relationships to increase the credibility of their messages.

The emails contained links to a fake website that appeared to belong to the Indian company («indicelectronics[.]net»), which was hosting a ZIP package (OrderList.zip) containing two PDF files and an XLS file. However, the XLS file was actually a Windows shortcut (LNK) that masqueraded as a Microsoft Excel document by using a double extension. The two supposed PDF files were revealed to be polyglots, one containing a ZIP archive and another posing as a HTML application file. These files were interpreted as valid formats by the recipients' systems, allowing the attackers to exploit vulnerabilities in the system.

The sequence of the attack involved launching cmd.exe with the LNK file and running the PDF/HTA polyglot file using mshta.exe. This triggered a script that unpacked the contents of the ZIP file, which included an internet shortcut file. This file then loaded a binary that searched for an image file, XORed it with a string, and decoded it to launch the Sosano DLL backdoor. This backdoor allowed the attackers to maintain persistent access to the targeted systems.

At the time of writing, the threat group, ATK300 (UNK_CraftyCamel), is believed to be linked to Iranian state-sponsored operations, sharing similar tactics, techniques, and procedures (TTPs) with known groups such as ATK35 (TA451), which have previously targeted aerospace organizations. Despite these similarities, researchers believe that ATK300 (UNK_CraftyCamel) is a separate and distinct threat cluster.



Roberto Giam
Debt Collector at [redacted]
Brussels Metropolitan Area · Contact info

Connect | Message | More

Activity
1 followers

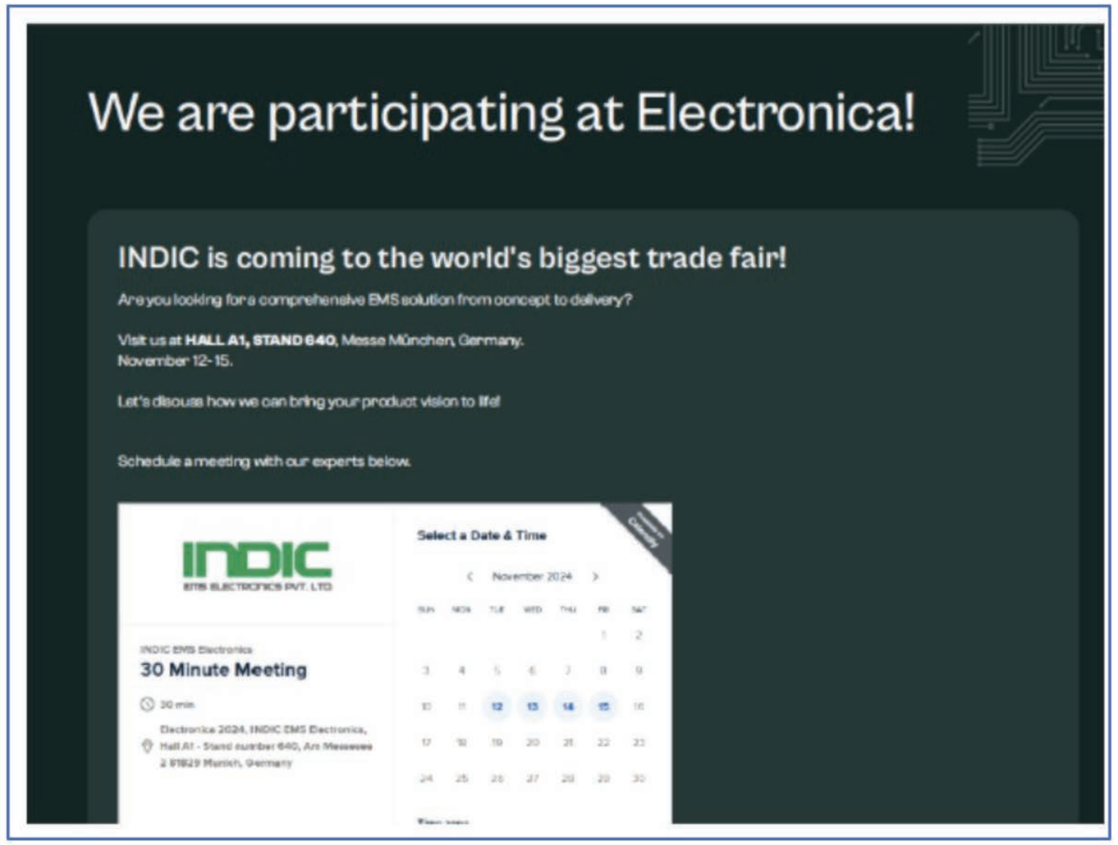
Roberto hasn't posted yet
Recent posts Roberto shares will be displayed here.

Show all activity →

Experience

Debt Collector
[redacted]

FIGURE 2: FAKE LINKEDIN ACCOUNT CREATED BY THE ATTACKERS TO ADD LEGITIMACY TO THEIR EMAILS (PROOFPOINT)



We are participating at Electronica!

INDIC is coming to the world's biggest trade fair!

Are you looking for a comprehensive EMS solution from concept to delivery?

Visit us at **HALL A1, STAND 640**, Messe München, Germany.
November 12-15.

Let's discuss how we can bring your product vision to life!

Schedule a meeting with our experts below.

INDIC
EMS ELECTRONICS PVT. LTD

INDIC EMS Electronics
30 Minute Meeting
30 min
Electronica 2024, INDIC EMS Electronics, Hall A1 - Stand number 640, Am Messesee 2 81829 Munich, Germany

Select a Date & Time
November 2024

FIGURE 3: ONE OF THE PDF FILES INCLUDED IN THE ORDERLIST.ZIP FILE (PROOFPOINT)

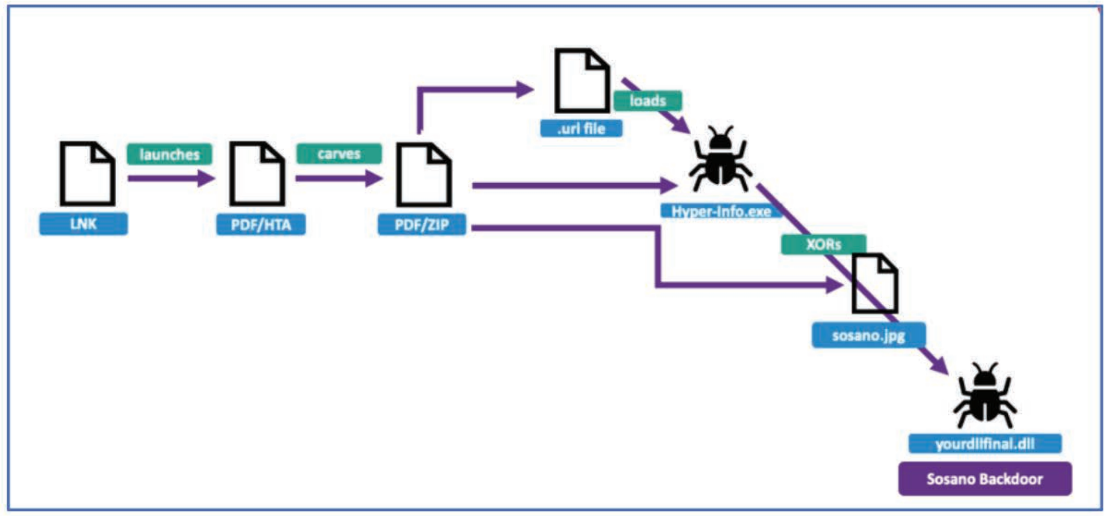


FIGURE 4: SOSANO BACKDOOR INFECTION CHAIN (PROOFPOINT)

SUPPLY CHAIN

Threat actors increasingly exploit trusted relationships between organizations and their suppliers or partners to gain access, establish persistence, or conduct fraud. In the aviation sector, which relies on a highly interconnected global supply chain, these attacks can be particularly damaging, as a compromise at any point in the chain can cascade across multiple organizations.

In 2024, SunExpress, a Turkish-German airline, reported that approximately 250,000 of its customers were affected by a data breach stemming from a cyberattack on a third-party service provider responsible for email newsletter distribution[13]. The incident involved unauthorized access to around 596,000 email addresses, including those belonging to SunExpress passengers. While SunExpress's own IT systems were not compromised, the breach led to the circulation of phishing emails impersonating the airline, raising the risk of further fraud and social engineering attacks. This event illustrates the indirect, yet critical exposure aviation companies face when customer data is processed by external partners.

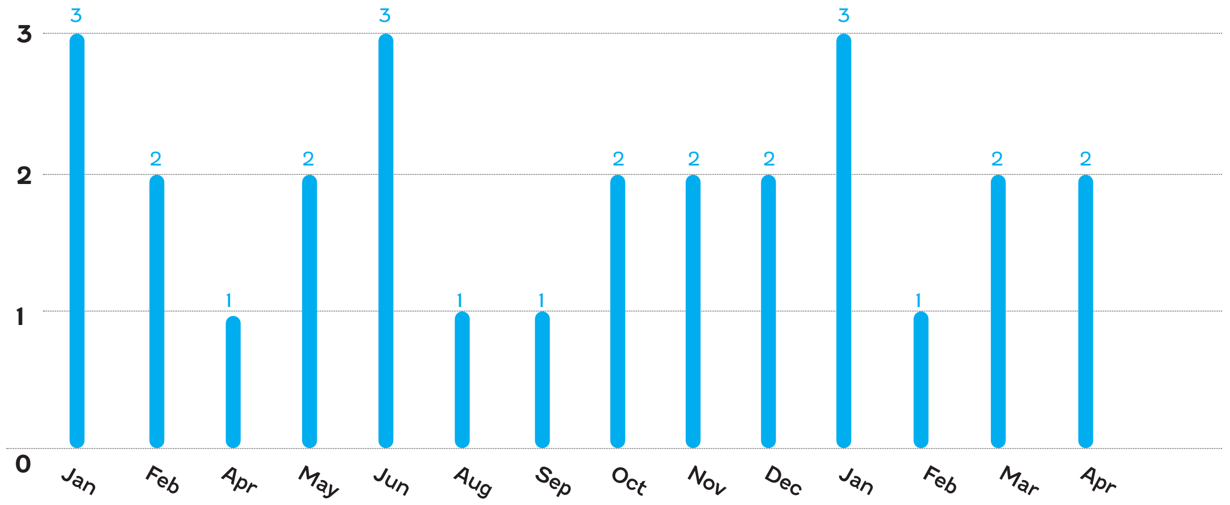
Threats to the supply chain are not limited to malicious cyberattacks. Disruptions can also arise from failures at third-party technology providers, whose software or infrastructure are deeply embedded in aviation operations. In July 2024, Delta Air Lines was forced to cancel thousands of flights following a software update failure attributed to cybersecurity vendor CrowdStrike[14]. According to legal filings, the malfunction originated from a faulty update to endpoint protection software deployed across Delta's systems. The issue disrupted essential IT infrastructure, grounding flights and causing widespread delays. The incident triggered a $500 million lawsuit against the vendor and underscored the severe operational and financial risks stemming from supply chain dependencies—even in the absence of deliberate compromise.

