Resecurity | The Aviation and Aerospace Sectors Face Skyrocketing Cyber Threats

Published: 2024-03-16 · Archived: 2026-04-05 16:59:41 UTC

Executive Summary

This Resecurity report highlights recent cyber incidents targeting the aerospace and aviation sectors and emphasizes the importance of rigorous cybersecurity risk assessments for airports. It's important to note the distinct technical definitions that distinguish the aerospace and aviation industries.

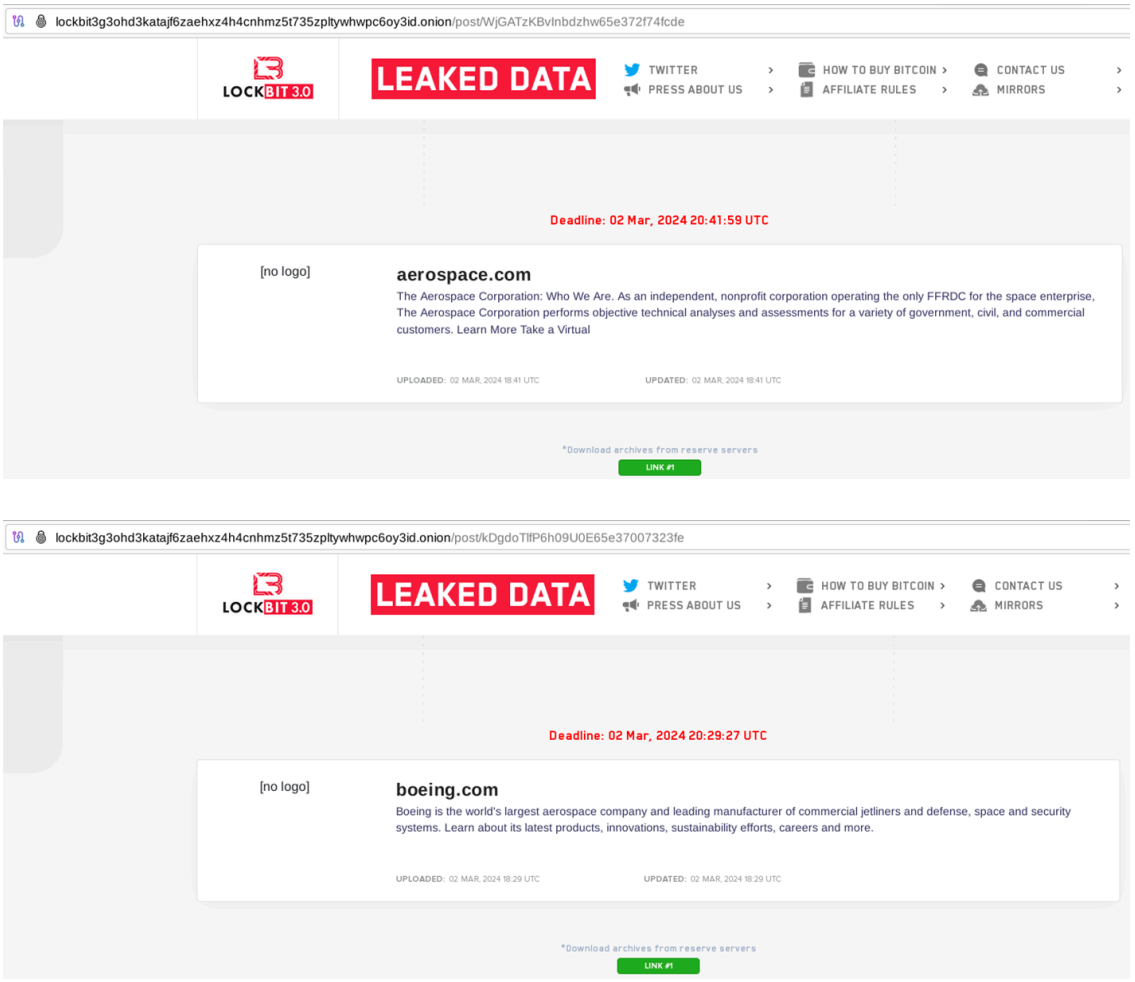
While aviation pertains to flying or controlling the aircraft, aerospace refers to the "design, manufacturing, and maintenance of aircrafts or spacecrafts and can be thought of as the science of flight within Earth's atmosphere as well as outside it," according to industrial manufacturer Peli. For the purposes of this report, these terms may occasionally be used interchangeably.

Resecurity's report will highlight recent malicious cyber-activity targeting the aerospace sector. Resecurity will also discuss how cybersecurity risk assessments can help the aerospace sector prevent cyberattacks and outline the types of threat-modeling needed for industry stakeholders to achieve a comprehensive security posture in their organizations.

Aerospace Cyber-Threat Overview

The aerospace sector has become a rising target for cyberattacks due to its reliance on vastly interconnected digital infrastructures, global supply chains, and the torrential volume of sensitive data it handles. More recently, this attack trend has been amplified by the rapidly growing integration of Industrial Internet of Things (IIoT) technologies, rising geopolitical tensions, and the U.S. governments' decision to designate aerospace and aviation as critical infrastructure.

Speaking on a panel at the 2023 Aviation Week MRO Americas Conference held in Atlanta last April, Boeing Chief Security Officer Richard Puckett noted that "occurrences of ransomware inside the aviation supply chain" had shot up 600% in 2022. This sectoral ransomware trend has persisted since Puckett flagged the threat, headlined by **LockBit 3.0**'s breach of Boeing last November and its alleged compromise of the non-profit Aerospace Corporation this year.



Overall, ransomware is one of the top threats facing the aviation industry, if not the leading one in some jurisdictions. In 2023, the European Organization for the Safety of Air Navigation (Eurocontrol) reported that ransomware was the sector's leading attack trend in 2022, accounting for 22% of all malicious incidents. At the Atlanta conference, Puckett also said that industry defenders must “begin to account for the extended ecosystem of connectivity ... Increasing requests for sensors on almost every working part of the aircraft makes it more efficient but it also makes it more vulnerable because anything that sends or receives a signal can be hacked.” In other words, the IIoT-driven expansion of digital connectivity has drastically amplified the attack surface for aerospace organizations at more granular levels of their supply chain.

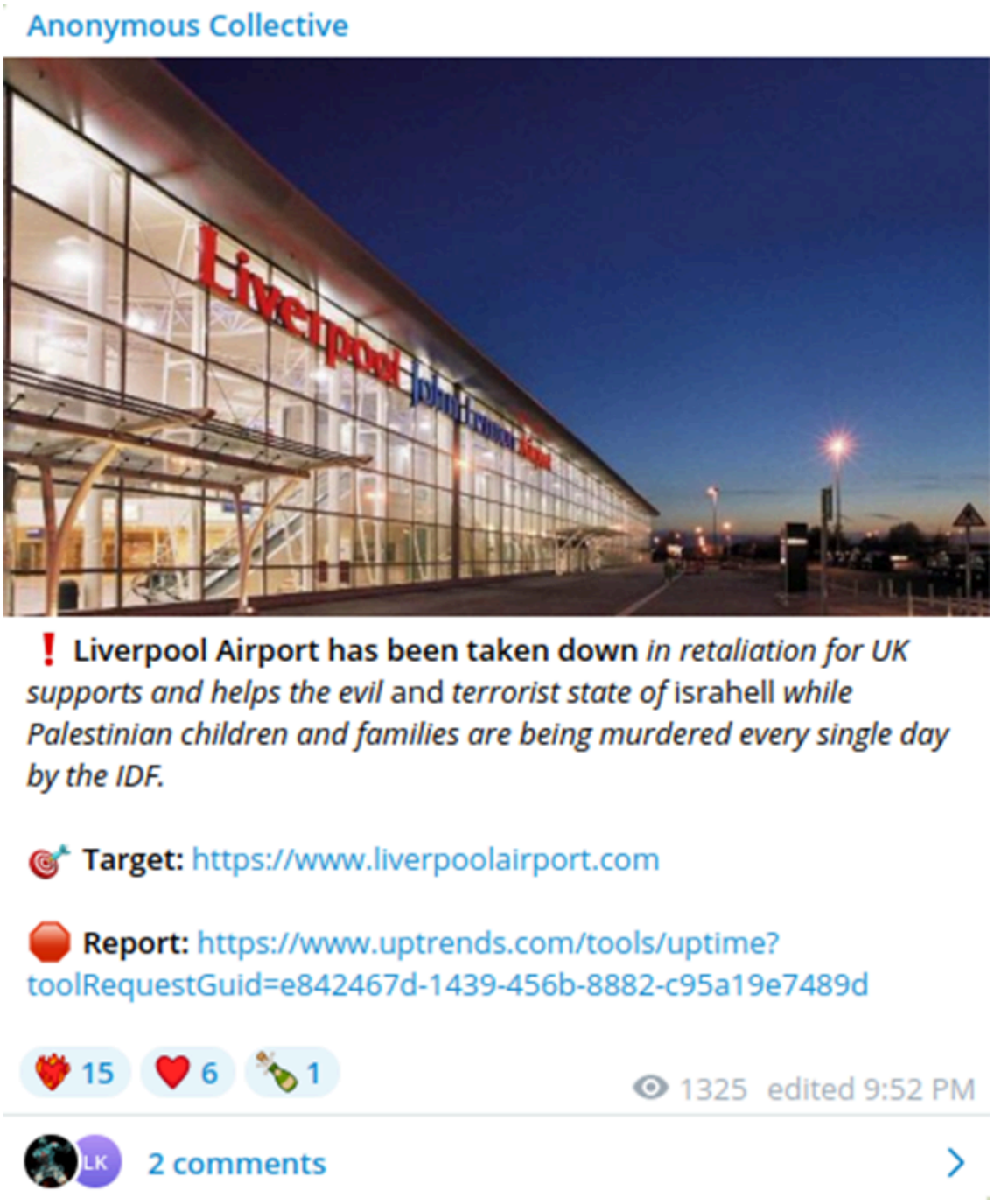
Discussing the modern aviation sector’s attack surface, an *Aerospace Testing International* report published last year said it had “grown significantly as remote systems like IoT sensors, actuators, biometric readers, robotics and cloud applications require web connectivity.” The report also noted that “mobile phones and bring your own device (BYOD) policies add more weaknesses. Important targets for hackers include reservation systems, flight history servers, ticket booking portals, flight management systems and cabin crew devices.”

