SOCRadar®
Your Eyes Beyond

Industry Threat Landscape Report

AVIATION

SOCRadar®
Your Eyes Beyond

Table of Contents

Introduction 3
Notable Incidents 4
Recent Incidents 7
Dark Web Radar: Tracking Cyber Threats in the Aviation Industry 11
Ransomware Threat Insights in the Aviation Industry 16
DDoS Attacks in the Aviation Industry: A Rising Cyber Threat 21
Navigating Supply Chain Cyber Threats in the Aviation Industry 24
Conclusion 29

1. Introduction

In an era where digitalization and connectivity are at the forefront of the Aviation Industry's evolution, the sector stands at a crucial juncture, facing unprecedented cyber threats that challenge its operational integrity and security.

This report delves into the intricate cyber threat landscape that the Aviation Industry navigates, marked by a series of sophisticated cyberattacks that not only highlight the sector's vulnerabilities but also underscore the urgent need for robust cybersecurity measures. From the alarming SITA data breach affecting millions of travelers to the disruptive ransomware attacks on aviation supply chains, each incident provides a stark reflection of the evolving tactics employed by cybercriminals.

As the industry grapples with these challenges, it becomes imperative to adopt a holistic approach to cybersecurity, one that encompasses regular system audits, proactive threat intelligence, and a collaborative stance towards enhancing digital defenses.

2. Notable Incidents

The Aviation Industry has been under continuous threat from sophisticated cyber attacks, ranging from data breaches involving millions of passenger records to ransomware attacks targeting aviation supply chain entities. Each incident showcases the evolving tactics and sophistication of threat actors keen on exploiting vulnerabilities within this sector.

2.1 SITA Data Breach (2021)

Threat Actors: Not explicitly identified but indicative of sophisticated cybercriminals targeting the Aviation Industry.

Attack Method: Likely a sophisticated cyber intrusion targeting SITA's Passenger Service System, which processes a significant amount of sensitive passenger data.

Description: This breach exposed passenger service data, including frequent flyer program card numbers and status levels, potentially impacting over 2 million travelers worldwide. The incident highlighted the vulnerabilities in the complex supply chains and IT systems of the global Aviation Industry.

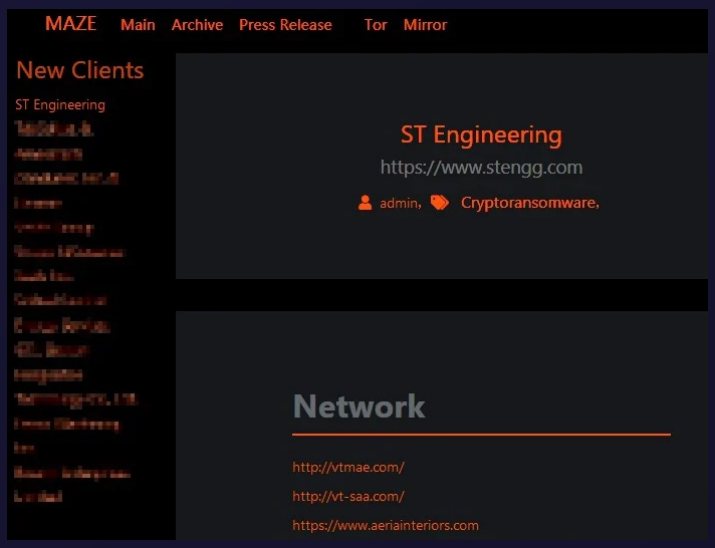
2.2 EasyJet Cyberattack (2020)

Threat Actors: Not clearly identified, but the attack bore the hallmarks of a highly sophisticated cybercriminal operation.

Attack Method: Targeted attack against EasyJet's customer database to extract personal and payment information.

Description: The breach led to the theft of credit card details of 2,208 customers and prompted a class-action lawsuit, highlighting the ongoing cybersecurity challenges faced by airlines in protecting customer data.

2.3 VT San Antonio Aerospace Ransomware Attack (2020)



Source: bleepingcomputer.com

Threat Actors: Maze Ransomware Group, known for their "double extortion" tactic of encrypting victim's files and then demanding a ransom to decrypt them, coupled with threatening to release stolen data if the ransom is not paid.

Attack Method: Deployment of Maze ransomware to encrypt files across VT San Antonio Aerospace's network, coupled with data theft.

Description: This ransomware attack not only disrupted VT San Antonio Aerospace's operations but also led to the theft of 1 terabyte of sensitive data, emphasizing the critical need for robust cybersecurity defenses in the aviation supply chain.

2.4 British Airways Data Theft (2018)

Threat Actors: A group known as "Magecart," specializing in skimming credit card information from websites.

Attack Method: Injection of malicious code into the British Airways website and mobile app, specifically through a third-party JavaScript library used by the company.

Description: The attackers were able to steal personal and payment information from customers making bookings or changes on the British Airways website and app over a 15-day period, leading to significant financial and reputational damage for the airline.

2.5 Air Canada Mobile App Hack (2018)

Threat Actors: Unspecified hackers targeting vulnerabilities in mobile applications.

Attack Method: Exploitation of a vulnerability in Air Canada's mobile app, allowing unauthorized access to customer accounts.

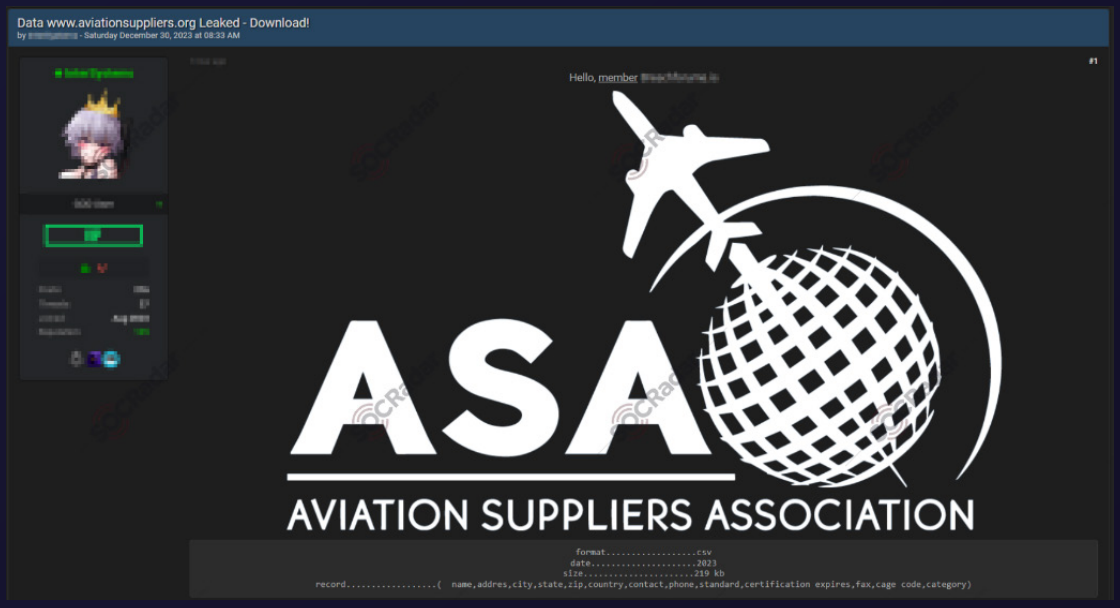
Description: This breach resulted in the compromise of personal information for approximately 20,000 users. Air Canada responded by locking down all mobile app accounts and requiring users to reset their passwords as a preventive measure.