RANSOMWARE THREAT

The aviation industry has become, over the last few years, a prime target for ransomware attacks, driven by a combination of factors ranging from system vulnerabilities to financial incentives.
The aviation sector is a critical infrastructure. Simply by that recognition of importance, cybercriminals become more interested in exploring it. Any disruption, whether at airports, airlines, or air-traffic control, can trigger widespread chaos, hampering day-to-day operations and rippling through the broader economy. Cybercriminals exploit this urgency: knowing their victims are desperate to avert major interruptions, they count on a higher willingness to pay ransom.
In addition to the former, the dependence that airlines and airports have on a large array of interconnected systems, to control baggage, flight operations, passenger management, maintenance, communication, etc., increases the possible attack surface. Plus, as stated, the systems are interlinked, a small disruption in only one system, can impact all the others – with what can be deemed as a small attack, cybercriminals can disrupt large operations across various systems, whose disruption is very costly to the target. Overall, the growing digital transformation within the sector makes it more vulnerable to cyber threats, increasing potential entry points for hackers.
In connection with the previous, the aviation sector works based on a highly complex supply chain which involves numerous third-party service providers and vendors. An attack on the attack chain, a smaller services provider, can create many cascading effects for the industry.
Usually, the victims of ransomware attacks in the aviation industry are high-profile targets, such as known airlines or airports. When targeted, these companies have a high amount of pressure to avoid public fallout, which may happen if the cyberattack isn't responded to correctly in a timely manner – given that high profile attacks often generate more media attention.
The sensitive data that companies in the aviation industry safeguard in their systems is another pro point in a cybercriminals list. Airlines and airports hold large amounts of data such as passenger records and payment details. When stolen, the data can be used for identity theft and fraud or even be sold on the black market for the same reasons, being financially appetizing. Besides, the more valuable the data, the more likely the company is willing to pay the ransom to retrieve it.
Although there was a notable decrease in ransomware incidents from 30 attacks in 2023 to 19 in 2024 (a reduction of approximately 37%), early 2025 figures point toward a potential rebound. Specifically, Eight attacks have already been recorded as of May 1st, with 6 of those occurring in the first trimester alone. This represents a 20% increase in attacks in Trimester 1 compared to the same period in 2024, when only 5 incidents were registered. While the absolute number of attacks in 2025 is still below previous years, the high concentration of incidents within the first few months is concerning. In just four months, the aviation sector has already experienced over 42% of the total ransomware attacks seen throughout all of 2024, indicating a significantly accelerated pace.

[14] «Delta blames CrowdStrike for flight chaos in lawsuit,» Digital Watch Observatory, October 28, 2024, https://dig.watch/updates/delta-blames-crowdstrike-for-flight-chaos-in-lawsuit.

FIGURE 5: RANSOMWARE ATTACKS TARGETING THE AVIATION SECTOR 2024 – 2025



Also, Twenty-two distinct ransomware groups were involved in the 27 attacks recorded across 2024 and early 2025. The most active groups were Space Bears and LockBit, each responsible for 3 attacks, followed by RansomHub, Babuk, and BlackSuit, with 2 each.

An important dimension of the data is the geographical distribution of the victims affected, which shows that ransomware attacks in 2024 and early 2025 impacted organizations in at least 16 different countries. The United States was the most affected, accounting for 10 out of the 27 incidents — more than one-third of the total. Other notable cases occurred in France (3), Malaysia (2), and Spain (2).

The remaining incidents were spread across a wide range of countries including Egypt, Belarus, Mexico, Slovakia, Canada, Turkey, Ireland, and Latvia, each with one attack reported. This global distribution shows that, although the aviation sector is often singled out, attackers make no distinction when it comes to their victims' nationalities.

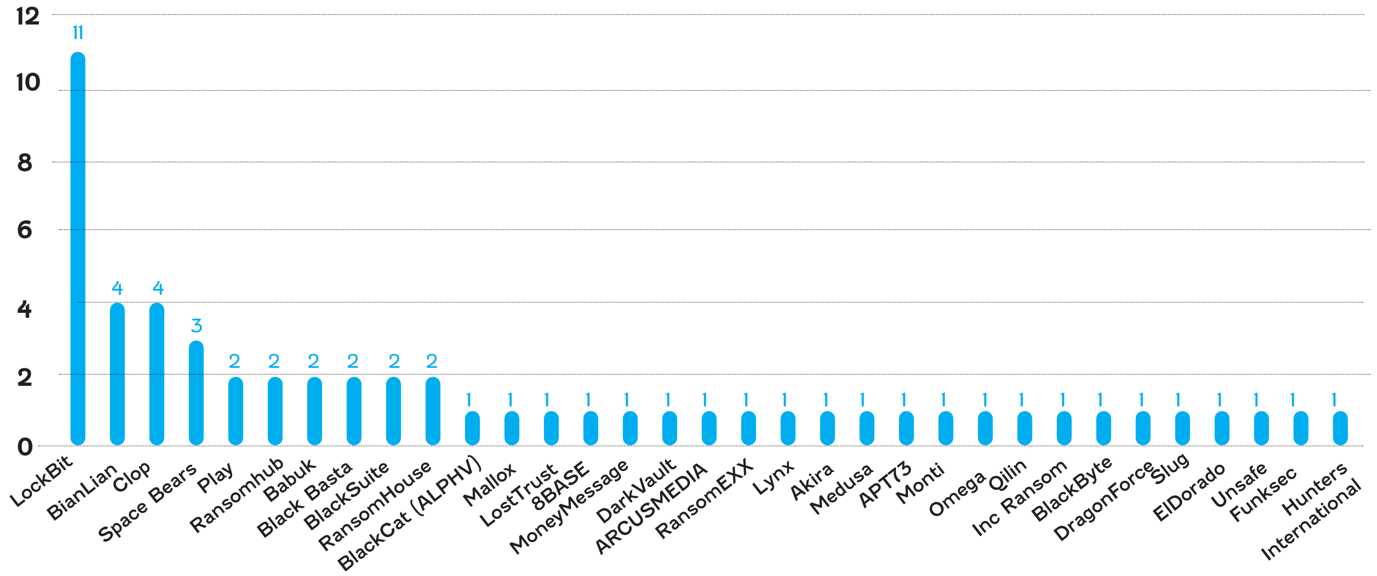


FIGURE 6: MOST ACTIVE RANSOMWARE GROUPS IN THE AVIATION INDUSTRY 2024 – 2025

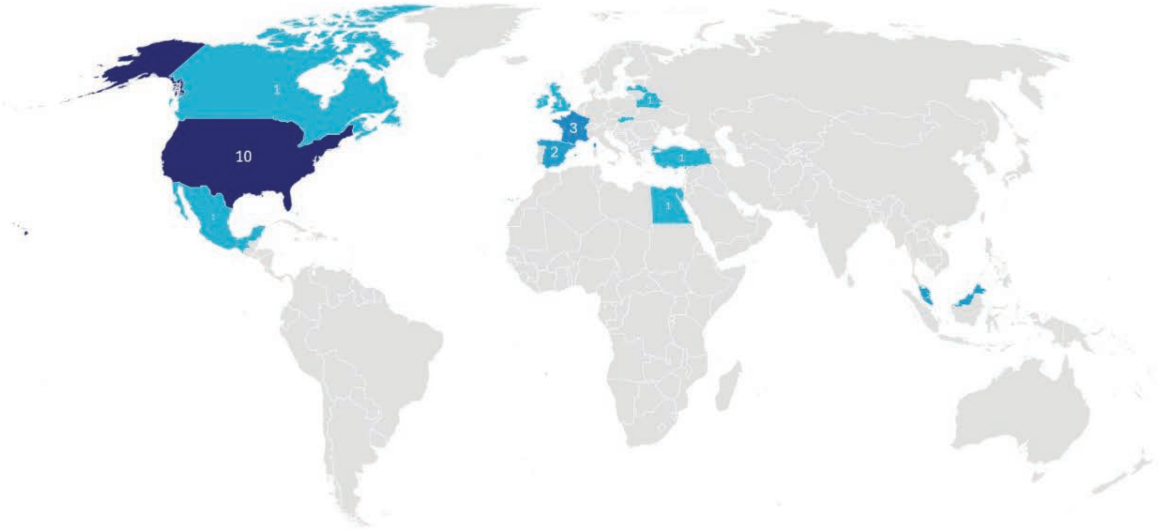
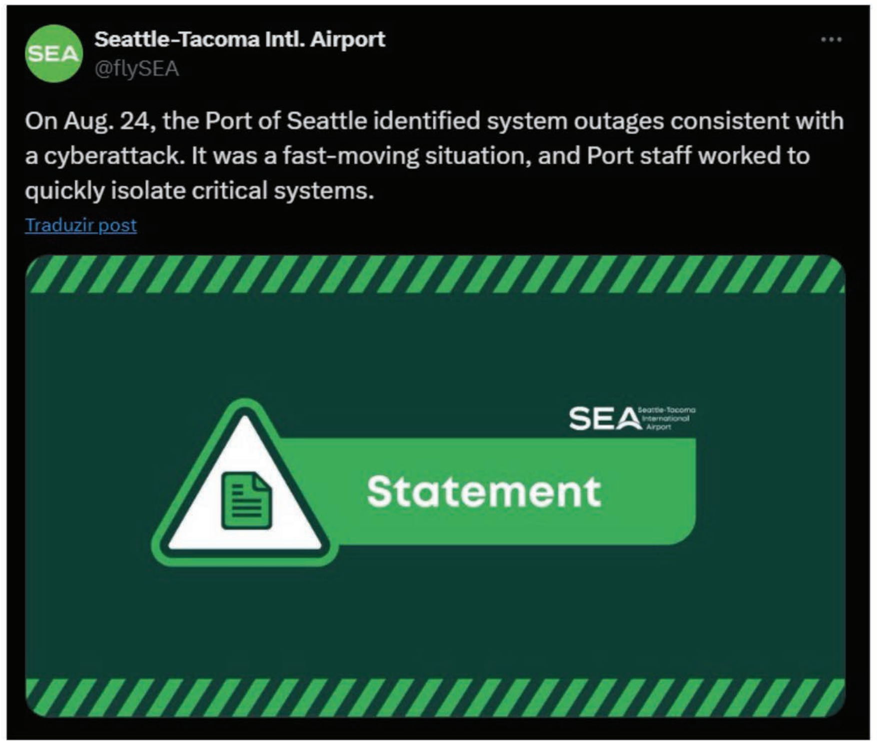