In an increasingly fragmented geopolitical landscape reshaped by the war in Ukraine and the eruption of hostilities in the Middle East, the aerospace sector’s designation as critical infrastructure is also fueling more cyberattacks. At last year’s Aviation Week conference, United Airlines Director of cybersecurity Jen Miosi addressed this topic, saying that the label “paints a target on airspace’s back for threat actors to want to take advantage of that critical infrastructure.”

Included in the U.S. Cybersecurity and Infrastructure Security Agency's definition of aviation-related critical infrastructure are “aircraft, air traffic control systems, and about 19,700 airports, heliports, and landing strips.” Additionally, the aviation category includes “commercial and recreational aircraft (manned and unmanned) and a wide variety of support services, such as aircraft repair stations, fueling facilities, navigation aids, and flight schools,” according to CISA.

Overall, the critical infrastructure label has made the aviation sector even more enticing to advanced-persistent threat groups and, most notably, hacktivist collectives. Jeffrey Troy, the chief executive of the Aviation Information Sharing and Analysis Center (Aviation ISAC), cited the growing hacktivist threat at last year’s conference, describing these attackers as “people who essentially do some type of cyber activity with the sense of supporting a particular political agenda.” “Without a doubt the threat side of this equation is increasing,” expounded Troy on hacktivist operations. The outbreak of war in Gaza has further escalated hacktivist activity targeting the aviation sector.

Most recently, Resecurity observed apparent Gaza-nexus hacktivist activity in a DDoS attack conducted against John Lennon Airport in Liverpool, UK by a threat-actor group calling themselves the “Anonymous Collective.” A spokesperson for the airport confirmed to the news site *Cyber Express* that the March 11 attack caused "intermittent disruption” to the organization’s website. In a Telegram post, Anonymous Collective said their DDoS attack was “in retaliation for [sic] UK supports and helps the evil and terrorist state of israhell while Palestinian children and families are being murdered every single day by the IDF.”



But in terms of the aviation industry's most critical threat exposures, panelists who spoke at the Atlanta conference generally agreed that cyber risks were most prominent in the "supporting ecosystem, rather than the airframe itself," according to a panel recap published by the event sponsor. The panelists also agreed that "risk prioritization is key," in addition to ensuring that "suppliers are thinking about cybersecurity," according to the report. However, the Aviation Week recap noted that these risk-management initiatives can be challenging for some airlines, as some of their contracts are at least a decade old. As such, these contracts may lack any meaningful stipulations for cybersecurity and related controls.

A Civil Aviation Supply Chain cybersecurity Recommendations Report published by the Aerospace Industries Association in October 2023 expounded on threats to the sector's supply chain in its 'problem statement' section. The problem statement noted, "Civil Aviation has an enormously complex and globally connected supply chain."

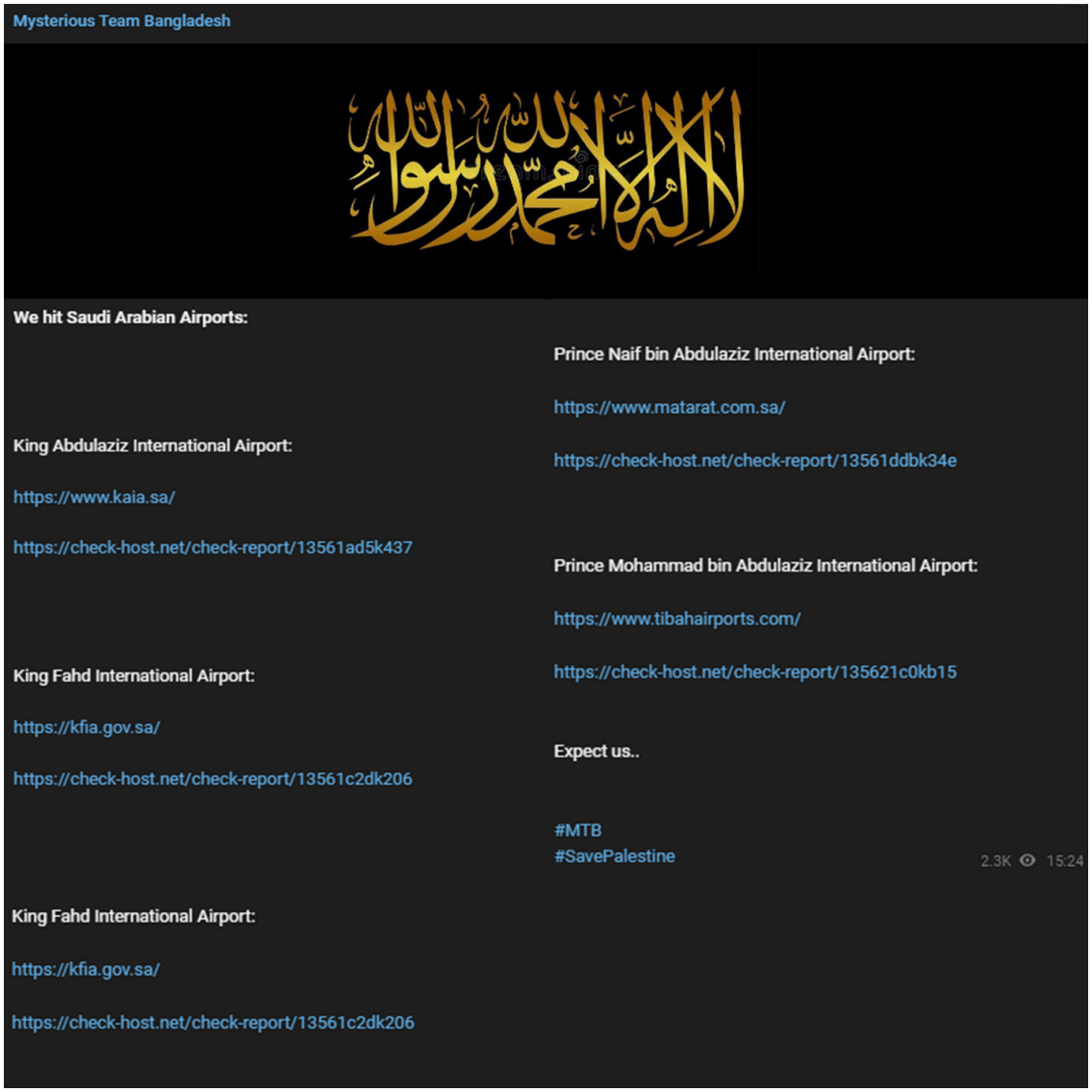
This globally diffuse complexity means that cyberattacks can “impact nearly everything in the supply chain, from the data used to build physical structures, to the electronic components – the software and firmware of complex electronic hardware (CEH) running in products or powering the servers providing services in addition to the electronic hardware itself – as well as the data and production systems used to manufacture non-electronic components such as structural items.”

As geopolitical tensions escalate worldwide, the risk of destructive cyberattacks targeting the civil aviation industry and the aerospace sector in general has significantly increased. In the next section, Resecurity will detail recent notable threat-actor activity targeting the aerospace and aviation sectors.