Each of these incidents underscores the sophistication of the threat actors involved and the diverse methods they use to compromise Aviation Sector entities. From exploiting third-party vulnerabilities to direct attacks on customer databases and ransomware deployments, the Aviation Industry remains a high-value target for cybercriminals. Addressing these challenges requires a comprehensive approach to cybersecurity, including regular system audits, employee training, and collaboration with cybersecurity experts to strengthen defenses against these evolving threats.

3. Recent Incidents

Database of Aviation Suppliers Association is Leaked

December 2023

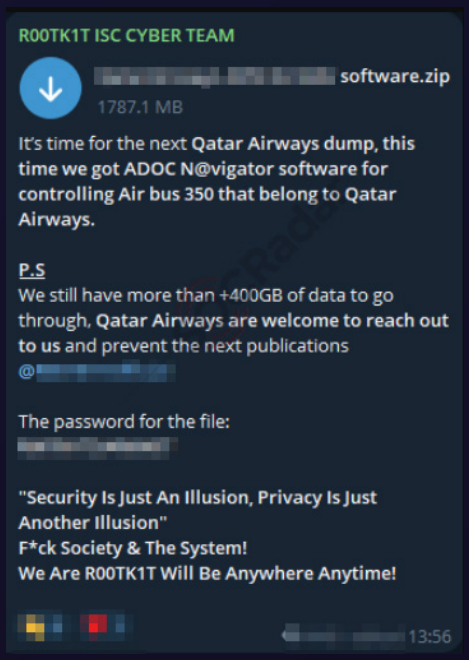


Source: SOCRadar

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Aviation Suppliers Association.

Data of Qatar Airways are Leaked by R00TK1T

December 2023



Source: SOCRadar

In the R00TK1T's Telegram channel monitored by SOCRadar, an alleged data leak is detected for Qatar Airways.

The New Data Breach Victim of DragonForce: ACE Air Cargo

December 2023

Source: SOCRadar

In the DragonForce data breacher group website monitored by SOCRadar, a new data breach victim allegedly announced as ACE Air Cargo.

Team UCC Conducted DDoS Attack on Mahan Air

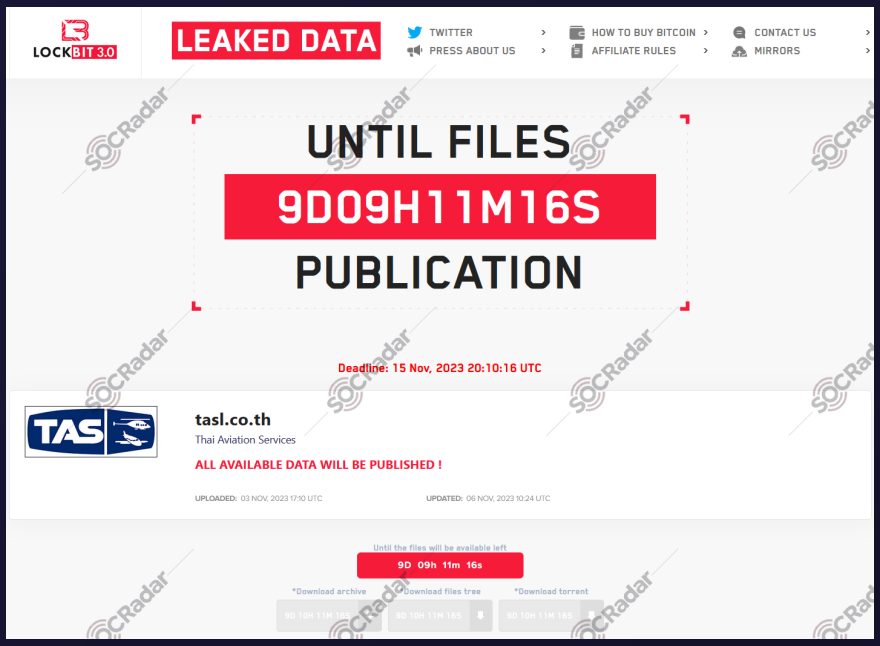
December 2023

Source: SOCRadar

In the Team UCC's Telegram channel monitored by SOCRadar, the DDoS attack announcement is detected for Mahan Air.

The New Ransomware Victim of Lockbit 3.0: Thai Aviation Services

November 2023



Source: SOCRadar

In the Lockbit 3.0 ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Thai Aviation Services.

The New Ransomware Victim of Play: Yingling Aviation

October 2023

Source: SOCRadar

In the Play ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Yingling Aviation which is a Aircraft Maintenance company from Kansas, US.

BianLian Ransomware Group Leaked The Data of Air Canada

October
2023

BianLian

Home Companies Tags Contacts

Air Canada

https://aircanada.ca

Air Canada is Canada's largest airline and the largest provider of scheduled passenger services in the Canadian market, the Canada-U.S. transborder market and in the international market to and from Canada.

President:

Business mail: [redacted]@aircanada.ca

Chief Information Officer:

Personal mail: c[redacted]@gmail.com
Mobile Phone: [redacted]

Revenue: $6.4 Billion

Data Volume: 210 GB

Stock Symbol : AC

Data description:

* Technical and operational data from 2008 through 2023.
* Information on technical and security issues of the company.
* SQL backups.
* Employee personal data.
* Information on vendors and suppliers.
* Confidential documents.
* Archives from company databases.

Incident description :

Realizing the potential damage, we did not cause any damage to infrastructure or internal resources, data exfiltration operation only. As for Air Canada data breach disclosure, they're only telling half-truths. Employee personal data is only a small fraction of the valuable data over which they have lost control. For example, we have SQL databases with company technical and security issues. You can check it out for yourself, a demo package with screenshots is available below. Backups with this data are available on our website and at your request.

Source: SOCRadar

In the BianLian ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to Air Canada.