FIGURE 7: GLOBAL DISTRIBUTION OF RANSOMWARE ATTACKS AFFECTING THE AVIATION SECTOR 2024 – 2025

In August 2024, the Port of Seatle, including SEA Airport, was forced to isolate its critical systems, after an outage of its internet and web-based systems[15]. Although flights still left and arrived at the airport, with the systems outage the processes of check-in would take substantially longer, delaying operations. Given the outage within the airport's system, the organization made a public statement advising passengers to check flight delays directly with the airlines companies, and to make their check-ins via the apps, facilitating the processes since it's baggage handling, check-in kiosks, ticketing, Wi-Fi, passenger display boards, and the Port's website and app, were all down[16].

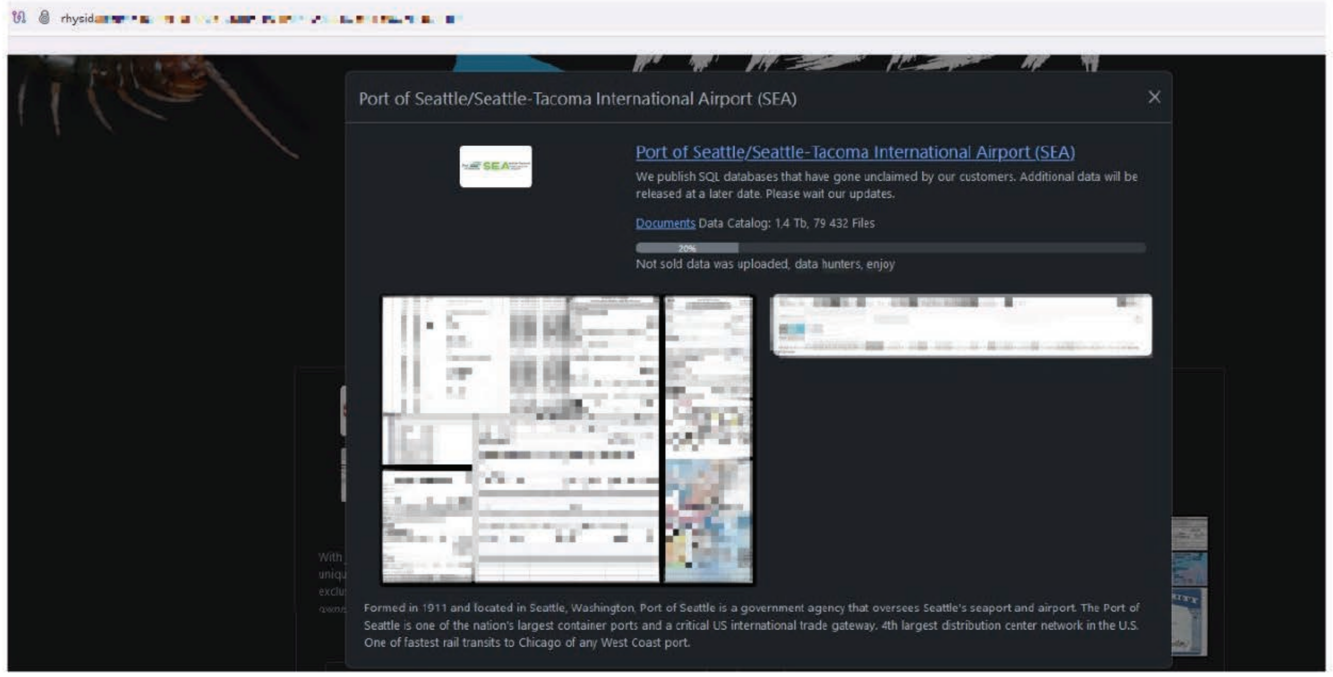
Later, in September, Port of Seatle revealed that the cyberattack had been a ransomware attack perpetrated by the Rhysida ransomware group. The ransomware group asked for a ransom for the stolen encrypted data. However, Port of Seattle refused to pay, making an official statement on how the payment of the ransom would go against the Port's values.


Seattle-Tacoma Intl. Airport
@flySEA

On Aug. 24, the Port of Seattle identified system outages consistent with a cyberattack. It was a fast-moving situation, and Port staff worked to quickly isolate critical systems.

Traduzir post

FIGURE 8: OFFICIAL SEA AIRPORT TWEET REPORTING CYBERATTACK


Port of Seattle/Seattle-Tacoma International Airport (SEA)

Port of Seattle/Seattle-Tacoma International Airport (SEA)

We publish SQL databases that have gone unclaimed by our customers. Additional data will be released at a later date. Please wait our updates.

Documents Data Catalog: 1.4 Tb, 79 432 Files

Not sold data was uploaded, data hunters, enjoy

Formed in 1911 and located in Seattle, Washington, Port of Seattle is a government agency that oversees Seattle's seaport and airport. The Port of Seattle is one of the nation's largest container ports and a critical US international trade gateway. 4th largest distribution center network in the U.S. One of fastest rail transits to Chicago of any West Coast port.

FIGURE 9: SCREENSHOT OF RHYSIDA'S DATA LEAK SITE

Im April 2025, Port of Seattle began notifying roughly 90,000 individuals of a data breach after their personal information was stolen in the August 2024 ransomware attack.[17]

The Rhysida ransomware emerged around May 2023 and is associated with a data leak site active since at least early June 2023. It is written in C++, and it encrypts files using ChaCha20 with randomly generated keys, which are then encrypted with a hard-coded RSA public key. A PowerShell variant, RHYSIDA.POWERSHELL, also exists. The ransomware iterates through attached drives, skipping specified directories and file types, and drops a ransom note calling themselves «cybersecurity team Rhysida».

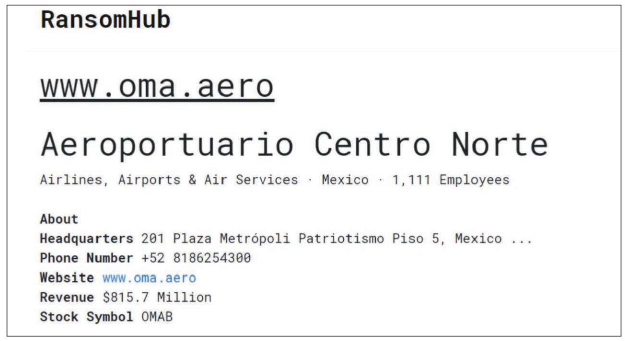
Furthermore, RHYSIDA.ESXI is a variant written in C that targets ESXi environments, encrypting local files and appending the «.rhysida» extension. It can take command-line arguments to specify encryption directories and modify the server's message of the day.

Both RHYSIDA and RHYSIDA.ESXI possess anti-VM capabilities, specifically targeting VMware. Key TTPs associated with RHYSIDA include Obfuscated Files or Information (T1027), Command and Scripting Interpreter (T1059), and Data Encrypted for Impact (T1486).

Later in the year, in October 2024, Grupo Aeroportuario Centro Norte (OMA), which operates 23 airports in Mexico, including major hubs, such as Monterrey, reported a cyber-attack that caused significant disruptions to its systems[18].

OMA's IT team had to revert to its backup systems to maintain operations across all the airports. Nevertheless, the airports were still down on some services, such as the flight terminal location screens.

In due course, the ransomware group RansomHub, claimed responsibility for the attack and, in their statement, threatened to release 3TB of stolen data if the requested ransom wasn't payed.


RansomHub

www.oma.aero

Aeroportuario Centro Norte

Airlines, Airports & Air Services · Mexico · 1,111 Employees

About
Headquarters 201 Plaza Metrópoli Patriotismo Piso 5, Mexico ...
Phone Number +52 8186254300
Website www.oma.aero
Revenue $815.7 Million
Stock Symbol OMAB

FIGURE 10: SCREENSHOT OF RANSOMHUB'S DATA LEAK SITE

[15] Seattle-Tacoma Intl. Aiport's X account, September 13, 2024, https://x.com/flySEA/status/1834675801117409745.

[16] «Critical infrastructure continues under threat, as hackers strike at Port of Seattle and Halliburton oilfield,» Industrial Cyber Security Solutions, August 26, 2024, https://industrialcyber.co/threat-landscape/critical-infrastructure-continues-under-threat-as-hackers-strike-at-port-of-seattle-and-halliburton-oilfield/.