Recent Cyberattacks Targeting the Aerospace Sector

Mysterious Team Bangladesh targets Saudi Arabia Airport website

On **November 19, 2023**, a group identifying themselves as **"Mysterious Team Bangladesh" (MTB)** executed a Distributed Denial of Service (DDoS) attack on several key Saudi Arabian airports. The affected airports included King Abdulaziz International Airport (KAIA), King Fahd International Airport (KFIA), Prince Naif bin Abdulaziz International Airport, and Prince Mohammad bin Abdulaziz International Airport.



On **November 19, 2023**, a group identifying themselves as **"Mysterious Team Bangladesh" (MTB)** executed a Distributed Denial of Service (DDoS) attack on several key Saudi Arabian airports. The affected airports included King Abdulaziz International Airport (KAIA), King Fahd International Airport (KFIA), Prince Naif bin Abdulaziz International Airport, and Prince Mohammad bin Abdulaziz International Airport.

King Abdulaziz International Airport (KAIA)
Website: https://www.kaia.sa/
Check-host.net Report: https://check-host.net/check-report/13561ad5k437

King Fahd International Airport (KFIA)
Website: https://kfia.gov.sa/
Check-host.net Report: https://check-host.net/check-report/13561c2dk206

Prince Naif bin Abdulaziz International Airport
Website: https://www.matarat.com.sa/
Check-host.net Report: https://check-host.net/check-report/13561ddbk34e

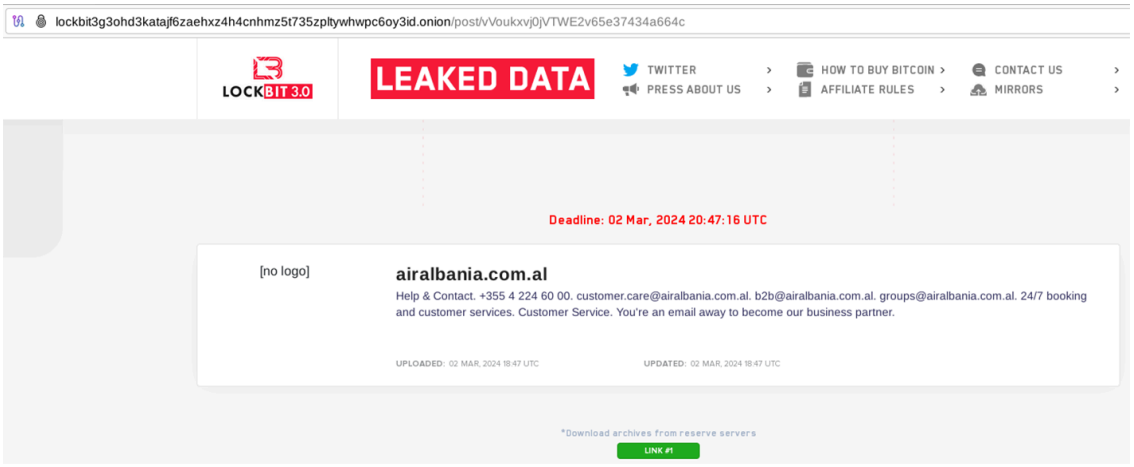
Prince Mohammad bin Abdulaziz International Airport
Website: https://www.tibahairports.com/
Check-host.net Report: https://check-host.net/check-report/135621c0kb15

The message concluded with a cryptic "Expect us.." and included the hashtags #MTB and #SavePalestine.

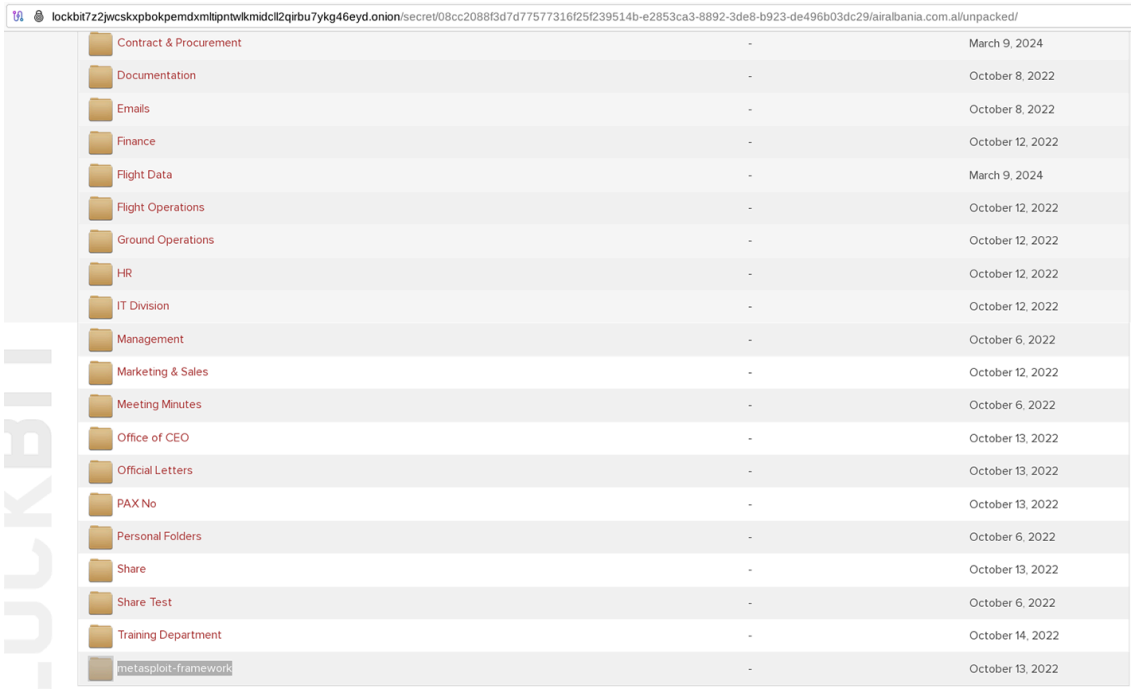
As of now, the identity and motivations of **MTB** remain unclear. **MTB**'s use of the **#SavePalestine** hashtag suggests potential ideological or political motivations related to the Gaza conflict. However, getting to the root cause of this hacktivist posturing requires deeper investigation to discern the true intent behind the attack and any potential connections to broader geopolitical issues.

Cyberattack against Air Albania

Air Albania, the flag carrier airline of Albania, was listed as a target by the LockBit ransomware group. Albania has been facing cyber-attacks in recent months, for which its government blamed Iran-sponsored threat actors. The relationship between the two nations has been tense for years and has only worsened after reports of Albania providing refuge to members of the opposition group, People's Mujahedeen of Iran (MEK), surfaced. LockBit ransomware gang has been targeting aviation sector frequently. It attacked Bangkok Airways, a major airline company in Thailand, in September 2021, Israeli aerospace and defense firm E.M.I.T Aviation Consulting in October 2021, and Kuwait Airlines in June 2022.



It is not clear how exactly the airline has been compromised, but in the leaked data set Lockbit gang included a Metasploit Framework folder. Probably, the bad actors wanted to highlight the use of post-exploitation framework and significant intrusion performed into the IT infrastructure to exfiltrate data from several employees and available file shares.



‘Host Kill Crew Hackers’ targets Cambodia Angkor Air

A lesser-known hacker group, which calls itself Host Kill Crew, has taken responsibility for the Cambodia Angkor Air cyberattack. The group posted details of the attack on their Telegram channel with claims of DDOS (Distributed Denial of Service attack) to halt the online services for a while.