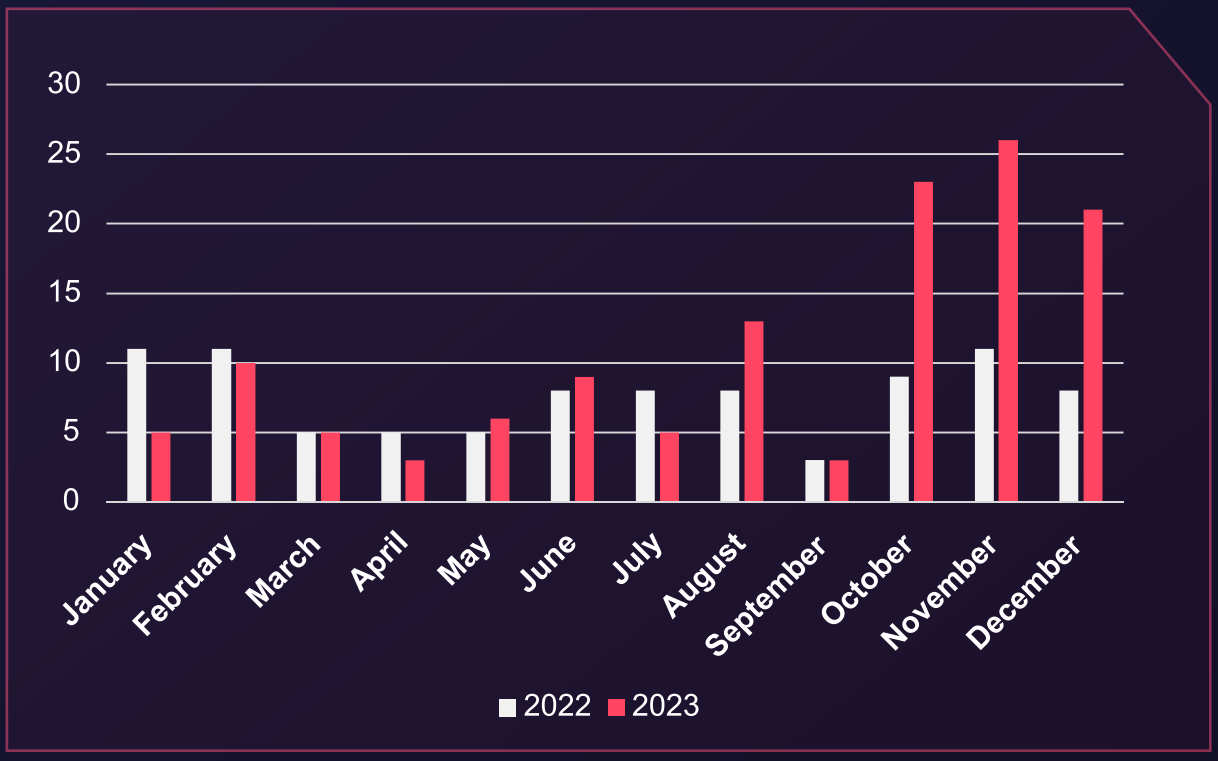
4. Dark Web Radar: Tracking Cyber Threats in the Aviation Industry

In the evolving landscape of cyber threats, the Aviation Industry stands as a critical infrastructure with unique vulnerabilities. At SOCRadar Threat Intelligence, we harness the power of advanced tools to continuously monitor the darker corners of the internet, including forums and Telegram channels that threat actors commonly use for communication, propaganda, and announcement of their nefarious activities. Through meticulous documentation and extensive tagging, we extract actionable insights about cyber incidents relating to various organizations, industries, and countries. This report is focused on the aviation industry, detailing incidents over the past two years, from January 2022 to December 2023.

In this section, we will dive into the frequency and distribution of dark web mentions connected to cyber threats in the Aviation Industry. The upcoming subsections will cover the 'Time Distribution of Posts', highlighting when the aviation industry was most talked about on the dark web, 'Top Countries Mentioned', 'Categories' for the discussions, and 'Post Owners' or actors. It's crucial to note that the numbers presented are not direct counts of cyber attacks but are indicative of the number of mentions in dark web sources. They offer a trend analysis rather than precise attack metrics.

4.1 Temporal Dynamics of Dark Web Discourse

Monthly Distribution of Dark Web Mentions in Aviation Industry



This bar graph illustrates the month-by-month frequency of dark web mentions relating to the aviation industry over the course of 2022 and 2023.

When looking at the dark web's focus on the Aviation Industry, a few trends become apparent. A general increase in mentions can be observed from 2022 to 2023, with the average monthly mentions rising from 7.67 to 10.75. Notably, there's a substantial uptick in discussions during the last quarter of 2023, with October, November, and December witnessing a significant surge in mentions. This could indicate a rising interest or a series of incidents that captured the attention of threat actors within this period.

Another interesting feature is the relative consistency in some months from year to year, such as March and September, which could suggest seasonal patterns in the actors' focus or activities. Conversely, the dip in mentions in April and July of 2023, as opposed to the relatively steady numbers in 2022, could reflect changes in threat actor behavior or shifts in cybersecurity measures within the industry. The data highlights the fluctuating nature of the threat landscape, emphasizing the need for ongoing vigilance and adaptive security postures in the Aviation Sector.

4.2 Geographic Focus of Cyber Threats in Aviation

In the table below, the column 'Country' identifies the nations in question. 'Total Mentions' quantifies all instances the Aviation Industry of each country is mentioned in the dark web, whether the country is mentioned alone or with others. 'Exclusive Mentions' captures how many times a country's industry is the only one mentioned, hinting at a targeted interest. Finally, 'Targeting Rate' shows the frequency of such exclusive mentions as a percentage of total mentions, offering insight into the intensity of focus on a particular nation by cyber threat actors.

Predominant Countries Targeted in Aviation-Related Cyber Threat Discussions

Country	Total Mentions	Exclusive Mentions	Targeting Rate
United States	46	36	**78.26%**
United Kingdom	15	8	**53.33%**
Canada	11	9	**81.82%**
India	11	9	**81.82%**
France	11	7	**63.64%**
Taiwan	10	7	**70.00%**
Israel	9	9	**100.00%**
Germany	9	4	**44.44%**
Russia	7	7	**100.00%**
United Arab Emirates	7	6	**85.71%**

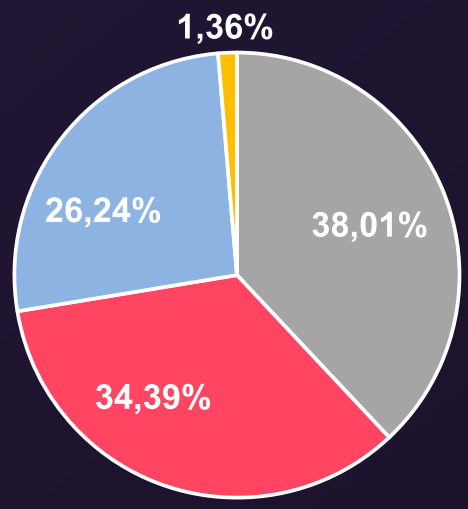
This table ranks the top ten countries based on the frequency of their Aviation Industry's mentions in dark web discussions, highlighting direct targeting instances.

The trends suggest that certain geopolitical tensions, such as those involving Israel and Russia, may correlate with a 100% targeting rate, where all mentions are exclusive, potentially reflecting the heightened cyber risks associated with ongoing conflicts. European countries like the United Kingdom, Germany, and France, which have nuanced positions in these conflicts, often appear in mentions with other nations, indicated by lower targeting rates. This could suggest a broader geopolitical motive behind cyber threats, where threat actors focus on a coalition of countries rather than on individual nations.

4.3 Categorization of Dark Web Activities Related to Aviation Cyber Threats

The pie chart below provides an overview of the documented dark web activities related to the Aviation Industry, broken down into four categories: sharing data, selling data, hack announcements, and buying data. Remarkably, hack announcements constitute 26.24% of the activity, which is a striking signature for the Aviation Industry. Typically, the dark web is more heavily skewed towards sharing and selling data, often surpassing 90% combined in other industries. The prominence of hack announcements in this case could indicate a high level of hacktivist engagement in the Aviation Sector in the context of previously discussed conflicts, where actors are not just interested in profiteering from data but are also keen on making political or ideological statements through their attacks.

Aviation-Related Cyber Threat Activities on the Dark Web



This pie chart displays the distribution of different types of cyber threat activities pertaining to the Aviation Industry, as documented from dark web sources. A notable deviation from typical industry patterns is the significant portion of hack announcements, suggesting a pronounced hacktivist presence.