[17] Port of Seattle says ransomware breach impacts 90,000 people," BleepingComputer, April 04, 2025, https://www.bleepingcomputer.com/news/security/port-of-seattle-says-ransomware-breach-impacts-90-000-people/.

[18] «OMA Informa Sobre Incidente de Ciberseguridad,» OMA - Grupo Aeroportuario Centro Norte, October 18, 2024, https://www.oma.aero/assets/005/6312.pdf.

Although OMA did not confirm the ransomware group's claims, it acknowledged that it was conducting appropriate investigations regarding the possible breach.[19]

RansomHub is written in Golang and can encrypt data using ChaCha20, xChaCha20, or AES256 algorithms, with the symmetric encryption key being per-file and protected by elliptic curve cryptography, ed25519. The group is capable of booting systems in safe mode, capturing system language, communicating using SMB, constructing mutexes, creating files and threads, deleting files, encoding using a custom Base64 alphabet, and encrypting or decrypting files.

In March 2025, the Kuala Lumpur Airport, in Malaysia, was also victim of a cyberattack. Although at first the official communications informed that only some systems had been affected and that the disruptions weren't significant, shortly after, travelers began to share their side of the story: the disabled airport's flight information display system, the disabled check-in counters, and the disabled baggage handling services, were forcing airlines and airport staff to rely on manual operations[20].

Afterwards, on a new official communication, the airport recognized the cyber-attack had had a significant impact within the airports, confirming the passengers experience.
The attackers targeted Malaysia Airports Holdings Berhad (MAHB), the company that runs most of the country's airports, and demanded a $10 million ransom.
The Malaysian Prime Minister Anwar Ibrahim confirmed that as soon as the ransom was requested, its payment was denied, claiming that the country would not comply with demands from traitors and criminals, whether they originate from within or outside the nation, further adding that the country and the system would never be safe if it did so[21]. The cyber-attack has not been publicly linked to any ransomware groups at the time of this writing.

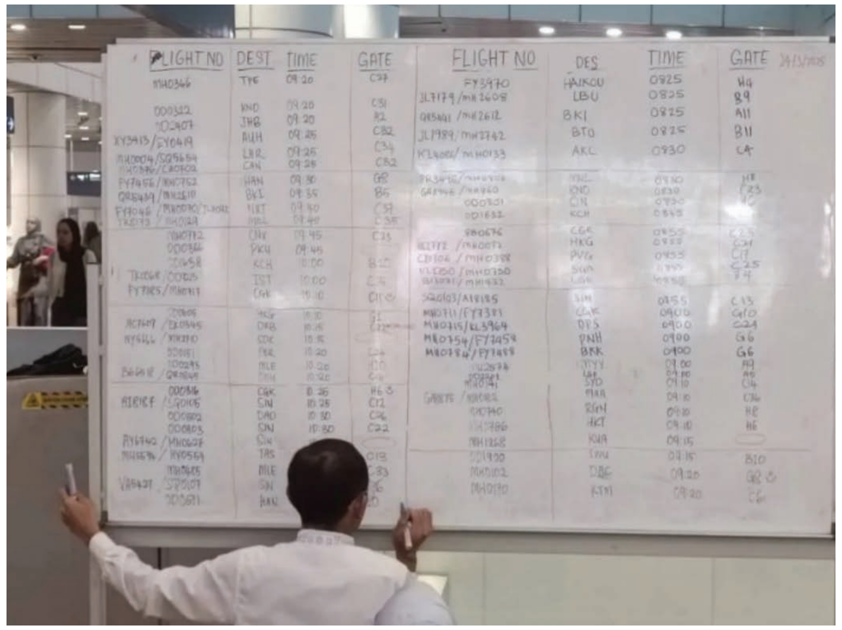


FIGURE 11: A WHITEBOARD USED TO TRACK FLIGHTS IN KUALA LUMPUR AIRPORT DURING THE OUTAGE (DARK READING)

HACKTIVISM

Hacktivism has re-emerged as a prominent cyber threat vector following Russia's full-scale invasion of Ukraine in February 2022. Since then, hacktivist activity has increasingly extended to other geopolitical and religious conflicts, notably the Israel–Hamas war that escalated in October 2023, or the India-Pakistan conflict in May 2025.

These events have catalyzed the involvement of a wide range of actors, from well-established hacktivist groups to lesser-known entities, driven largely by ideological or religious motivations.

The ongoing global instability has fueled a resurgence of hacktivist campaigns, often opportunistic in nature and designed to maximize media visibility. Many of these actors operate in support of specific narratives, such as anti-Israeli, pro-Palestinian, or pro-Hamas stances and have carried out cyberattacks including website defacements, Distributed Denial of Service (DDoS) attacks, and data leaks.

DDoS attacks, which aim to disrupt critical systems, are becoming an increasingly common tactic against the aviation sector, disrupting operations and, subsequently, causing financial losses.

DDoS attacks to target the aviation industry are attractive to cybercriminals since system availability is crucial for the normal occurrence of daily operations, given that airlines and airports rely on digital infrastructures for most operations, ticketing, baggage handling, flight information displays, and communication with other systems. A DDoS attack capable of provoking an outage on one of the systems causes chaos mainly withing the passengers, but also on the organization of operations, having effects such as delays and cancelations of flights.

The most common targets for DDoS attacks on the aviation industry are the ticketing and reservation systems, the baggage handling systems, the communication systems, the customer service portals and mobile application, and the flight information displays, as seen on the attack on Japan Airlines.

[19] “RansomHub gang allegedly behind attack on Mexican airport operator,” The Record, October 25, 2025, https://therecord.media/ransomhub-gang-behind-attack-mexican-airport-operator.

[20] «Malaysian Airport's Cyber Disruption a Warning for Asia,» Dark Reading, April 2, 2025, https://www.darkreading.com/cyberattacks-data-breaches/malaysian-airport-cyber-disruption-warning-asia.

These activities are commonly orchestrated and publicized through open Telegram channels and underground forums on the dark web, including BreachForums, XSS, DarkForums, Cracked, and LeakBase. Although many of the direct targets are located within the zones of conflict, hacktivist campaigns have also affected organizations in countries outside the immediate theatres of war due to their perceived political alignment or support for one of the parties involved.

In this context, the aviation sector has emerged as a high-profile, symbolically charged target, drawing increasing attention from ideologically motivated threat actors. The following section explores concrete examples of hacktivist campaigns directed at aviation organizations during 2024 and 2025.

In December 2024, Japan Airlines (JAL) suffered a cyber-attack, namely a DDoS attack in which the airline's systems became so overwhelmed in traffic that it was not possible to communicate with external networks. The attack led to JAL having to shut down the affected system, consequently suspending ticket sales and online services for passengers, given that the attack impacted the airline's mobile app, along with JAL's baggage management system[22].

The attack resulted in some delayed flights, but the airline company confirmed that costumer information was not accessed, as there was no sign of malware within the systems.[23]

Earlier in the year, in September 2024, Guarulhos International Airport (GRU), in São Paulo, Brazil, the busiest airport in the country, saw its official website down during a short period of time, however, according to the concessionaire of the airport, the page did not suffer any alterations, and the airports operations were not disrupted. Later, the attack was claimed by “Azael” a cybercriminal that had already been targeting other facilities in Brazil[24] [25].

In recent years, airports have increasingly become symbolic targets for hacktivist groups aiming to draw attention to geopolitical conflicts or ideological causes. These cyberattacks, often in the form of DDoS campaigns, are typically publicized by the threat actors themselves on social media or messaging platforms.

The table below highlights selected incidents where hacktivist groups have targeted airports with DDoS attacks, including known attribution and timing:

DATE	VICTIM	THREAT ACTOR	
14/04/2025	Nice Côte d'Azur Airport	Russian Partisan, Mr. Hamza	https://t.me/c/2586337929/61
14/04/2025	Paris Charles de Gaulle Airport	Russian Partisan, Mr. Hamza	https://t.me/c/2586337929/55
03/04/2025	John F. Kennedy International Airport	Dark Storm Team	https://t.me/DarkStormTeam3/160
28/12/2024	Milan Malpensa Airport	NoName057(16)	https://www.reuters.com/technology/cybersecurity/cyber-attack-italys-foreign-ministry-airports-claimed-by-pro-russian-hacker-2024-12-28/
28/12/2024	Milan Linate Airport	NoName057(16)	https://www.reuters.com/technology/cybersecurity/cyber-attack-italys-foreign-ministry-airports-claimed-by-pro-russian-hacker-2024-12-28/
24/05/2024	Milan Bergamo Airport	JUST EVIL	https://t.me/hackberegini/2290
23/05/2024	Montpellier–Méditerranée Airport	Dark Storm Team	https://x.com/DailyDarkWeb/status/1793582650537439447
22/05/2024	Hamburg Airport	JUST EVIL	https://t.me/hackberegini/2288
25/02/2024	Copenhagen Airport	NoName057(16)	https://x.com/CPHAirports/status/1761778731511648395

[21] “Malaysia PM says country rejected $10 million ransom demand after airport outages,” The Record, March 25, 2025, https://therecord.media/malaysia-pm-says-country-rejected-ransom-demand-airport-cyberattack.

[22] “Japan Airlines resumes operations after cyberattack delays flights,” The Record, December 26, 2024, https://therecord.media/japan-air22 lines-resumes-operations-after-cyberattack.

[23] ”Japan Airlines Restores Service After Cyberattack Disrupts Operations,” Aviation Source News, December 27, 2024, https://aviationsourcenews.com/japan-airlines-restores-service-after-cyberattack-disrupts-operations/.

[24] “Site da Força Aérea Brasileira está fora do ar; hacker assume ataque,” Olhar Digital, March 19, 2025, https://olhardigital.com.br/2025/03/19/seguranca/site-da-forca-aerea-brasileira-esta-fora-do-ar-hacker-assume-ataque.