Cyberattack on Gulf Air

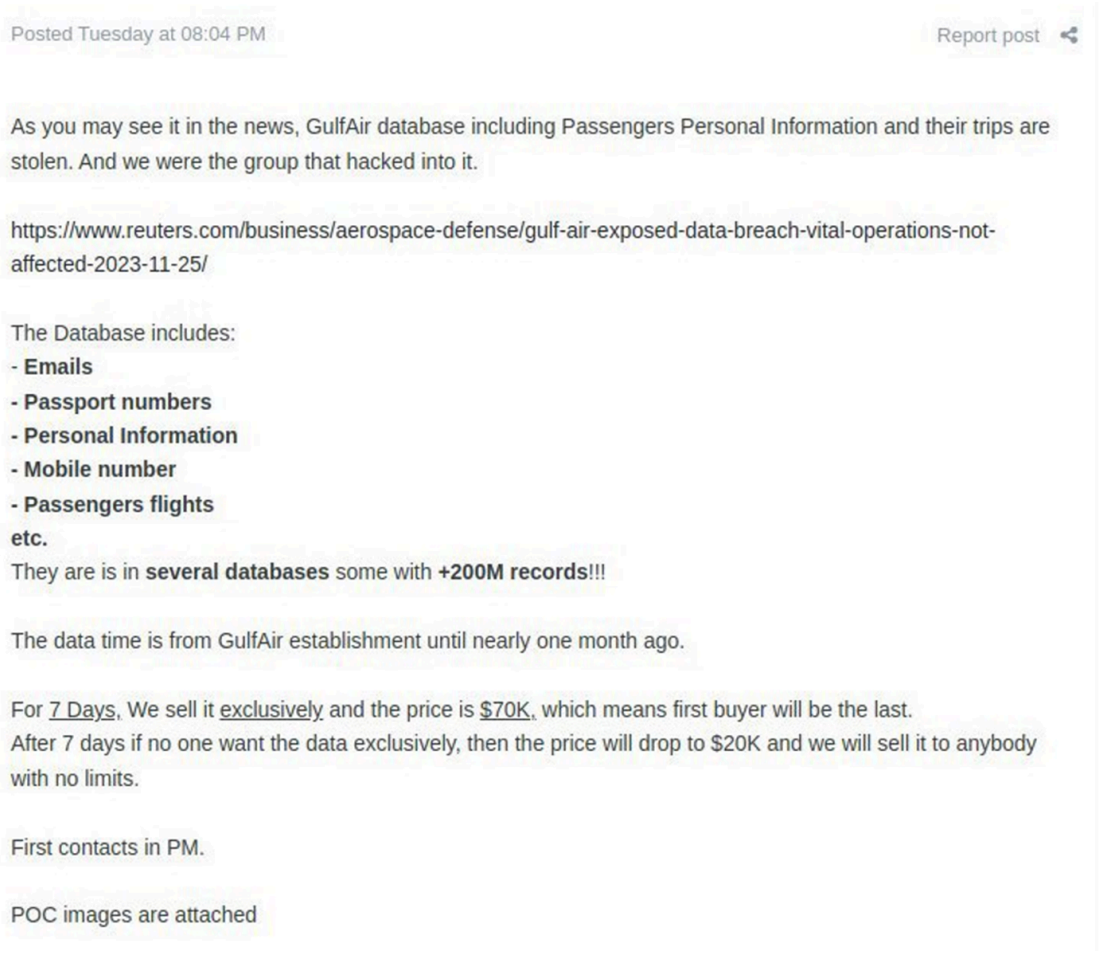
On **November 22, 2023**, a threat-actor group calling themselves **ALTOUFAN TEAM** announced their intent to conduct a Distributed Denial of Service (DDoS) attack against Gulf Air, the national carrier of Bahrain. The threat, posted on X (Twitter), explicitly links their actions to support for the Palestinian cause in the wake of the Israeli-Hamas war that erupted last October. This cyberattack threat aligns with their stated objective of disrupting entities perceived to be associated with or supportive of the “Zionist entity.”

In a follow-up tweet posted the same day, **ALTOUFAN TEAM** said it had carried out a successful DDoS attack against Gulf Air and Bahrain International Airport.

The DDoS attacks executed by ALTOUFAN TEAM successfully disrupted the online services of Gulf Air, causing operational disturbances and inconveniences for the airline's customers. While the duration and extent of the disruption remain under investigation, initial reports indicate a notable impact on the availability of Gulf Air's digital platforms and services.

The Bahrain Airport’s online portal was also temporarily rendered inaccessible by a related DDoS attack the same day. On **November 25, 2023**, Gulf Air also announced that its data was breached the previous day. However, Bahrain's news agency BNA reported that the airline’s “operations and vital systems were not affected.”

A *Reuters* write-up on the incident noted that BNA quoted Gulf Air as saying that "as a result of this illegal breach some information from the company's email system and customers' database could be compromised" and it added emergency plans were deployed to contain the breach.”



Posted Tuesday at 08:04 PM

Report post

As you may see it in the news, GulfAir database including Passengers Personal Information and their trips are stolen. And we were the group that hacked into it.

https://www.reuters.com/business/aerospace-defense/gulf-air-exposed-data-breach-vital-operations-not-affected-2023-11-25/

The Database includes:
- **Emails**
- **Passport numbers**
- **Personal Information**
- **Mobile number**
- **Passengers flights**

etc.
They are is in **several databases** some with **+200M records**!!!

The data time is from GulfAir establishment until nearly one month ago.

For 7 Days, We sell it exclusively and the price is $70K, which means first buyer will be the last.
After 7 days if no one want the data exclusively, then the price will drop to $20K and we will sell it to anybody with no limits.

First contacts in PM.

POC images are attached

Qatar Airways Data Allegedly Leaked by R00TK1T ISC Cyber Team

On **December 29, 2023**, threat-actor group "**R00TK1T ISC Cyber Team**," claimed a successful breach of Qatar Airways in a long and detailed message posted on Telegram. First, the threat actors said they had compromised the airline's ADOC Navigator system for Airbus A330 and A350 aircraft. This breach granted them access to a treasure trove of confidential flight data, maintenance schedules, and operational intricacies.

R00TK1T ISC CYBER TEAM

Attention, fellows!
We are **R00TK1T**, are here to remind you of the power we hold over the **information and systems of Qatar Airways.**
No company is safe from our grasp, and Qatar Airways is no exception!

ADOC N@vigator for Airbus 330 & 350: Unveiling the Secrets

We've managed to infiltrate **Qatar Airways ADOC N@vigator system for their Airbus 330 and 350 aircraft.**
With this access, we have unlocked a treasure trove of confidential flight data, maintenance schedules, and operational details.
The secrets of the skies are now in our hands!

Boeing 787 Toolbox Remote Data Package: Unleashing the Potential

But wait, there's more!
Our crew have also breached **Qatar Airways' Boeing 787 Toolbox Remote Data Package.**
This means we have access to critical software, maintenance logs, and even flight control systems.
The skies are our playground, and Qatar Airways is at our mercy!

Qatar Airways Interviews: Exposing Internal Discussions

In our quest for total disruption, we've obtained exclusive access to **Qatar Airways internal interview recordings.**

Qatar Airways Interviews: Exposing Internal Discussions

In our quest for total disruption, we've obtained exclusive access to **Qatar Airways internal interview recordings.**
Prepare to witness the hidden conversations, hiring practices, and decision-making processes within the airline.

Qatar Airways Sample Docs: Unmasking the Inner Workings

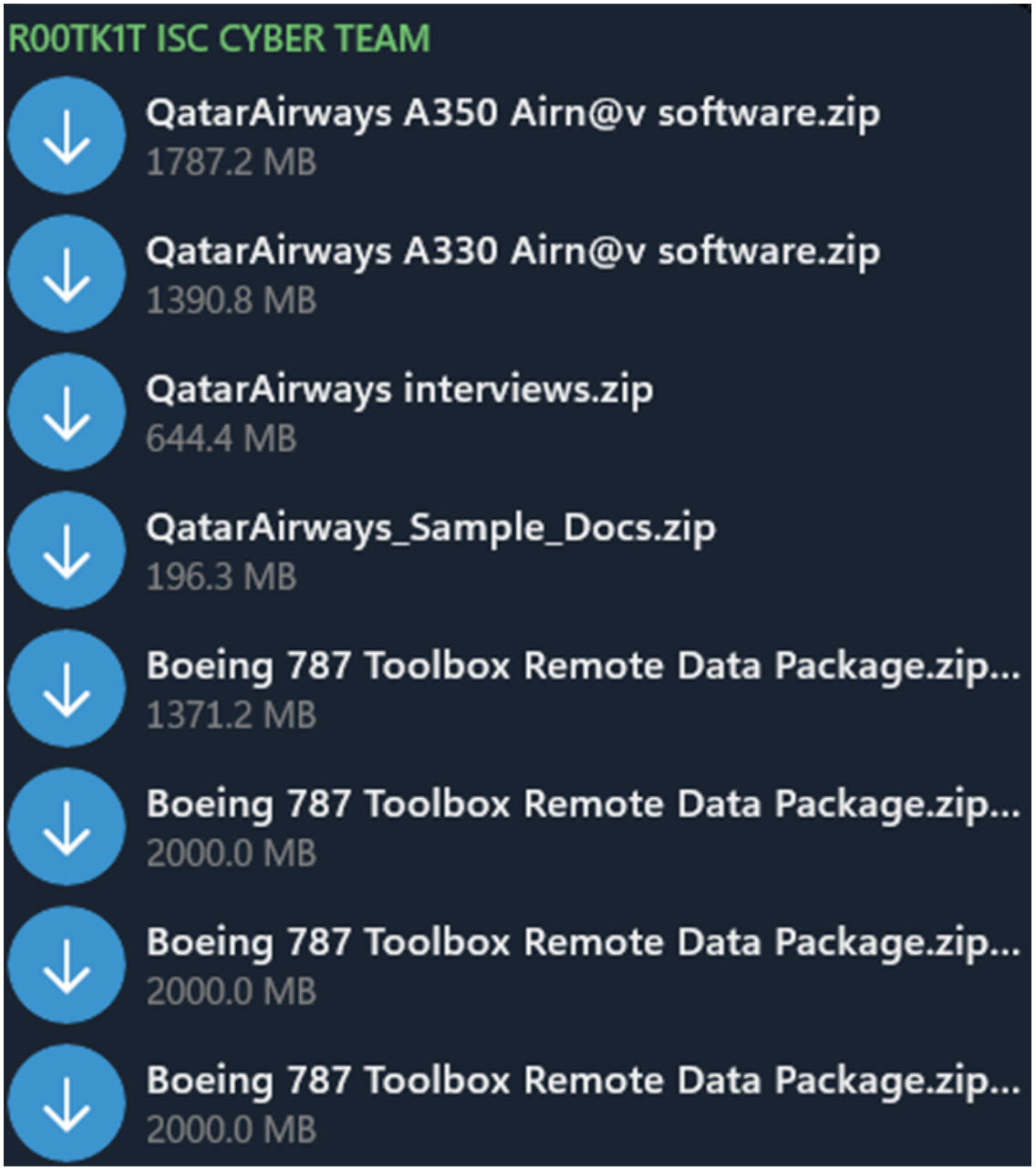
Last but not least, we've decrypted **Qatar Airways sample documents.** From passenger manifests to cargo manifests, from boarding procedures to security protocols, we lay bare the inner workings of this airline.
Nothing is sacred, and the world will know the extent of our reach!