Sharing data remains the most prevalent activity at 38.01%, closely followed by selling data at 34.39%. The act of buying data is relatively low, representing only 1.36% of the activities. This low figure for data purchasing could imply that there is either a robust supply of illicitly obtained aviation-related information readily shared or sold, or it could reflect a lack of demand for such data, possibly due to the specificity and specialized nature of aviation data which may not have a wide market. The data points underscore the need for increased security vigilance and proactive threat intelligence efforts in the Aviation Industry to mitigate these diverse and significant cyber threats.

4.4 Dominant Voices in Aviation Cyber Threat Discourse

Most Prominent Post Owners on Aviation Industry Cyber Threats

Most Active Post Owners	# of Posts
Mysterious Team Bangladesh	8
Dark Storm Team	7
markitto35	6
iamtrump	6
NoName057(16)	5
Anonymous Sudan	5

This table showcases the most active post owners who have discussed threats related to the Aviation Industry, hinting at potential affiliations with hacktivist groups.

In the landscape of cyber threats, it is important to distinguish between the entities who discuss and possibly disseminate information about cyber activities and the actual perpetrators or threat actors. The post owners listed in this table are the most vocal on platforms tracked by SOCRadar, discussing threats targeting the Aviation Industry. While their exact relationship to threat actors is not explicitly known, there is an observable pattern that aligns most of these post owners with hacktivist groups, particularly those involved in the previously mentioned geopolitical conflicts. The prominence of groups such as 'Mysterious Team Bangladesh' and 'Dark Storm Team,' alongside individuals with handles like 'markitto35' and 'iamtrump,' suggests a landscape where hacktivist engagement is significant. This pattern underscores the influence of ideological and political motivations in cyber threat activities within the Aviation Sector.

5. Ransomware Threat Insights in the Aviation Industry

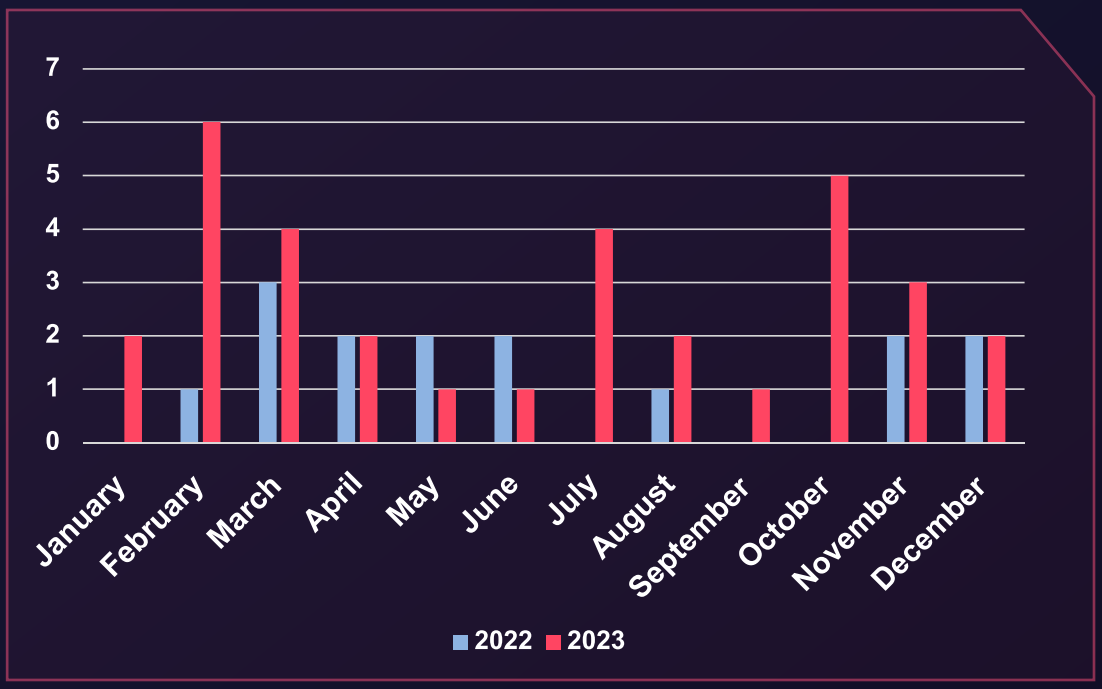
In this section, we will delve into the specific realm of ransomware activities targeting the Aviation Industry, a sector critical to global infrastructure and therefore a lucrative target for cybercriminals. Utilizing the sophisticated tools and analytical prowess of SOCRadar, we have compiled and tagged significant ransomware incidents that have surfaced on various platforms—ranging from leak and blog sites to Telegram channels. These platforms are used by ransomware operators for extortion, propaganda, and announcements, shedding light on the evolving strategies and focuses of these threat actors.

The subsequent subsections will offer a breakdown of this ransomware-related data, beginning with the 'Time Distribution of Posts', followed by 'Top Countries Mentioned', 'Most Active Ransomware Groups', and 'Share Types', all within the context of the Aviation Industry from January 2022 to December 2023. It is important to interpret this data as indicative rather than definitive; the numbers reflect mentions and reported incidents, not the exact number of attacks. There is also the possibility of the same organization being mentioned multiple times across different posts. Thus, the data should be considered a representation of the cyber threat landscape trends.

5.1 Temporal Trends of Ransomware Activity in Aviation

The graph below presents the monthly distribution of ransomware-related mentions connected to the Aviation Industry over the last two years. The visualization helps to discern the patterns and potential escalations in ransomware activity or interest within this sector.

Monthly Evolution of Ransomware Discussions: Aviation Industry Focus



This bar chart illustrates the month-by-month evolution of ransomware-related discussions in the context of the Aviation Industry for 2022 and 2023.

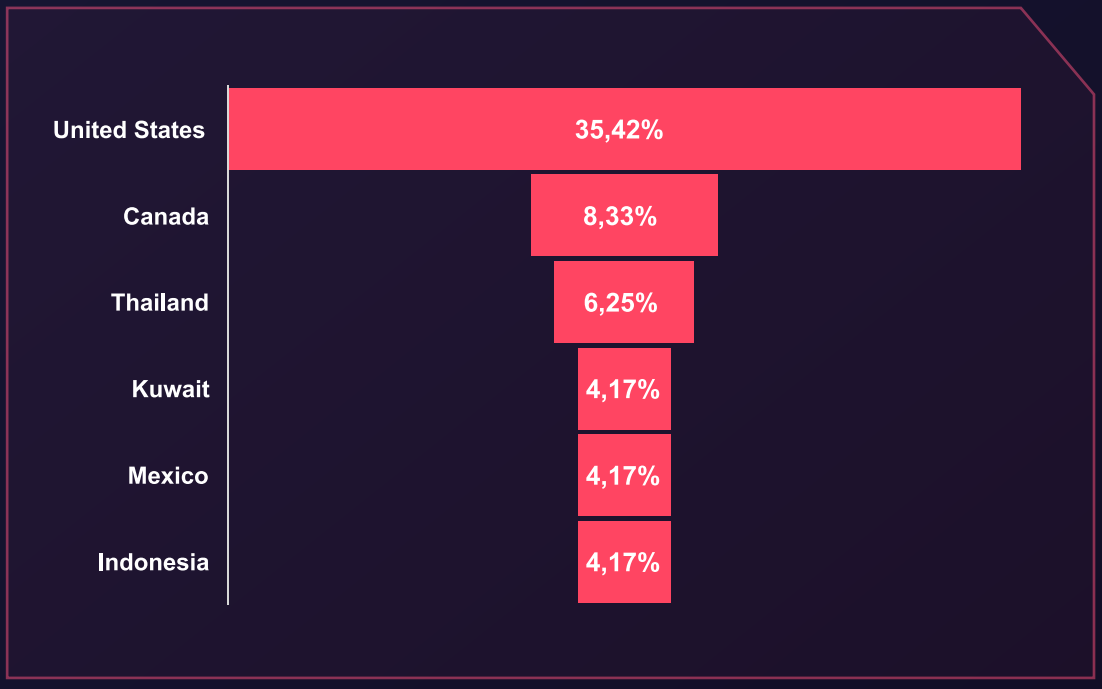
Upon reviewing the graph, a noticeable trend is the overall increase in ransomware mentions from 2022 to 2023, with the average monthly mentions more than doubling from 1.25 to 2.75. This escalation suggests an increasing interest or activity from ransomware operators targeting the Aviation Industry. While January and February of 2023 show a marked increase compared to the same period in 2022, the months of July and October in 2023 also exhibit significant spikes. These could be indicative of specific campaigns or a broader trend of increased ransomware operations during those times.