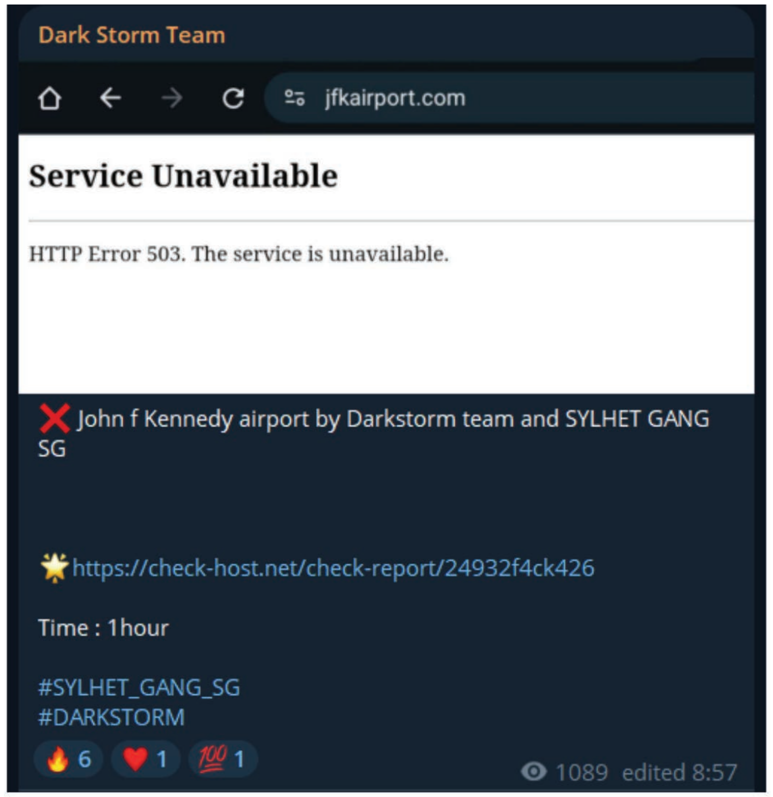
[25] “Site do Aeroporto de Guarulhos é alvo de ciberataque,” Security Leaders, September 14, 2024, https://securityleaders.com.br/site-do-aeroporto-de-guarulhos-e-alvo-de-ciberataque.

Below are examples of DDoS attack claims made by hacktivist groups on their Telegram channels, illustrating how these actors publicly take responsibility for cyberattacks against airports as part of their propaganda and influence operations:

While Distributed Denial-of-Service (DDoS) attacks aim to disrupt access to online services, hacktivists often complement these efforts with defacement attacks — a tactic that involves the unauthorized modification of official digital interfaces. These attacks are typically used to convey political or ideological messages by replacing legitimate content with propaganda, slogans, or offensive imagery, often targeting public-facing systems to maximize visibility.

A notable example occurred in May 2025, when a hacker identifying as a member of Anonymous targeted Global Crossing Airlines Group (GlobalX), a U.S.-based airline involved in deportation flights for U.S. Immigration and Customs Enforcement (ICE)[28].

The attacker defaced the airline's website with a politically charged message — an act designed to publicly shame and delegitimize the company — before allegedly stealing and leaking flight records and passenger manifests linked to deportation operations. The incident was later confirmed in a filing with the U.S. Securities and Exchange Commission (SEC), although the company stated that its core operations were not disrupted.



Dark Storm Team

jfkairport.com

Service Unavailable

HTTP Error 503. The service is unavailable.

❌ John f Kennedy airport by Darkstorm team and SYLHET GANG SG

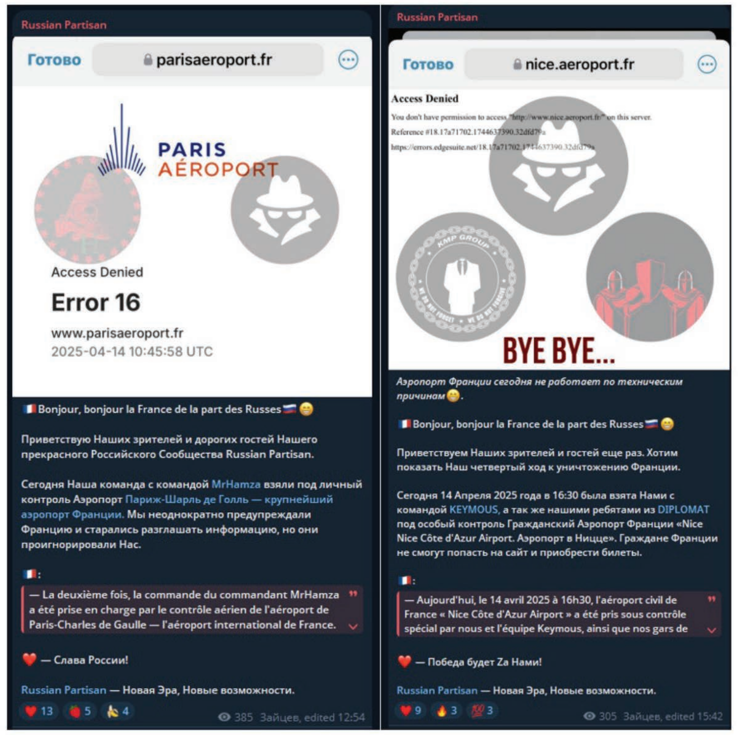
🌟https://check-host.net/check-report/24932f4ck426

Time : 1hour

#SYLHET_GANG_SG
#DARKSTORM

🔥 6 ❤️ 1 💯 1 👁 1089 edited 8:57

FIGURE 12: DARK STORM TEAM CLAIMS DDOS ATTACK ON JOHN F. KENNEDY AIRPORT[26]



Russian Partisan

Готово parisaeroport.fr

Access Denied

Error 16

www.parisaeroport.fr
2025-04-14 10:45:58 UTC

🇫🇷 Bonjour, bonjour la France de la part des Russes🇷🇺😁

Приветствую Наших зрителей и дорогих гостей Нашего прекрасного Российского Сообщества Russian Partisan.

Сегодня Наша команда с командой MrHamza взяли под личный контроль Аэропорт Париж-Шарль де Голль — крупнейший аэропорт Франции. Мы неоднократно предупреждали Францию и старались разглашать информацию, но они проигнорировали Нас.

🇫🇷:

> — La deuxième fois, la commande du commandant MrHamza a été prise en charge par le contrôle aérien de l'aéroport de Paris-Charles de Gaulle — l'aéroport international de France.

❤️ — Слава России!

Russian Partisan — Новая Эра, Новые возможности.

❤️ 13 🍅 5 🍌 4 👁 385 Зайцев, edited 12:54

Russian Partisan

Готово nice.aeroport.fr

Access Denied

You don't have permission to access "http://www.nice.aeroport.fr/" on this server.

Reference #18.17a71702.1744637390.32dfd79a

https://errors.edgesuite.net/18.17a71702.1744637390.32dfd79a

Аэропорт Франции сегодня не работает по техническим причинам😁.

🇫🇷 Bonjour, bonjour la France de la part des Russes🇷🇺😁

Приветствуем Наших зрителей и гостей еще раз. Хотим показать Наш четвертый ход к уничтожению Франции.

Сегодня 14 Апреля 2025 года в 16:30 была взята Нами с командой KEYMOUS, а так же нашими ребятами из DIPLOMAT под особый контроль Гражданский Аэропорт Франции «Nice Nice Côte d'Azur Airport. Аэропорт в Ницце». Граждане Франции не смогут попасть на сайт и приобрести билеты.

🇫🇷:

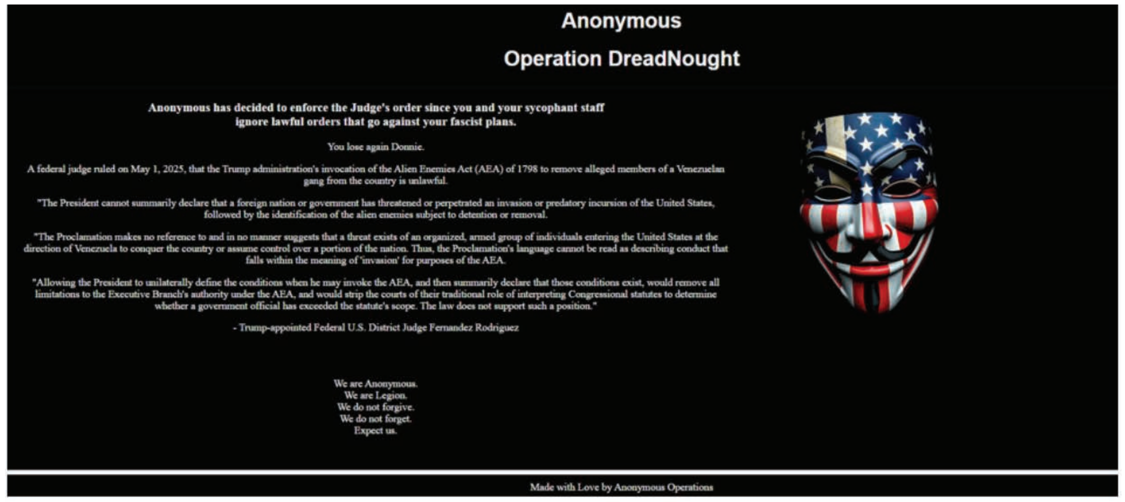
> — Aujourd'hui, le 14 avril 2025 à 16h30, l'aéroport civil de France « Nice Côte d'Azur Airport » a été pris sous contrôle spécial par nous et l'équipe Keymous, ainsi que nos gars de

❤️ — Победа будет Za Нами!

Russian Partisan — Новая Эра, Новые возможности.