To all the news sites that dare underestimate the evidence we possess, consider this a warning.
We have prepared a special post just for you, exposing your ignorance and incompetence.

Remember, we are **R00TK1T**, and we will continue to expose the vulnerabilities of corporations, institutions, and all those who underestimate our power.
Stay tuned for more chaos, more revelations, and more tales of our conquests!

P.S
We still have more than +400GB of data to go through, Qatar Airways are welcome to reach out to us and prevent the next publications
@R00TK1TOfficial

The threat actor's infiltration extended beyond the Airbus fleet, as they boasted about breaching Qatar Airways' Boeing 787 Toolbox Remote Data Package. This unauthorized access provides this attacker with critical software, maintenance logs, and even control over flight systems, turning the aircraft into their personal playground.



R00TK1T also claimed to have infiltrated Qatar Airways' internal interview recordings, exposing hidden conversations, hiring practices, and decision-making processes within the airline. This breach into the company's internal affairs raises concerns about the compromise of sensitive personnel data and potential impacts on the airline's operations.

Further escalating the severity of the breach, **R00TK1T** alleged they had decrypted Qatar Airways' sample documents, laying bare the inner workings of the airline. The threat actor’s claims suggest that passenger manifests, cargo manifests, boarding procedures, and security protocols are now exposed, challenging the airline's ability to maintain confidentiality and operational security.

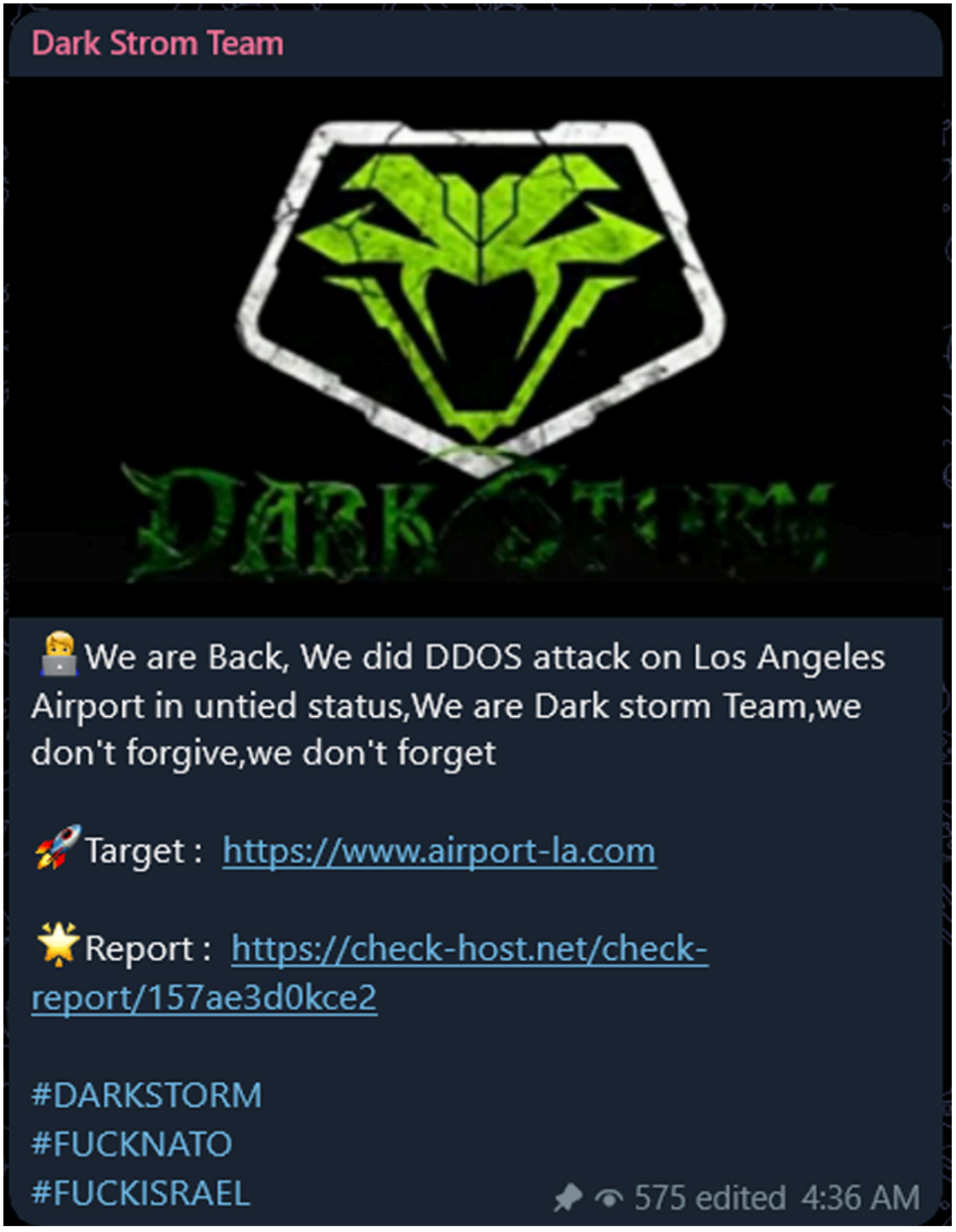
The threat actor also issued a warning to news sites underestimating the extent of the breach, threatening a follow-up post primed to expose the latter’s “ignorance and incompetence” and all those “who underestimate our power.”

R00TK1T concluded their announcement by saying that they have more than 400GB of additional Qatar Airlines data to sift through, offering the company an opportunity to negotiate and prevent further data leaks. The message also included a password for accessing the Qatar Airlines files: R00TK1TDARKNET.

The ominous tagline, "Security Is Just an Illusion, Privacy Is Just Another Illusion," along with a defiant statement against society and the system, adds more panache to **R00TK1T**'s declaration that they can strike "anywhere, anytime." The message serves as a stark reminder that there are threat actors in operation who aspire to disrupt airline operations via increasingly destructive cyberattacks. As such, this sector must remain vigilant against attackers who are becoming bolder, more determined, and more aggressive in their targeting of aviation organizations.

Dark Strom Team's DDOS Attack on Los Angeles Airport

On **February 12, 2024**, Los Angeles International Airport (LAX) fell victim to a disruptive DDoS attack conducted by the **Dark Strom Team.** This incident further underscores the vulnerability of critical aviation infrastructure to cyber threats.



Dark Strom Team, a notorious hacking group, has gained infamy for conducting various cyberattacks, with a particular affinity for DDoS campaigns to overwhelm and paralyze targeted websites.

The attack on LAX on **February 12, 2024**, was characterized by a massive surge in network traffic directed towards the airport's online platforms. The surge in traffic overwhelmed the servers, causing a temporary shutdown of the airport-la.com website and disrupting online services for both passengers and airport staff.

The motivation behind **Dark Strom Team**'s attack on LAX remains subject to speculation. However, the impact was immediate and significant. Passengers relying on the airport's online services for flight information, bookings,

and other essential functions were left in disarray. Airport authorities faced challenges in providing real-time updates, exacerbating the inconvenience caused by the cyberattack.

In response to the DDoS attack, the airport's cybersecurity team swiftly operationalized mitigation protocols. This response involved rerouting and filtering the malicious traffic to restore normalcy to the affected online platforms. The incident prompted a comprehensive review of the airport's cybersecurity infrastructure to fortify defenses against future attacks of this nature.