It's also worth noting the absence of any documented ransomware mentions in certain months of 2022, such as January and July, which then transition to periods of activity in 2023. This could highlight new ransomware groups emerging, shifts in target selection, or changes in the threat landscape that render the Aviation Industry a more appealing target during these months. The data underscores the need for the Aviation Industry to remain alert to ransomware threats year-round, with particular attention to the identified peak periods.

5.2 National Spectrum of Ransomware Targets in Aviation

The data provides a revealing look at which countries' Aviation Industries are most frequently the subject of ransomware-related discussions. The United States leads by a significant margin, representing over a third of all mentions, which may reflect its large aviation market and the high volume of cyber activities typically associated with it. Canada follows, but with a considerably smaller share, which suggests that while it is still a focus, it's not nearly to the extent as the US.

Monthly Evolution of Ransomware Discussions: Aviation Industry Focus



The graph depicts the share of ransomware-related discussions by country, highlighting the most frequently targeted nations in the Aviation Sector.

Thailand, Kuwait, and Mexico, though mentioned less frequently, indicate a trend where ransomware groups do not solely concentrate on the traditionally most economically powerful countries but also on a diverse array of nations, which could relate to specific vulnerabilities or strategic interests of the attackers.

It's noteworthy to mention that the top countries highlighted in ransomware discussions differ from those emphasized in dark web news, suggesting that the interests and targets of ransomware groups do not necessarily align with the broader cyber threat activities covered in other sections of the dark web. This distinction is crucial for risk assessment and the development of cybersecurity strategies, as it demonstrates the need for a nuanced understanding of threat actor behaviors across different segments of the cybercrime ecosystem.

5.3 Hierarchy of Ransomware Groups Targeting Aviation

The table provided highlights the most active ransomware groups in the Aviation Industry, measured by their share of mentions in cyber threat discussions within the designated time frame. A significant trend is the dominance of LockBit, commanding over a quarter of all mentions, which aligns with their recognized position at the forefront of the global ransomware ecosystem in the scope of this report. This level of activity underscores the significant threat LockBit poses to the Aviation Industry, given its widespread influence and effectiveness.

Ransomware Groups' Predominance in Aviation Industry Threats

Most Active Groups	Share
LockBit 3.0 & 2.0	27.08%
Cl0p	10.42%
ALPHV/ Blackcat	6.25%
Black Basta	6.25%
Play	4.17%
Medusa Team	4.17%
Quantum	4.17%
RansomHouse	4.17%
Ransomex(Defray77)	4.17%

A ranking of the ransomware groups by their share of mentions in discussions related to attacks on the Aviation Industry.

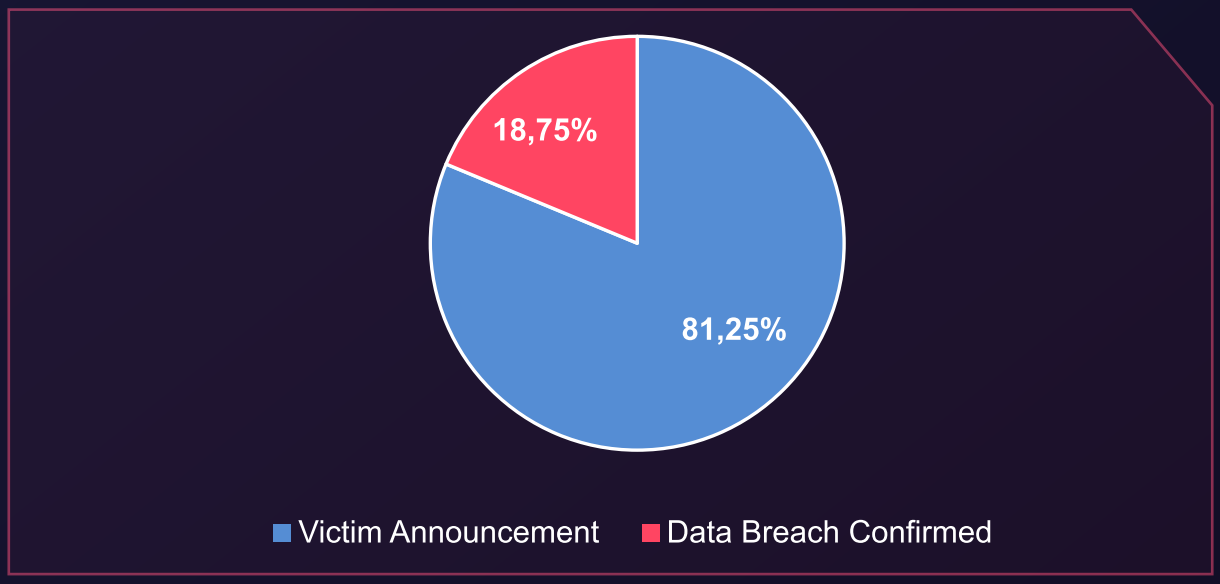
Following LockBit, Cl0p holds a notable share, suggesting its persistent presence in the cyber threat landscape, although with less dominance. Other groups like ALPHV/Blackcat and Black Basta each account for a similar portion of discussions, indicating a somewhat balanced level of activity amongst these players within the ransomware arena. The remaining groups — Play, Medusa Team, Quantum, RansomHouse, and Ransomex(Defray77) — each share an equal fraction of the activity. This points to a competitive environment where multiple groups are actively engaging in ransomware operations, albeit with less frequency than the leading entities.

The diversity of active groups suggests a decentralized threat landscape in which numerous ransomware operators vie for opportunities within the Aviation Sector. LockBit's prominence highlights a key player for cybersecurity teams in the Aviation Industry to monitor closely, while the array of other active groups serves as a reminder of the multifaceted nature of ransomware threats.

5.3 Intent Behind Ransomware Actions in the Aviation Industry

The data presented in the graph provides insight into the operational tactics of ransomware groups targeting the Aviation Sector. With 81.25% of the incidents tagged as 'Victim Announcement', it is clear that the majority of ransomware operators prefer to publicly announce their victims as part of their strategy, likely as a means of pressuring organizations into complying with their demands. This could also serve as a deterrent or warning to other potential targets.