❤️ 9 🔥 3 💯 3 👁 305 Зайцев, edited 15:42

FIGURE 13: RUSSIAN PARTISAN CLAIMS DDOS ATTACKS ON FRENCH AIRPORTS[27]



Anonymous

Operation DreadNought

Anonymous has decided to enforce the Judge's order since you and your sycophant staff ignore lawful orders that go against your fascist plans.

You lose again Donnie.

A federal judge ruled on May 1, 2025, that the Trump administration's invocation of the Alien Enemies Act (AEA) of 1798 to remove alleged members of a Venezuelan gang from the country is unlawful.

"The President cannot summarily declare that a foreign nation or government has threatened or perpetrated an invasion or predatory incursion of the United States, followed by the identification of the alien enemies subject to detention or removal.

"The Proclamation makes no reference to and in no manner suggests that a threat exists of an organized, armed group of individuals entering the United States at the direction of Venezuela to conquer the country or assume control over a portion of the nation. Thus, the Proclamation's language cannot be read as describing conduct that falls within the meaning of 'invasion' for purposes of the AEA.

"Allowing the President to unilaterally define the conditions when he may invoke the AEA, and then summarily declare that those conditions exist, would remove all limitations to the Executive Branch's authority under the AEA, and would strip the courts of their traditional role of interpreting Congressional statutes to determine whether a government official has exceeded the statute's scope. The law does not support such a position."

- Trump-appointed Federal U.S. District Judge Fernandez Rodriguez

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
Expect us.

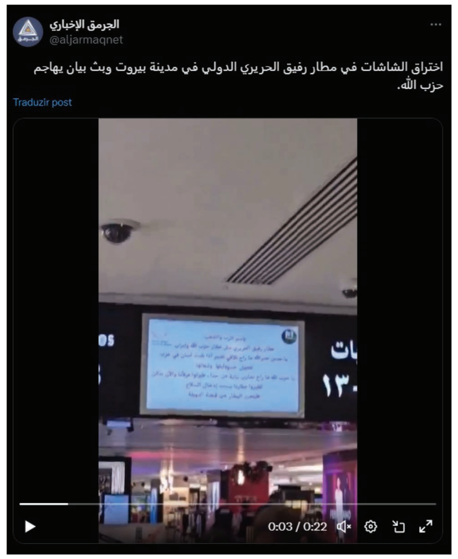
Made with Love by Anonymous Operations

FIGURE 14: GLOBALX'S DEFACED WEBSITE[29]

On the other hand, in January 2025, the Beirut-Rafic Al Hariri International Airport (BEY) suffered a politically motivated cyberattack that disrupted several operations. The hackers used the departure and arrival screens of the airport to display a statement accusing Hezbollah, the Iran-backed militant group, of escalating tensions between Israel and Lebanon. The cybercriminals did so by replacing the flight's data with several messages, one being "You bear your responsibility and its consequences, Hezbollah.[30]

The attack is a consequence of the geopolitical tensions between Lebanon and Israel, which have been escalating, with fire exchanges between both. On the day of the attack, an Israeli airstrike is said to have killed a senior commander form Hezbollah.[32]
The cyberattack resulted in a brief disruption of the airport's baggage inspection system, and the authorities supposedly disconnected the systems from the internet to limit further damage.

According to ongoing investigations, there are two possible groups being suspected "The One Who Spoke" and "Soldiers of God", however, the latter has already dismissed its involvement.



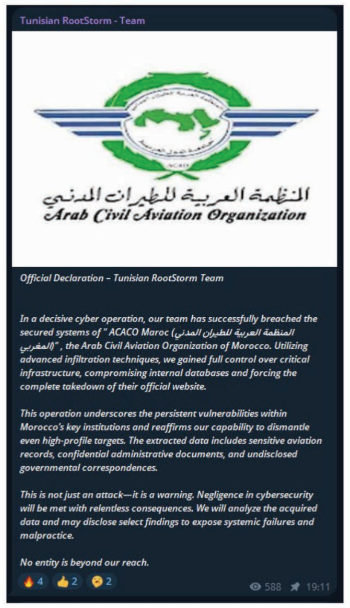
الجرمق الإخباري
@aljarmaqnet

اختراق الشاشات في مطار رفيق الحريري الدولي في مدينة بيروت وبث بيان يهاجم
حزب الله.

Traduzir post

FIGURE 15 : HACKED SCREENS AT RAFIK HARIRI AIRPORT SHOW A STATEMENT AGAINST HEZBOLLAH[31]

In addition to disruptive operations such as DDoS and defacement, hacktivist actors also engage in more sophisticated forms of cyber aggression, including network intrusions and data breaches. These attacks often target governmental or aviation-related institutions and aim to extract and potentially leak sensitive information. In doing so, hacktivist groups seek to expose what they perceive as institutional weaknesses or political misconduct, using the stolen data as leverage or propaganda.
A notable example involves the group «Tunisian RootStorm», which publicly claimed responsibility for breaching the Arab Civil Aviation Organization of Morocco:



Tunisian RootStorm - Team

المنظمة العربية للطيران المدني
Arab Civil Aviation Organization

Official Declaration – Tunisian RootStorm Team

In a decisive cyber operation, our team has successfully breached the secured systems of " ACACO Maroc (المنظمة العربية للطيران المدني المغربي)" , the Arab Civil Aviation Organization of Morocco. Utilizing advanced infiltration techniques, we gained full control over critical infrastructure, compromising internal databases and forcing the complete takedown of their official website.

This operation underscores the persistent vulnerabilities within Morocco's key institutions and reaffirms our capability to dismantle even high-profile targets. The extracted data includes sensitive aviation records, confidential administrative documents, and undisclosed governmental correspondences.

This is not just an attack—it is a warning. Negligence in cybersecurity will be met with relentless consequences. We will analyze the acquired data and may disclose select findings to expose systemic failures and malpractice.

No entity is beyond our reach.

🔥 4 👍 2 😥 2 👁 588 19:11

FIGURE 16: TUNISIAN ROOTSTORM CLAIMS A DATA BREACH ON ACACO MAROC[33]

[26] https://t.me/DarkStormTeam3/160.
[27] https://t.me/c/2586337929/55, https://t.me/c/2586337929/61.
[28] "Airline carrying out deportation flights confirms cyberattack to SEC," The Record, May 12, 2025, https://therecord.media/airline-carrying-out-deportation-flights-confirms-cyberattack-sec.

[29] https://web.archive.org/web/20250505140730/https://foqa.globalxair.com/.
[30] "Hackers disrupt Beirut airport with anti-Hezbollah message," The Record, January 8, 2024, https://therecord.media/beirut-airport-hack-information-screens-baggage-screening.
[31] https://x.com/aljarmaqnet/status/1744049633838391755.
[32] "Beirut Airport screens hacked with message to Nasrallah," L'Orient Today, January 7, 2024, https://today.lorientlejour.com/article/1363491/bia-screens-hacked-with-message-to-nasrallah.html.
[33] https://t.me/TunisanRootStorm/925.

STATE-SPONSORED

The aviation sector, with its critical technologies, economic value, and strategic importance, is a prime target for cyberespionage. The sector is inherently intertwined with national security interests, as both military aviation and civilian play essential roles in shaping global power dynamics. Countries with advanced aviation technologies and manufacturers, such as the U.S., Russia, and France, are at the forefront of cyber espionage campaigns, especially those with significant geopolitical interests.

The aviation industry spans various segments, including aircraft manufacturing, defense contracting, air traffic control systems, and aviation technology research. These areas are not only valuable economically but also form the backbone of military operations, logistics, and defense strategies in global conflicts.

Russian APTs

Russia, through its cyber operations and Advanced Persistent Threat (APT) groups, such as ATK5 (Fancy Bear, APT28) and ATK7 (Cozy Bear, APT29), has long utilized cyberattacks as a means of geopolitical warfare. These groups have been implicated in numerous campaigns targeting NATO nations.

- *ATK5 (APT28)*

ATK5 (APT28), also known by various aliases including Fancy Bear, STRONTIUM, and Sednit, remains one of the most prolific Russian state-sponsored cyber threat actors. Since its emergence in 2007, it has demonstrated a consistent interest in strategic targets aligned with the Kremlin's geopolitical and military objectives.

Over the past three years, coinciding with Russia's full-scale invasion of Ukraine, APT28 has evolved its methods and broadened its scope, increasingly targeting entities in the aviation and aerospace sectors, both for espionage and strategic disruption. Recent investigations show that APT28's tactics now include advanced lateral movement via wireless access, exploitation of insecure satellite networks, and phishing campaigns against defense contractors and aviation authorities. These developments suggest a deliberate shift from traditional espionage operations toward hybrid cyber warfare, aimed at degrading Western military readiness and technological superiority in critical domains such as air traffic control and space-based communication.

On September 1, 2024, Germany's air traffic control agency, DFS (Deutsche Flugsicherung), reported a cyberattack targeting its administrative IT systems. Although air traffic operations remained unaffected, the compromise of internal office communications raised serious concerns about potential future disruptions.

German cybersecurity authorities attributed the attack to APT28, marking it as part of a broader campaign by the group against German critical infrastructure[34].

This incident cannot be viewed in isolation. It coincided with other confirmed APT28 operations targeting members of Germany's ruling Social Democratic Party, as well as aerospace and defense contractors, over the prior two years[35]. The group reportedly exploited a vulnerability in Microsoft Outlook to access sensitive email accounts.

The DFS breach represents an evolution in targeting—while air traffic systems were not directly hit, the proximity to operational infrastructure indicates a potential reconnaissance or preparatory phase for more impactful operations.

Also, while initially attributed to solar activity, a 2015 event that saw Sweden's entire airspace closed for over an hour is now suspected to have been the result of a cyberattack by APT28[36].

Iranian APTs

- *ATK49 (TA455/ UNC1549)*

An operation tracked as perpetrated by ATK49 (TA455), a subgroup of APT35, was discovered at the end of 2024. The espionage campaign had as its main target the aerospace industry and the semi-conductor's sector. The operation worked as a fake worker scheme, which is usually attributed to North Korean cyber threat groups and was recorded as the «Dream Job» campaign - giving that the threat group manipulates its targets by offering them a «dream job» in the aerospace industry[37].