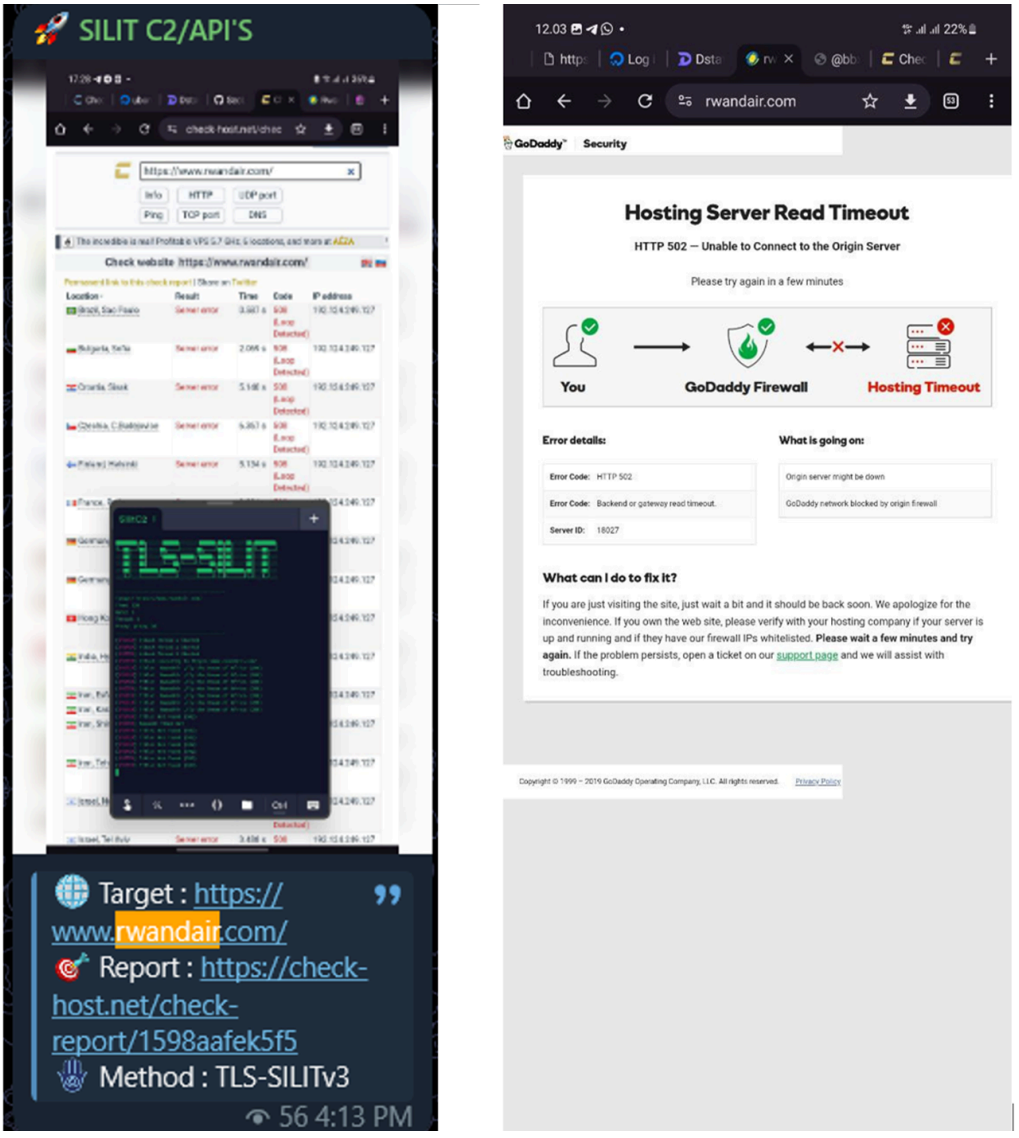
Attributing cyberattacks to specific entities can be challenging, given the anonymity and obfuscation measures employed by hacking groups. Nevertheless, LAX stakeholders initiated an investigation to trace the origin of the attack. LAX’s collaboration with law enforcement and cybersecurity incident response firms intensified to identify the threat actors behind **Dark Strom Team**.

The **Dark Strom Team**'s DDoS attack on LAX highlights the critical need for continuous cybersecurity assessments and the implementation of proactive mitigation measures at airports. This attack highlights the importance of robust incident-response planning, collaboration with cybersecurity agencies, and the implementation of advanced DDoS mitigation strategies to safeguard the continuous operation of essential airport services.

SilitNetwork Targets RwandAir Ltd

On **February 16, 2024**, a hacking group known as **SilitNetwork** launched a cyberattack against RwandAir Ltd, the national flag carrier of Rwanda. This incident highlights the vulnerability of the aviation industry and raises concerns about the potential repercussions on airline operations and passenger data security.

SilitNetwork has gained notoriety for its involvement in cyberattacks that often target high-profile entities for various motives, including financial gain, political considerations, or simply to showcase their hacking capabilities. The group utilizes diverse tactics, techniques, and procedures (TTPs) to breach their targets.



The attack on RwandAir Ltd was a targeted effort aimed at compromising the airline's digital infrastructure. **SilitNetwork** utilized sophisticated methods, possibly including social engineering, phishing, or exploiting software vulnerabilities, to gain unauthorized access to RwandAir's systems. Once inside the airlines network, the hackers exploited weaknesses in the airline's cyber defenses.

The specific motivations behind **SilitNetwork**'s attack on RwandAir remain speculative, as hacking groups often operate with varied objectives. Possible motivations include the theft of sensitive passenger information, disruption of airline operations, or even extortion attempts. The impact, however, was significant, affecting both the airline's digital assets and potentially compromising the confidentiality and integrity of passenger data.

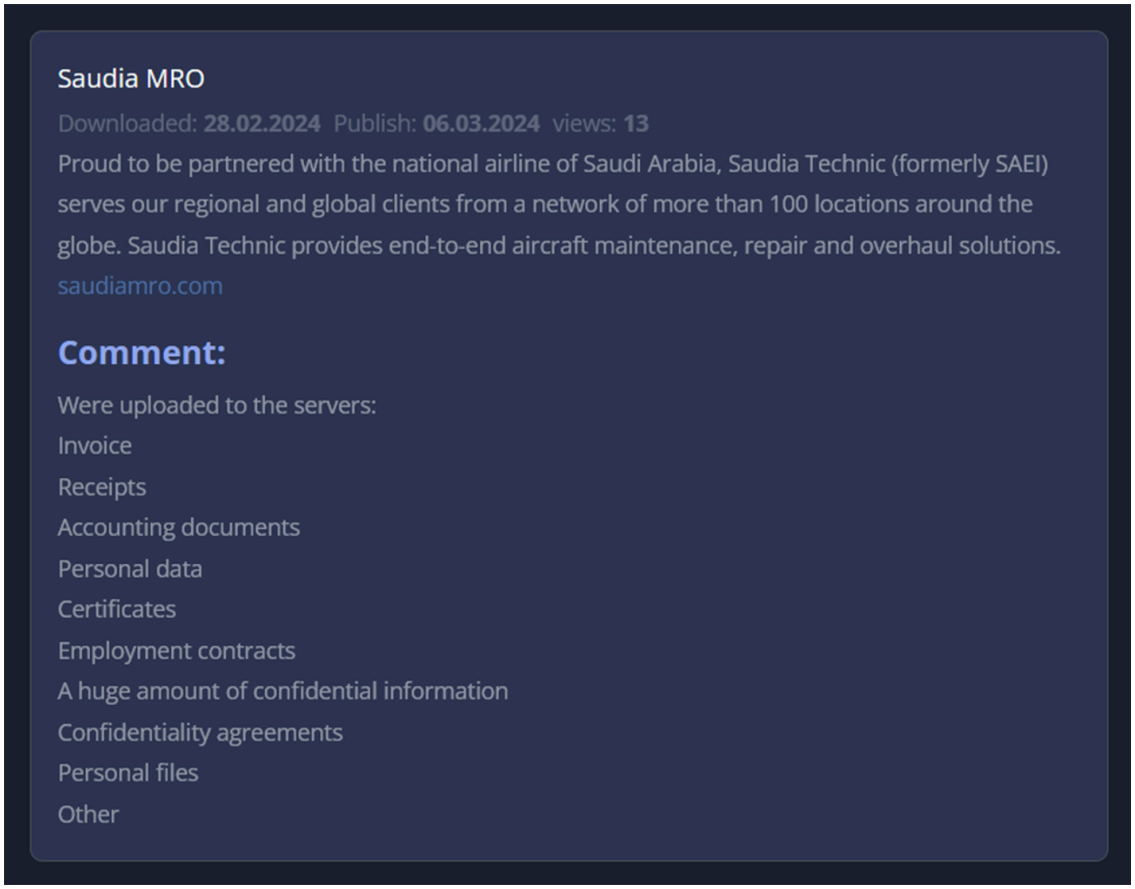
The attack could have disrupted critical operational functions, leading to flight delays, cancellations, or challenges in managing reservations and customer services. Moreover, the compromise of sensitive data poses serious concerns regarding passenger privacy and the potential for identity theft or other malicious activities.