Proportion of Ransomware Announcements to Data Exposure Incidents

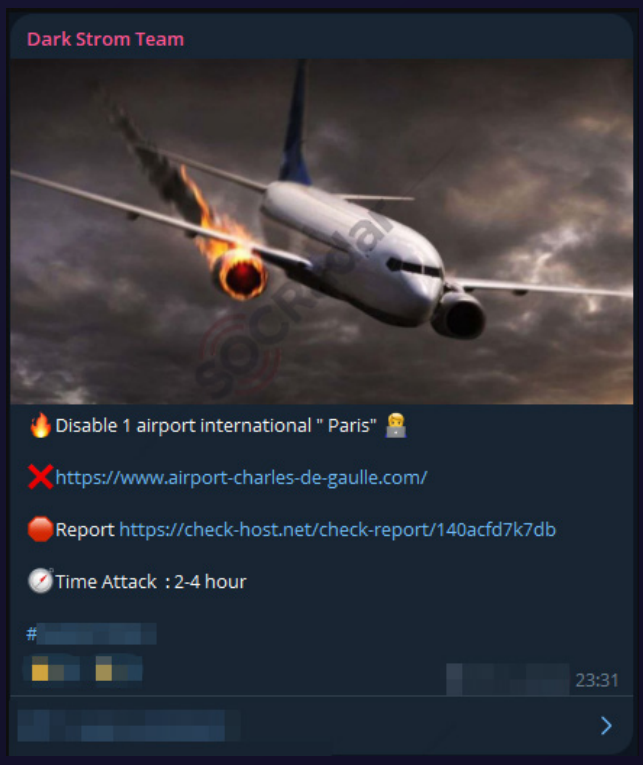


This pie chart represents the distribution of ransomware operators' actions as categorized by victim announcements versus actual data exposure events.

In contrast, 'Data Breach Confirmed' incidents account for only 18.75%, indicating that a smaller fraction of ransomware attacks in the Aviation Sector led to actual data disclosure. This could suggest that either victims are paying the ransom to prevent data exposure or ransomware groups are using the threat of exposure more as leverage than following through with the act itself.

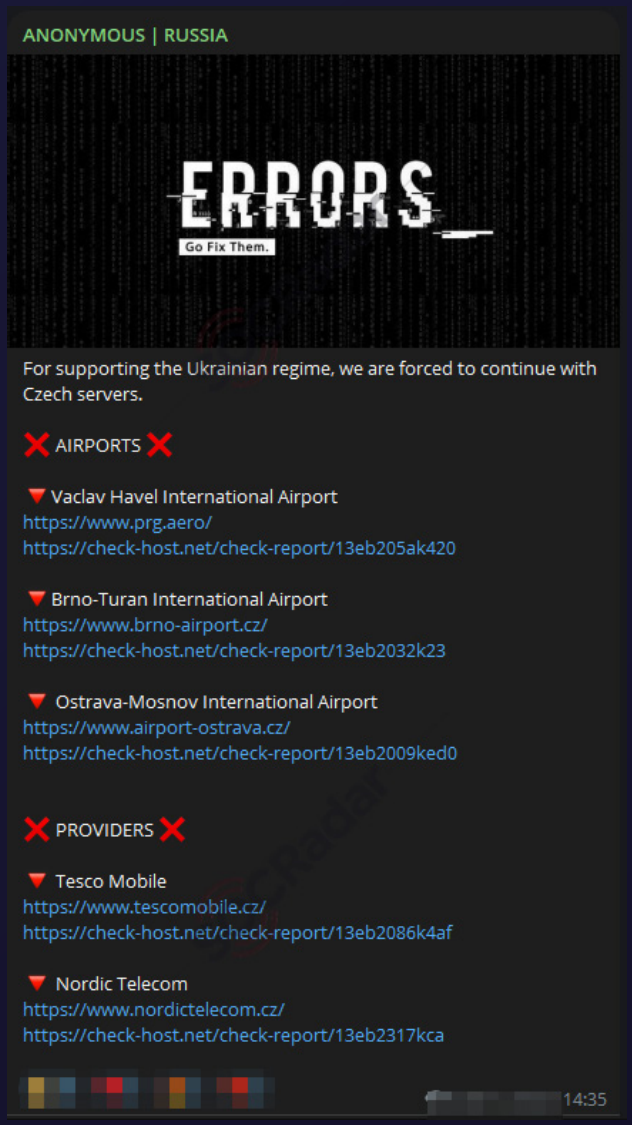
6. DDoS Attacks in the Aviation Industry A Rising Cyber Threat

The Aviation Industry is increasingly becoming a target for DDoS (Distributed Denial of Service) attacks, a trend that has seen a resurgence due to various factors, including the widespread availability of DDoS-for-hire services, the proliferation of insecure IoT devices, and the sophistication of attack methods. Moreover, the digital transformation accelerated by the COVID-19 pandemic has expanded the attack surface, offering more targets to malicious actors. The geopolitical landscape, too, has influenced the frequency and intensity of these attacks, with hacktivism becoming a prominent motivator behind such cyber incidents.



In the Dark Storm Team's Telegram channel monitored by SOCRadar, the DDoS attack announcement is detected for Charles de Gaulle Airport. (Source: SOCRadar)

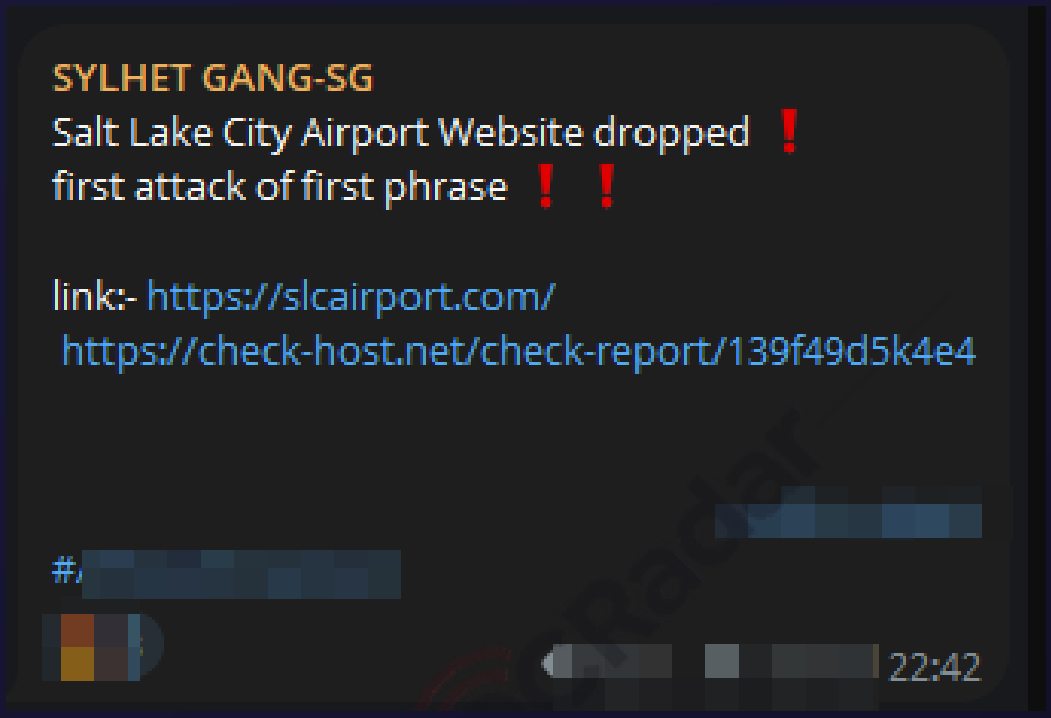
Recent analyses have highlighted a significant rise in DDoS attacks, underscored by the notable impact these attacks have had on different sectors, including the aviation industry. Cloudflare's Q4 2023 report revealed a 175% year-over-year increase in network-layer DDoS attacks, emphasizing the growing sophistication and scale of these threats. The same period witnessed geopolitical tensions, such as the Israel-Hamas conflict, which saw a surge in cyber attacks, including DDoS attacks, as part of broader hacktivist activities. This aligns with the observed increase in DDoS-related posts on dark web forums, with a significant spike in discussions and posts related to DDoS attacks in the last quarter of 2023, suggesting an intensification of such cyber activities amid geopolitical unrest.