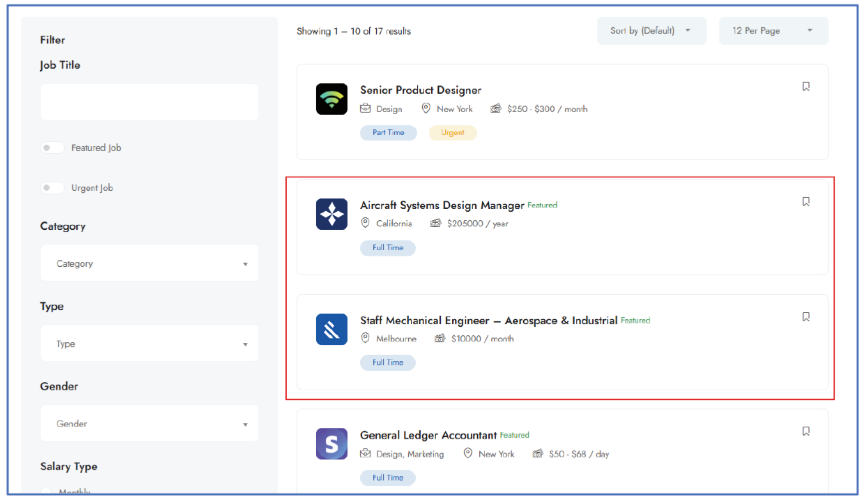
Seeing as the tactics to this operation are significantly like the campaigns perpetrated by the North Korean APT, Lazarus, two options regarding the operation were considered: the APT35 impersonated the Lazarus group to conceal its identity, or there was an exchange of knowledge between both groups.

The «Dream Job» campaign was followed since September 2023, having been carried out until the end of 2024, with the LinkedIn profiles associated with the most recent activity being the same as the one's in 2023. For example, one fake profile associated with the fake company «Careers 2 Find», had previously «worked» for the fake recruiting website, that had already been uncovered, «1st Employer».

The campaign showed the sophistication of the threat group and its capabilities for social engineering. At first, by impersonating other threat actors, the threat group is able to remain unidentified for longer, creating confusion, furthermore, the threat group hosts their malicious domains on legitimate online services, such as Cloudflare, as exploit others like GitHub to host encoded C2 server information to then retrieve it.

As a social engineering tactic, the use of LinkedIn profiles allows the threat actor to gain trust and credibility from targets, avoiding suspicion, seeing as upon consultation, the profiles appear to be real people working in real companies - this tactic allows the threat group to bypass certain measures, such as identifying the email as suspicious. That being said, the operation worked with a multi-infection process initiating with spear-phishing emails with malicious attachments masquerading as job-related files, containing ZIP files within themselves with various malicious and legitimate files - in order to bypass security measures and to trick victims into executing the malware - the malware used, designed to evade detection, and the infrastructure is constantly adapting, making it difficult to identify and mitigate for researchers. Furthermore, the recruiting websites, when accessed would offer a PDF file to download, containing malicious files, promoting it as a guide for the safe utilization of the website.

The campaign, by having specific targets, as can be observed by the above images, the jobs related to aerospace, aviation and defense systems appear much more appealing in comparison to the others, demonstrates an interest by the Iranian state in acquiring information within the industries or even cause disruption to these critical sectors



Filter
Job Title
Featured Job
Urgent Job
Category
Category ▾
Type
Type ▾
Gender
Gender ▾
Salary Type
Monthly

Showing 1 – 10 of 17 results
Sort by (Default) ▾
12 Per Page ▾

Senior Product Designer
Design · New York · $250 - $300 / month
Part Time · Urgent

Aircraft Systems Design Manager Featured
California · $205000 / year
Full Time

Staff Mechanical Engineer – Aerospace & Industrial Featured
Melbourne · $10000 / month
Full Time

General Ledger Accountant Featured
Design, Marketing · New York · $50 - $68 / day
Full Time

FIGURE 17: FAKE JOB POSTS FOR AEROSPACE EMPLOYEES

North Korean APTs

The above-mentioned "Dream Job" campaign was not the first campaign targeting job seekers in the aviation industry. In June 2020, a similar campaign probably linked to the North Korean ATK3 (Lazarus Group), was discovered.

During the campaign, the North Korean cyber group successfully deceived their targets using fraudulent job offers. These offers appeared to come from top U.S. defense and aerospace companies, including Boeing, Lockheed Martin, and BAE Systems. The attackers conducted a sophisticated and far-reaching social engineering operation that involved reconnaissance, the creation of fake LinkedIn profiles, emails sent to personal addresses, and prolonged direct communication with the victims via phone and WhatsApp[38].

Once the victims' systems were compromised, the attackers gathered intelligence on both company operations and financial matters, likely with the dual aim of espionage and financial theft. This combination of spying and monetary theft is characteristic of North Korean operations, where cyber units are tasked with acquiring both strategic information and financial resources for the state.

In September 2019, a similar campaign was discovered, named Operation In(ter)ception, also possibly linked to ATK3 (Lazarus Group) and targeting aviation and aerospace companies in the Middle East and Europe. The files were sent directly via LinkedIn messaging, or via email containing a OneDrive link. After a successful attack, the attackers attempted to use the victim's compromised corporate account to lure money from other companies, sending fake invoices or asking for a due payment notice[39].

Chinese APTs

As of 2025, the International Civil Aviation Organization, a United Nations agency responsible for setting standards for international aviation safety and security, is investigating a recently found data breach, that was claimed on January 5 on a hacking forum.

According to the post, the threat actor had access to 42,000 documents belonging to ICAO, including personal information. The data breach is said to have affected 11,929 individuals, that saw their recruitment-related information, such as names, email addresses, dates of birth, and job history accessed.

In this cyberattack, the hackers were not interested in disrupting the company in operational terms – they didn't target IT/OT processes – but in gathering intelligence on specific individuals – a tactic of traditional espionage.

Although attributions of the attack remain speculative, researchers believe to it originating from a state-sponsored group linked to China[40].

In a similar attack, shortly after the ICAO data breach, shared on a hacking forum on February 4, the Arab Civil Aviation organization suffered a cyber-attack: documents with records of members and their credentials were exfiltrated form the ACAO systems – thanks to a successful SQL injection exploita-

[34] «Is Russian group APT28 behind the cyber attack on the German air traffic control agency (DFS)?,» Security Affairs, September 05, 2024, https://securityaffairs.com/168070/apt/apt28-cyber-attack-german-air-traffic-control-agency-dfs.html.

[35] «APT 28 group is ramping up information warfare against Germany,» Security Affairs, December 10, 2016, https://securityaffairs.com/54252/intelligence/apt-28-infowar-germany.html.

[36] «Sweden's airspace shut down by Russian APT, not a solar storm,» SC Media, April 13, 2016, https://www.scworld.com/news/swedens-airspace-shut-down-by-russian-apt-not-a-solar-storm.

[37] «Iranian "Dream Job" campaign,» ClearSky Cyber Security Ltd., November 2024, https://www.clearskysec.com/wp-content/uploads/2024/11/Iranian-Dream-Job-ver1.pdf.

[38] «Operation 'Dream Job',» ClearSky Cyber Security Ltd., August 2020, https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf.

[39] «Operation In(ter)ception: Targeted Attacks Against European Aerospace and Military Companies,» ESET, June 2020, https://web-assets.esetstatic.com/wls/2020/06/ESET_Operation_Interception.pdf.

[40] "Cyberespionage groups target ICAO, ACAO — threaten global aviation safety", Biometric Update, February 6, 2025, https://www.biometricupdate.com/202502/cyberespionage-groups-target-icao-acao-threaten-global-aviation-safety.

tion in a vulnerable web application.

The affected individuals were Safety Aviation Specialists and Incident Investigators, representatives of the Qatar Aircraft Accident and Incident Investigation Unit (QAAI), the Aviation Investigation Bureau (AIB) of the Kingdom of Saudi Arabia, the Iran Civil Aviation Authority, the Jordan Civil Aviation Regulatory Commission (CARC), and various members of the Aviation Accident Investigation Division (AAID). Therefore, highly regarded individuals involved in sensitive communications related to the field, and with access to first-hand knowledge – these victims saw their includes logins (usernames), hashes of passwords, emails, titles, and communications, exposed.

However, there is still no speculation regarding the origin of the attack on ACAO. Nevertheless, both attacks are being attributed to state-sponsored groups, particularly because researchers believe that traditional cybercriminals would not have interest in the breached documents, therefore the speculation on the perpetrators remains on state-sponsored actors, which have used the information to pursuit other cyber espionage campaigns[41].

- *ATK2 (APT41)*

ATK2 (APT41), a Chinese APT also known as Wintti, Double Dragon, and Barium, has been conducting a cyberattack campaign since 2023, targeting transportation organizations in Europe, Asia, and the Middle East. The objective of APT41 is to infiltrate the systems of transportation companies, maintain access to compromised networks, and steal sensitive information. Their methodology employs advanced tools that enable persistent intrusion and data theft.

The aviation sector is particularly vulnerable to these attacks, as it is a critical infrastructure that relies on complex IT systems and interconnected networks. APT41 has demonstrated its ability to exploit these vulnerabilities to gain access to key information. Moreover, with its persistent attack capabilities, the group can continue exploiting systems for extended periods without being detected.
As of February 2025, a campaign exploiting the Check Point vulnerability CVE-2024-24919—reported and patched in May 2024—was observed stealing user credentials to gain initial access via VPN logins using valid accounts. The activity has been attributed, with low confidence, to APT41.

The campaign resulted in various organizations being affected – around thirty – all over the world, but mainly in the United States of America and Latin America. Many of the targeted organizations were significant supply chain manufacturers to aviation and aerospace companies[42].