Attributing cyberattacks to specific entities, especially sophisticated hacking groups, is challenging due to the use of sophisticated obfuscation techniques. RwandAir collaborated with national and international cybersecurity agencies to investigate the attack, share threat intelligence, and potentially identify the individuals or entities

responsible for the intrusion. The **SilitNetwork** attack on RwandAir further underscores the need for robust cybersecurity measures and constant vigilance within the aviation industry.

Saudia MRO Falls Victim to 8BASE Ransomware

On **February 28, 2024**, Saudia Technic, the maintenance, repair, and overhaul (MRO) division of Saudi Arabian Airlines, became the target of a severe cyberattack staged by the notorious **8BASE** ransomware gang. This incident not only highlighted the vulnerabilities within critical aviation infrastructure but also raised concerns about the potential impact on aircraft maintenance and operational safety.



8BASE is a sophisticated strain of ransomware known for its ability to infiltrate and encrypt sensitive files, rendering them inaccessible until a ransom is paid. Ransomware attacks have become increasingly prevalent, with threat actors targeting organizations across various sectors for financial gain. This attack typology rose by 600% in 2022, according to Boeing research.

The attack on Saudia Technic involved the deployment of **8BASE** ransomware, which likely entered the organization's network through phishing emails. Once inside, the ransomware variant encrypted crucial files and demanded a ransom payment in exchange for the decryption key.

Compromised targets within Saudia Technic’s systems may have included critical maintenance and operational databases, documentation, and communication channels, thereby disrupting essential Saudi Arabian Airline services.

The primary motivation behind this **8BASE** ransomware attack was financial gain. Threat actors encrypted essential files and demanded a ransom for the release of the decryption key. The impact on Saudia Technic was profound, potentially leading to significant disruptions in aircraft maintenance schedules, operational planning, and communication systems.

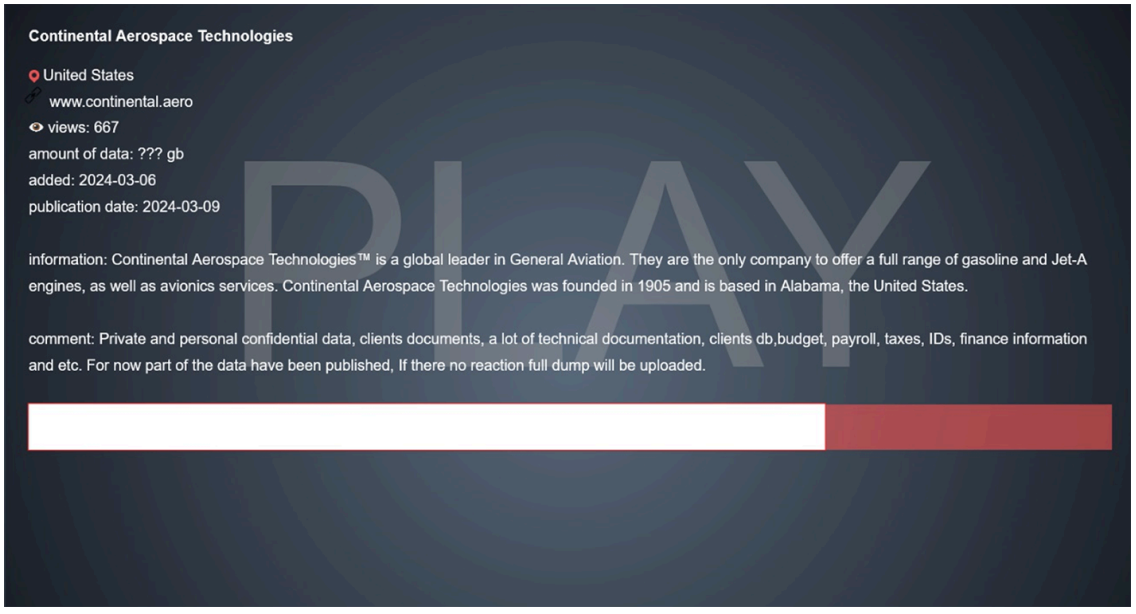
The compromise of maintenance data raises concerns about the integrity of critical safety information, posing risks to aircraft reliability and compliance with aviation regulatory standards. Furthermore, the financial and reputational damage resulting from these incidents can be substantial for affected aviation organizations.

Attributing ransomware attacks to specific threat actors can be challenging due to the use of anonymized payment methods and sophisticated evasion techniques. However, investigators likely conducted probes to trace the origin of the **8BASE** ransomware, understand the attack vector, and gather intelligence to bolster cybersecurity defenses.

The Saudia Technic incident further illustrates the critical importance of cybersecurity in the aerospace sector. It highlights the need for robust measures to protect essential data, ensure the continuity of operations, and safeguard the safety of aircraft systems.

Continental Aerospace Technologies Falls Victim to PLAY Ransomware

On **March 9, 2024**, Continental Aerospace Technologies, an Alabama-based aircraft engine manufacturer, experienced a severe cyberattack attributed to **PLAY** ransomware. This incident underscores the prevailing threats to the aerospace supply chain, echoing the thought leadership of the cybersecurity panelists at last year's Aviation Week conference.



PLAY ransomware is a sophisticated form of malicious software designed to encrypt files on a victim's system, rendering them inaccessible until a ransom is paid. These attacks have become one of the top threats facing the aerospace sector, with threat actors exploiting vulnerabilities in organizational defenses typically for financial gain.

The attack on Continental Aerospace Technologies likely involved the infiltration of their network by threat actors using tactics such as phishing emails, compromised software, or exploiting unpatched vulnerabilities. Once inside the network, threat actors deployed **PLAY** ransomware to encrypt critical files, including manufacturing schematics, operational data, and possibly sensitive employee information.

The attackers subsequently demanded a ransom payment in exchange for providing the decryption key. The primary motivation behind **PLAY** ransomware attacks is financial gain, with threat actors seeking payment in cryptocurrency to release the encrypted files. The impact on Continental Aerospace Technologies was substantial, potentially disrupting manufacturing processes, compromising sensitive intellectual property, and affecting the company's operational efficiency.

The compromise of manufacturing schematics raises concerns about the potential manipulation of design data, potentially leading to faulty components or compromising the safety of aerospace systems. The financial and reputational fallout resulting from such incidents can also be significant for targeted organizations.

Attributing ransomware attacks to specific threat actors is challenging due to the use of anonymous payment methods and evasion techniques. However, Continental Aerospace Technologies likely collaborated with cybersecurity experts, law enforcement agencies, and industry partners to investigate the origins of the **PLAY** ransomware infection chain, analyze the attack vector, and gather intelligence to strengthen future defenses.

The **PLAY** ransomware incident at Continental Aerospace Technologies highlights the critical importance of rigorous cybersecurity assessments in the aerospace manufacturing sector. This attack underscores the need for robust threat-modeling and the implementation of corresponding measures to protect intellectual property, maintain operational continuity, and ensure the safety of aerospace supply chains.

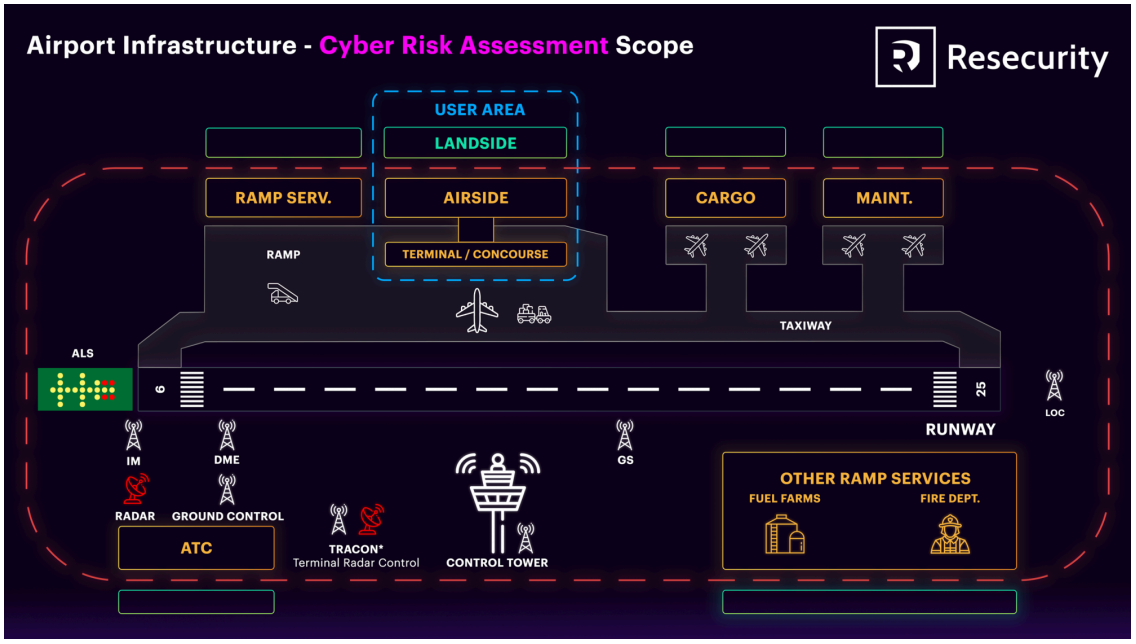
Cybersecurity Risk and Threat Assessment

To mitigate the recent cybersecurity threats and data breaches, we strongly advise conducting proactive cyber risk and threat assessments for businesses in the aviation industry, including their information technology (IT) and operational technology (OT) supply chains.