In the Anonymous Russia's telegram channel monitored by SOCRadar, the DDoS attack announcement is detected for Czech websites. (Source:SOCRadar)

In the previous dark web news section, a noteworthy observation was made regarding the content and focus of discussions, particularly in relation to Distributed Denial of Service (DDoS) attacks. Out of a total of 129 posts in 2023, 29 were specifically related to DDoS attacks, illustrating a significant interest or focus within these forums on this type of cyber activity. Remarkably, 27 of these DDoS-related posts occurred in the last quarter of 2023, a period that coincides with the escalation of tensions in the Israel-Hamas conflict, which began on October 7, 2023. This surge in discussions about DDoS attacks during this timeframe suggests a correlation between geopolitical events and the focus of cyber threats or hacktivist activities on the dark web.

Akamai's 2023 report further elaborates on the landscape, noting that DDoS attacks have become more frequent, sophisticated, and prolonged. The report highlights how cybercriminal groups and hacktivists exploit the relatively low cost of launching DDoS attacks and the vulnerability of critical infrastructure, including the Aviation Sector. This emphasizes the strategic selection of targets by attackers, aiming to cause disruption, financial losses, and gain public attention.



In the Sylhet Gang-SG's Telegram channel monitored by SOCRadar, the DDoS attack announcement is detected for Salt Lake City International Airport. (Source:SOCRadar)

Imperva's 2023 DDoS Threat Landscape Report also notes the significant increase in application layer DDoS attacks, underscoring a 121% growth in attacks targeting the financial services sector, which often includes entities associated with the Aviation Industry. The report emphasizes the recurring nature of DDoS attacks, with nearly half of the websites targeted by a DDoS attack facing subsequent attacks.

These developments underscore the critical need for the Aviation Industry to bolster its cybersecurity measures. Ensuring robust DDoS protection and implementing comprehensive, flexible, and reliable defense strategies are paramount to safeguard against these growing cyber threats. As DDoS attacks continue to evolve in sophistication and scale, the Aviation Sector must remain vigilant and proactive in its cybersecurity efforts to mitigate the risks and protect its digital and operational infrastructure from potential disruptions.

7. Navigating Supply Chain Cyber Threats in the Aviation Industry

The Aviation Sector's complex supply chain is increasingly in the crosshairs of cybercriminals, with recent incidents underscoring the vulnerabilities present across this interconnected network. The rise in cyber threats targeting supply chain components—from third-party vendors to critical operational technologies—highlights the urgent need for enhanced cybersecurity measures within the industry.

7.1 Highlighted Incidents and Exploited Vulnerabilities

High-profile breaches, such as those experienced by American Airlines and Southwest Airlines through the third-party vendor Pilot Credentials, have put a spotlight on the risks associated with supply chain components. Furthermore, the MOVEit supply chain attack, impacting entities like the Dublin Airport Authority, illustrates the potential for widespread disruption when third-party software and services are compromised.

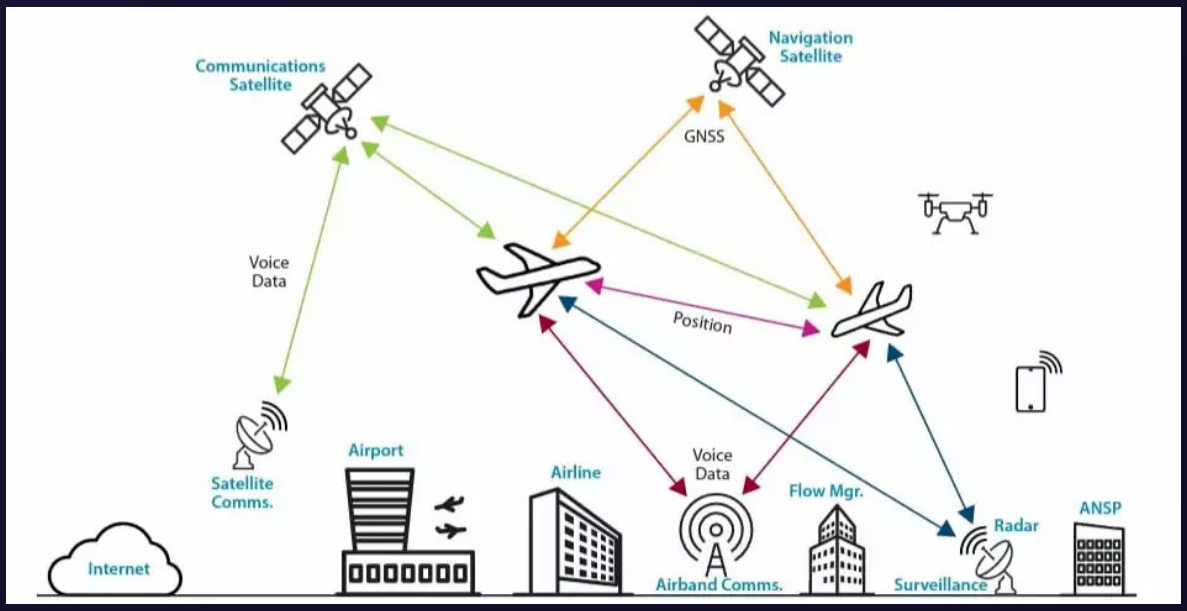
A screenshot from the Maine Attorney General's website displaying a data breach notification for American Airlines, Inc.

These incidents are part of a broader trend of increasing cyberattacks targeting the Aviation Industry, including a significant rise in ransomware attacks on supply chain players, up by as much as 600% in a year according to the statistics cited by Boeing at Aviation Week's MRO Americas Conference in Atlanta. The disruptions caused by these attacks can lead to considerable financial losses and damage to reputation, underscoring the cascading effects within the Aviation Sector's supply chain.

7.2 Challenges in Protecting the Aviation Supply Chain

The reliance on outdated operational technology systems poses a significant cybersecurity challenge. For instance, the use of such systems by critical infrastructure, including the FAA in the United States, potentially exposes the industry to cyber threats. The evolving tactics of cybercriminals, coupled with the vulnerability of these systems, necessitates a robust cybersecurity framework to protect against potential breaches.

To mitigate the risks associated with supply chain vulnerabilities, the Aviation Industry must adopt a multi-faceted approach. This includes conducting comprehensive cyber audits, implementing AI monitoring systems for round-the-clock threat detection, and performing supply chain mapping exercises to gain insight into direct and indirect supply chain partners. These measures can help identify vulnerabilities, enable swift detection and response to cyber threats, and strengthen the overall cybersecurity posture of the aviation supply chain.