After gaining initial access, they then used RDP or SMB to travel laterally and perform network scanning to obtain greater privileges, primarily connecting to the Domain Controller. Using the DLL Sideloading approach, attackers ran genuine apps to load malicious DLLs, unintentionally infecting victims' computers with ShadowPad malware, which communicates with a remote server to create continuous remote access to target PCs and employs sophisticated obfuscation and anti-debugging tactics. On some occasions, in addition to the ShadowPad infections, the threat group also deployed the NailaoLocker ransomware[43].

_Analyst's observation

The aviation sector continued to face a complex and evolving cyber threat landscape throughout 2024 and into 2025. Threat actors ranging from financially motivated cybercriminals to ideologically driven hacktivist groups and state-sponsored adversaries increasingly targeted aviation due to its strategic value, operational complexity, and high dependency on interconnected digital systems.
Business Email Compromise (BEC) attacks remained a persistent threat, often exploiting trusted internal communications to conduct financial fraud. Notable incidents included the spoofing of an aviation firm in the EMEA region.
Supply chain attacks also surged, exploiting vulnerabilities in third-party relationships. The compromise of SunExpress via a newsletter service provider exposed data of 250,000 customers, while a failed software update from cybersecurity vendor CrowdStrike led to operational paralysis at Delta Air Lines, underscoring the fragility of aviation's digital dependencies.
Ransomware continued to exert significant operational and financial pressure. Although the total number of ransomware incidents dropped from 30 in 2023 to 19 in 2024, a resurgence has been observed in early 2025 with 8 attacks recorded by the beginning of May, 6 of which occurred in Q1 alone, suggesting a steep upward trend. These attacks spanned at least 16 countries, with the United States accounting for over a third of recorded incidents. Groups such as Space Bears, LockBit, and Rhysida were among the most active.
Hacktivism re-emerged with intensity, fueled by global conflicts such as the Russia-Ukraine war, the Israel-Hamas escalation, and India–Pakistan tensions.
All four major adversary blocs: Russia (APT28), Iran (TA455), China (APT41 and affiliates), and North Korea (Lazarus), are investing in long-term campaigns that reach beyond classic defense espionage into civilian air-traffic and supply-chain systems. That shift signals that attackers view disruption of air-transport services and the theft of aviation R&D as high-leverage levers in geopolitical competition.
Altogether, the events of 2024 and 2025 reaffirm the aviation industry's status as a high-value cyber target, where financial incentives, geopolitical rivalry, and ideological agendas converge. The sector's increasing digitalization and operational interdependence presents both opportunities for innovation and expanding attack surfaces, demanding heightened resilience and sustained threat monitoring across all layers of the aviation ecosystem.

[41] "Cyberespionage groups target ICAO, ACAO — threaten global aviation safety", Biometric Update, February 6, 2025, https://www.biometricupdate.com/202502/cyberespionage-groups-target-icao-acao-threaten-global-aviation-safety.
[42] "Chinese APT Uses VPN Bug to Exploit Worldwide OT Orgs," Dark Reading, February 27, 2025, https://www.darkreading.com/ics-ot-security/chinese-apt-vpn-bug-worldwide-ot-orgs.
[43] "Patch Now: Check Point Research Explains Shadow Pad, NailaoLocker, and its Protection, " February 21, 2025, https://www.scrible.com/view/source/R2IO1C0L20LQG2MG3443K8O48P4CM20E:1424161239/.

_3 Most used attack techniques

A comprehensive understanding of the techniques leveraged by threat actors is essential for aviation stakeholders to detect, respond to, and mitigate cyber threats. This section examines the most frequently observed tactics, techniques, and procedures (TTPs) used in attacks against the aviation sector, based on recent case studies and threat intelligence reporting. Emphasis is placed on initial access methods, malware deployment, and the abuse of legitimate services for persistence and evasion. These insights help identify behavioral patterns and technical vulnerabilities commonly exploited in the industry.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

Cyber operations against aviation entities are driven by different types of threat actors: state-sponsored groups, ransomware groups, hacktivist collectives, etc. Each actor type brings its own methodology and TTPs, but all exploit the sector's technological complexity and heavy reliance on third-party vendors. Below is a breakdown of the most common techniques observed in aviation cyberattacks, mapped to MITRE ATT&CK tactics and illustrated with real-world use cases.

MITRE TACTIC	TECHNIQUE (ID)	EXAMPLE IN AVIATION
Initial Access	Phishing (T1566.001)	The 8BASE ransomware group likely entered Saudia Technic's (the maintenance, repair and overhaul division of Saudi Arabian Airlines) systems through phishing emails[44].
	Social Network Persona (T1341)	Fake recruiter profiles on LinkedIn used to target Airbus subcontractors[45]
	Supply Chain Compromise (T1195)	In 2024, SunExpress, a Turkish-German airline, reported that approximately 250,000 customers were affected by a data breach stemming from a cyberattack on a third-party service provider responsible for email newsletter distribution[46].
	Exploit Public-Facing Application (T1190)	In 2023, Honeywell — a major aerospace and aviation systems provider — was impacted by the mass exploitation of a zero-day vulnerability in MOVEit Transfer software, exploited by the Clop ransomware group[47].
	Command and Scripting Interpreter (T1059)	In March 2024, PLAY ransomware attacked Continental Aerospace Technologies by executing scripts to encrypt systems.
Execution	Scheduled Task/Job (T1053)	Sosano malware maintained persistence in airport systems in the UAE using scheduled tasks[48].
Persistence	Data Encrypted for Impact (T1486)	In February 2024, 8BASE ransomware encrypted critical systems at Saudia Technic, disrupting maintenance operations.
Impact	Hamburg Airport	JUST EVIL
25/02/2024	Copenhagen Airport	NoName057(16)
	Network Denial of Service (T1498)	In February 2024, the Dark Storm Team launched a DDoS attack against Los Angeles International Airport (LAX), taking web services offline.

[44] "The Aviation and Aerospace Sectors Face Skyrocketing Cyber Threats," Resecurity, March 15, 2024, https://www.resecurity.com/blog/article/the-aviation-and-aerospace-sectors-face-skyrocketing-cyber-threats.
[45] Airbus' LinkedIn account, 2019, https://www.linkedin.com/posts/airbusgroup_attention-we-are-aware-that-some-scam-messages-activity-6524629357946761216-6HcK/.
[46] "Cyberangriff auf IT-Dienstleister betrifft 250.000 Sun-Express-Kunden," July 24, 2024. https://www.airliners.de/cyberangriff-it-dienstleister-betrifft-250000-sun-express-kunden/75768.
[47] "Honeywell confirms impact by MOVEit hacks," November 15, 2025, https://cybernews.com/news/honeywell-confirms-impact-moveit-hacks-clop/.
[48] "Call It What You Want: Threat Actor Delivers Highly Targeted Multistage Polyglot Malware," March 4, 2025, https://www.proofpoint.com/us/blog/threat-insight/call-it-what-you-want-threat-actor-delivers-highly-targeted-multistage-polyglot.

_4 Prospective

The increasingly tenuous link between geopolitical dynamics and aviation activities is transforming the industry into a strategic, even conflict-ridden, space. The war in Ukraine, tensions in the Gulf and the Indo-Pacific, and the military use of civilian infrastructures are all positioning aviation players as targets of divergent interests. Aviation is thus becoming a technological extension of geopolitical tensions, exposing its digital systems to acts of sabotage, espionage or show of force.`

The trends observed in 2024 and early 2025 confirm the anchoring of the aviation sector in cybercriminal and state concerns. Business Email Compromise (BEC) attacks against European companies in the sector, sophisticated phishing campaigns, and indirect attacks via the supply chain reveal a growing maturity of offensives. These actions also demonstrate the quest for maximum leverage: achieving maximum disruption with a targeted effort. The trend is amplified by a renewed wave of ransomware and the active presence of state-sponsored APTs from Russia, China, Iran and North Korea, whose operations now edge into sabotage and industrial espionage.

From a technical standpoint, attackers are adapting their methods to match the sector's complexity. Privilege escalation, hijacking of industrial protocols, attacks on embedded technologies, and compromises of satellite services or reservation systems all demonstrate that threats are now capable of operating in hybrid environments that blend IT, OT, and critical systems. This intersection of high technical sophistication and operational criticality creates an ideal attack surface for APTs and organized cybercriminal groups.

Looking ahead, the convergence of geopolitical pressures, technical sophistication, and economic or ideological motivations will further increase the vulnerability of the aviation sector. We can anticipate larger-scale scenarios: coordinated attacks aimed at disrupting airport logistics chains, compromise of air traffic management systems, or hybrid threats combining disinformation and digital sabotage.

Conclusion

_A Shared Mission: Building a Resilient Aviation Ecosystem

Cybersecurity in aviation is not a destination, it's a continuous flight path through an ever-evolving threat landscape. As air travel becomes more connected, digital and critical to geopolitical dynamics, cyber risk is no longer a future scenario, it's a present reality.

From ransomware attacks on global airports to state-backed campaigns targeting airlines aligned with diplomatic adversaries, the sector is under pressure. But with the right cyber threat intelligence, collaborative regulation, and proactive defenses, resilience is within reach.

Thales is committed to helping Airlines, Air Navigation Service Provider (ANSP), and Airports navigate this complex environment. Our global expertise, award-winning capabilities (including the Frost & Sullivan Cybersecurity for Airports Award), and strategic alliances with regulators and operators make us your trusted partner in aviation cybersecurity. By anticipating threats, sharing anonymized incident data and contributing to key standards at EUROCAE and ICAO, we're not just monitoring cyber threats—we're actively shaping a safer future for global aviation.
Let's take off together—resilient, compliant, and secure.

For further information
please contact us:

cds.thalesgroup.com

THALES
Building a future we can all trust

cds.thalesgroup.com/cyberthreat-hitmap

© 2025 – Création Agence ID Deux Points pour Cyber Threat Intelligence – Thales – www.iddeuxpoints.com – Crédits photos : Shutterstock