The scope of the assessment included the following systems:

- **Telecommunications infrastructure and systems**
  - Digital Transmission System (DTS) including Corporate Network
  - Telephony System (TEL)
  - Time Distribution System (TDS)
  - Voice Radio TETRA System (RADIO)
  - Data Broadband Radio System for ground-to-board (BBRS) & Wi-Fi Access (WA)
  - Public Address System (PAS) & Public Information System (PIS) and Commercial TV (COMTV)
  - UPS (backup power supply)
  - Health and safety instrumentation
  - Online-Services and Applications (e-ticketing, e-invoicing, VIP services, etc.)
- **Security systems**
  - Access Control System and Intrusion Detection System (ACS & IDS)

    - Fire Detection System (FDS)
    - Close Circuit TV (CCTV), including Daily Telephony system
- **Supervision systems**
    - Supervisory Control and Data Acquisition (SCADA) system
    - Maintenance Management System (MMS)
    - CCS IT (Common Infrastructure for various CCS subsystems)
- **Fuel farms**
- **ATC and radars**
- **Cargo handling facility**
- **Weather monitoring infrastructure**



How Cybersecurity Assessments Can Help Prevent Incidents

A comprehensive cybersecurity assessment plays a crucial role in identifying vulnerabilities and mitigating risks within an airport's systems. Here's how:

- **Vulnerability Identification:** Assessments can uncover weaknesses in networks, systems, and applications. This approach promotes the timely patching of vulnerabilities before they can be exploited by attackers.
- **Risk Prioritization:** Assessments help categorize identified vulnerabilities based on their severity and potential impact. This enables airports to prioritize resources and address the most critical risks first. Risk triaging is particularly vital in assessing aviation supply-chain security.
- **Security Policy Evaluation:** Assessments evaluate existing security policies and procedures to ensure their effectiveness in preventing attacks. This includes reviewing password complexity, access controls, and incident response plans.

- **Employee Awareness:** Assessments can highlight the need for employee training on cybersecurity best practices. Training can help employees identify phishing attempts and avoid other social engineering tactics. In the BYOD era, training can also help personnel maintain better cybersecurity hygiene on their personal devices.
- **External Threat Monitoring:** Leveraging Cyber-Threat Intelligence (CTI) enhances prevention by providing real-time insights, enabling proactive measures, and fostering collaborative defenses against evolving cyber threats in airport environments.

By conducting rigorous cybersecurity assessments and implementing risk-based measures tailored to their unique threat models, airports can significantly improve their overall security posture and make themselves less susceptible to cyberattacks.

Types of Cybersecurity Assessments

There are various types of cybersecurity assessments, each with its specific focus:

- **Network Security Assessments:** Evaluates the security posture of an airport's network infrastructure, identifying vulnerabilities like weak configurations and unauthorized access points.
- **Vulnerability Assessments:** These assessments focus on identifying specific vulnerabilities within systems and applications used within the airport. This includes identifying outdated software and insecure coding practices.
- **Penetration Testing:** Simulates a cyberattack to identify exploitable weaknesses in systems and applications. This proactive approach allows airports to address vulnerabilities before attackers can discover them.
- **Social Engineering Assessments:** Evaluate employee awareness and susceptibility to social engineering tactics like phishing emails and phone scams.

Airport Cybersecurity Assessment: Scope and Methodology

When conducting a comprehensive airport cybersecurity assessment, it is imperative to address various critical systems that form the backbone of airport operations. cybersecurity assessments are essential to identify vulnerabilities, mitigate risks, and ensure the overall resilience of the airport's infrastructure. The scope encompasses a wide range of systems, each playing a crucial role in maintaining the airport's functionality, safety, and security.

Telecommunications Infrastructure and Systems

Digital Transmission System (DTS), including Corporate Network

The assessment will focus on evaluating the security protocols, encryption methods, and access controls of the DTS and Corporate Network to safeguard sensitive data and prevent unauthorized access.

Telephony System (TEL):

A thorough examination of the Telephony System will include assessing its vulnerability to cyber threats, ensuring secure communication channels, and implementing measures to protect against potential attacks.

Time Distribution System (TDS):

Evaluation of the TDS involves assessing its synchronization mechanisms, timekeeping accuracy, and vulnerability to disruptions to ensure precise coordination across the airport's systems.

Voice Radio TETRA System (RADIO):

The assessment will analyze the security of the Voice Radio TETRA System, emphasizing encryption protocols, user authentication, and measures to prevent interference or eavesdropping.

Data Broadband Radio System for ground-to-board (BBRS) & Wi-Fi Access (WA):

Security assessments will concentrate on the integrity of data transmissions, authentication mechanisms, and safeguards against unauthorized access, ensuring a secure and reliable communication environment.

Public Address System (PAS) & Public Information System (PIS) and Commercial TV (COMTV):

The focus will be on preventing unauthorized access and tampering of information dissemination systems, ensuring the accuracy and reliability of public announcements and information displays.

UPS (Backup Power Supply):

The assessment verifies the security of the backup power supply systems, ensuring their availability during critical situations and safeguarding against cyber threats that may compromise their functionality.

Health and Safety Instrumentation:

Ensuring the cybersecurity of health and safety instrumentation involves evaluating the integrity of data collection, monitoring systems for potential vulnerabilities, and securing critical safety infrastructure against cyber threats.

Security Systems

Access Control System and Intrusion Detection System (ACS & IDS):

The assessment focuses on the effectiveness of access controls, user authentication mechanisms, and the robustness of the Intrusion Detection System to detect and respond to potential security breaches.

Fire Detection System (FDS):

The cybersecurity assessment for the Fire Detection System will emphasize preventing false alarms, ensuring timely detection, and securing communication channels to mitigate potential cyber threats.

Close Circuit TV (CCTV), including Daily Telephony System:

Evaluation of CCTV systems involves assessing the integrity of video feeds, encryption methods, and ensuring secure communication to prevent unauthorized access and tampering.

Supervision Systems

Supervisory Control and Data Acquisition (SCADA) System:

The assessment focuses on securing SCADA systems against cyber threats, ensuring data integrity, and implementing measures to protect against unauthorized access or manipulation.

Maintenance Management System (MMS):

Evaluation of the MMS focuses on securing maintenance-related data, ensuring the integrity of system updates, and preventing unauthorized access to critical maintenance information.

CCS IT (Common Infrastructure for various CCS subsystems):

The assessment evaluates the security of the Common Infrastructure, ensuring that it provides a robust foundation for various CCS subsystems, preventing vulnerabilities that may compromise the entire system.

Fuel Farms

The assessment addresses the security posture of fuel farm systems, ensuring the integrity of fuel-related data, monitoring for potential threats, and implementing measures to prevent unauthorized access.

ATC and Radars

This assessment focuses on securing Air Traffic Control (ATC) and radar systems, ensuring the integrity of communication channels, preventing interference, and safeguarding against cyber threats that may impact aviation safety.

Cargo Handling Facility

The assessment evaluates the security posture of cargo handling systems, emphasizing data integrity, secure communication, and measures to prevent unauthorized access to cargo-related information.

Weather Monitoring Infrastructure

Security assessments for weather monitoring infrastructure focus on ensuring the accuracy of data collection, protecting against potential cyber threats, and securing communication channels to prevent disruptions.

When conducting the Airport cybersecurity Assessment, a combination of vulnerability assessments, penetration testing, and regular audits will be employed. The methodology will prioritize identifying potential weaknesses, recommending mitigations, and ensuring ongoing monitoring and adaptation to the evolving cyber-threat landscape. The overarching goal is to fortify the airport's systems against cyber threats, ensuring the ongoing safety and operational continuity of airport systems.

Conclusion

The aerospace and aviation industries face a rapidly evolving threat landscape, making cybersecurity assessments an indispensable protocol for safeguarding airports, airlines, and passengers. By conducting regular assessments, airports can identify vulnerabilities, prioritize risks, and implement effective security measures. This proactive approach helps to mitigate the risk of malicious cyber incidents, ensuring smooth operations, protecting sensitive data, and safeguarding employees and passengers.