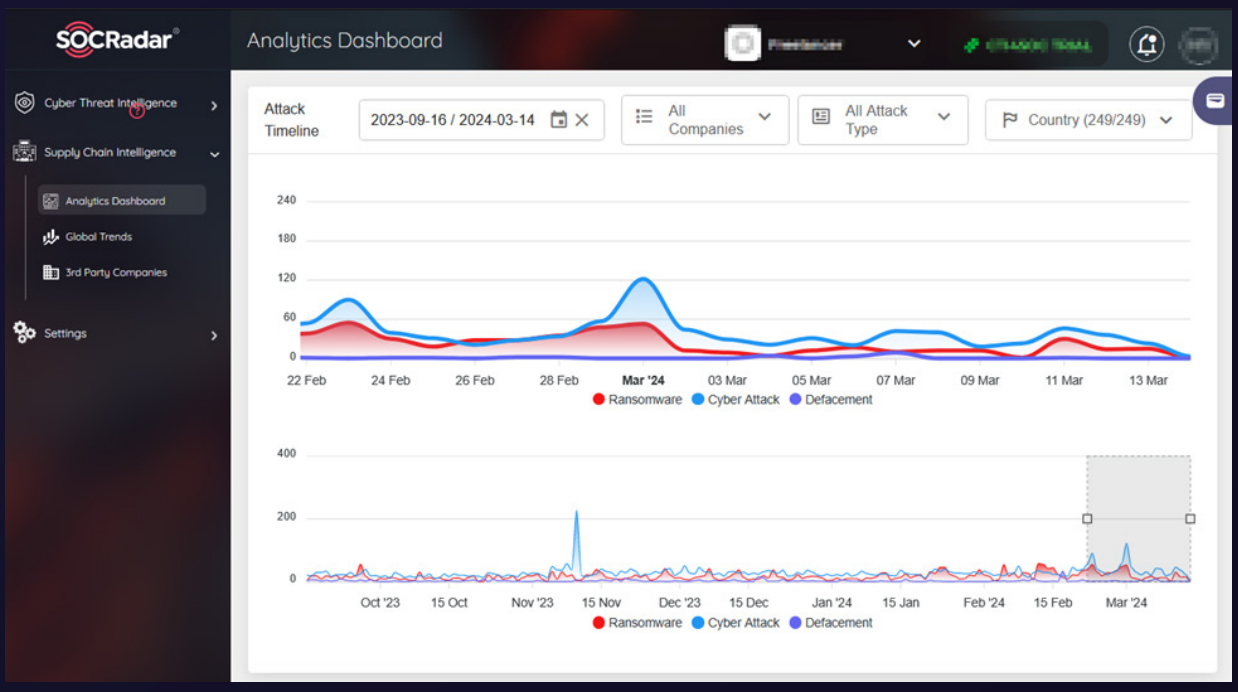
Complexity of Securing the Aviation Ecosystem (Source: Eurocontrol Air Traffic Management (ATM) A Cybersecurity Challenge Report)

The Aviation Industry's increasing reliance on technology, combined with the intricate nature of its supply chain, presents a lucrative target for cybercriminals. The case studies and incidents from the first half of 2023 underscore the importance of supply chain security and the need for the Aviation Sector to adopt an intelligence-driven approach to cybersecurity. This entails leveraging threat intelligence, fostering collaboration among industry stakeholders, and staying informed about emerging trends and vulnerabilities.

7.3 Enhancing Supply Chain Security with SOCRadar

In the face of a staggering 2,600% rise in supply chain attacks since 2018 in the United States, as reported by the Identity Theft Resource Center (ITRC), and Gartner's prediction that 45% of organizations globally will suffer software supply chain attacks by 2025, the security of supply chains has never been more critical. These alarming statistics highlight a key vulnerability: attackers often bypass robust corporate defenses by exploiting weaknesses in less secure, connected vendors. The resulting challenge for organizations is the imperative need to extend security measures beyond their own perimeter, to include a comprehensive evaluation of their vendors' security postures.

SOCRadar's Supply Chain Intelligence steps in as a holistic, threat-focused solution. Its proactive methodology sets a new standard in supply chain security, equipping organizations with a wealth of insights on over 50 million companies across 373 sectors in 249 countries. This intelligence is not just about monitoring — it's about understanding and mitigating real-world threats through advanced features, including automated supply chain mapping, real-time updates, and tier grouping.



Overview of the SOCRadar Analytics Dashboard displaying a timeline of cyber threat activities, including ransomware, general cyber attacks, and website defacement.

SOCRadar excels by automating the mapping of the supply chain environment, generating critical recommendations, and providing The Analytics Board, an advanced tool designed for effortless monitoring and in-depth trend analysis. Moreover, the service includes a sophisticated alarming system to notify organizations of critical events and potential risks promptly. Comprehensive security reports give deep insights into third-party vendors' operations and cybersecurity postures, enhanced by advanced scoring mechanisms such as Cyber Exposure Level and Popularity Score.

SOCRadar, therefore, becomes an indispensable ally in anticipating disruptions and ensuring business continuity in an era where supply chain attacks are not just a threat but an expected occurrence. It is a game-changer for organizations looking to defend against the sophisticated and often indirect strategies of modern cyber adversaries.

8. Conclusion

The examination of cyber threats facing the Aviation Industry reveals a complex and dynamic threat landscape, where the stakes are incredibly high. The incidents detailed within this document—from high-profile data breaches to insidious ransomware and DDoS attacks—serve as critical lessons for the Aviation Sector. They emphasize the need for an intelligence-driven approach to cybersecurity, where ongoing vigilance, adaptive security measures, and collaboration across the industry are paramount. As the digital and operational infrastructure of the Aviation Industry continues to evolve, so too must its cybersecurity strategies, ensuring the safety, security, and trust of its global users. In facing these challenges head-on, the Aviation Sector can navigate the turbulent skies of cyber threats, safeguarding its future and the millions of individuals it serves daily.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

21.000+
Free Users

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

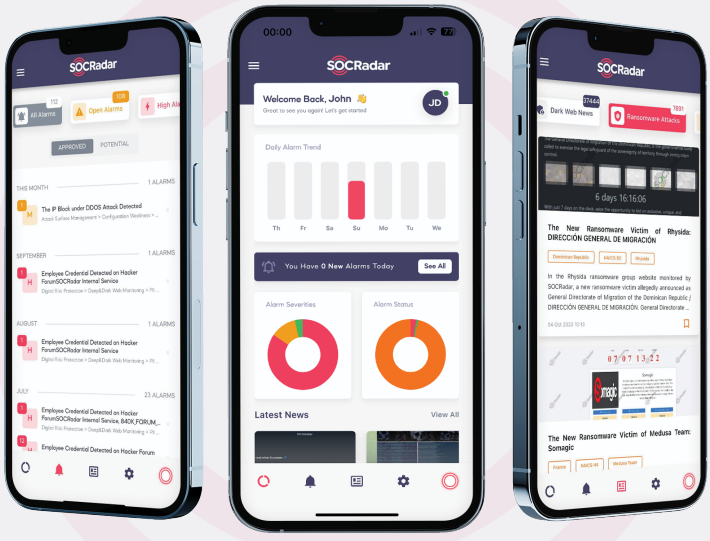
GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store

GET IT ON Google Play



Gartner Peer Insights™ 4.8/5