EATM-CERT

European Air Traffic Management
Computer Emergency Response Team

EUROCONTROL

2024 Report on Cyber in Aviation

TLP:GREEN

CONSORTIUM COORDINATOR sesar DEPLOYMENT MANAGER

FOUNDING MEMBER sesar JOINT UNDERTAKING

NETWORK MANAGER

Contents

Foreword

by Patrick MANA
EUROCONTROL
EATM-CERT Manager

We proudly unveil the **fifth** edition of our annual report on cyber in aviation, offering unprecedented insights into the industry's cyber threat landscape. This report marks a **significant step forward** in our collective endeavour to comprehend and counter the cyber risks confronting aviation. Our gratitude extends to the **multitude of organizations worldwide** who have generously **contributed** to this report, resulting in an unparalleled wealth of data.

This past year has seen a notable **surge** in both the **quantity and diversity of reported cyber events** impacting aviation. Additionally, for the first time, our report showcases a **"wall of fame"**, adorned with the logos of entities that have shared their cyber events with us, embodying a spirit of collaboration within the aviation community. When we conceived this idea and sought contributors' approval, uncertainty lingered regarding its reception. However, the overwhelmingly positive response surpassed our expectations, signalling a shift in perception: **being the victim of a cyber-attack carries no stigma or blame.** It is a shared reality, and collective sharing is caring.

The burgeoning cyber-security culture of sharing is evolving to our mutual advantage, with the "wall of fame" serving as evidence and a catalyst for fostering and elevating this culture to greater heights of excellence. As in the previous editions, we have taken meticulous care to ensure the **anonymization of all events,** preserving confidentiality and preventing any association between events and organizations within this report.

Another noteworthy enhancement in this edition lies in the **quality of event** descriptions. Virtually all contributors have adhered to our suggested reporting template, furnishing comprehensive details conducive to more in-depth analysis. This demonstrates a marked **maturity advancement** within aviation stakeholders, evidencing their heightened proficiency in identifying and analysing encountered cyber threats and attacks.

Trend analyses become more and more pertinent for some aspects of the aviation cyber threat landscape as the reporting baseline matures over the years and editions of this report, in particular, for the number of reported ransomware, DDoS, scams impersonating EUROCONTROL, and detected credential leaks and fraudulent websites impersonating aviation stakeholders.

I extend my heartfelt gratitude to all organizations whose invaluable contributions have facilitated the creation of this comprehensive global aviation cyber threat landscape report. By sharing their cyber events from 2023, these entities have played an indispensable role in revealing the evolving cyber risks faced by the aviation industry. A special expression of gratitude is reserved for those who graciously consented to be featured on our "wall of fame."

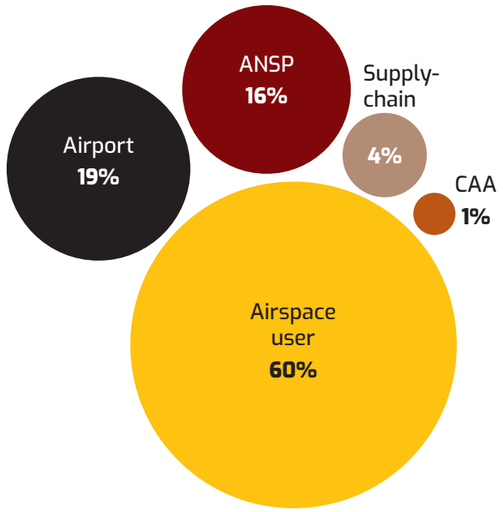


Figure 1: 2023 Attack surface

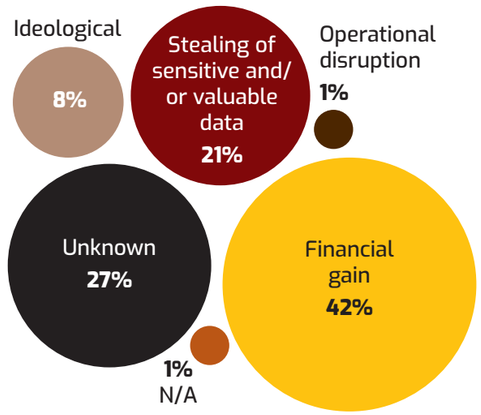


Figure 2: Threat actor motivation

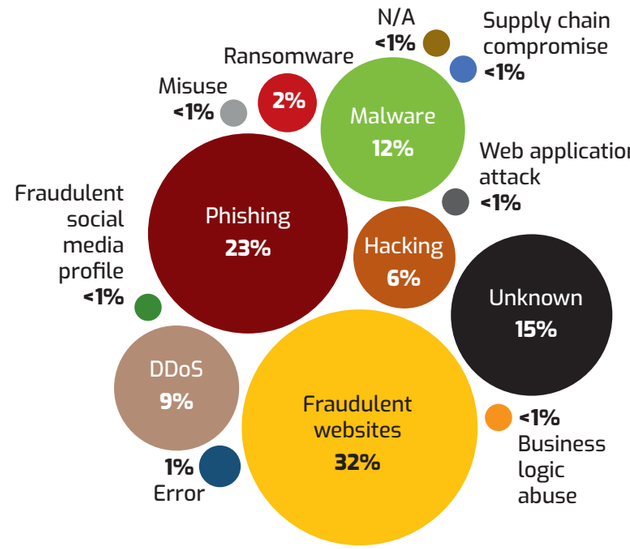


Figure 3: 2023 Adversaries Threat Vector

Executive Summary

We are pleased to present the fifth edition of the EUROCONTROL/EATM-CERT report on cyber in aviation, reflecting a significant enhancement in our dataset. This year, we have detected and collected **2.3 times more events** compared to last year, thanks to increased contributions from a broader range of stakeholders.

The report, which exclusively uses this enriched dataset, paints a detailed picture of the aviation cyber threat landscape for 2023. Notably, we have refined our stakeholder categories by introducing a new one: the **Supply Chain**. This category includes entities providing services, systems, or applications to aviation operators such as ANSPs, Airport Operators, Airspace Users, and Civil Aviation Authorities. It now covers Original Equipment Manufacturers (OEMs) as well as various manufacturers or vendors whose products, services and systems are integral to aviation.

While **Airspace Users remain the primary targets** of cyber-attacks, enhanced reporting from **airports and ANSPs** has resulted in a more balanced distribution of events. The Supply Chain's reported events, although increasing from 164 in 2022 to 225 in 2023, still represent a smaller percentage (4%) due to the substantial rise in overall reports from aviation operators. Enhancing the collection of reports from the Supply Chain stakeholders is a focus for future editions. It is increasingly evident that aviation's reliance on the cyber-resilience of its supply chain is crucial. Promoting **security by default for products, services, and systems**, e.g. cloud services, and elevating the supply chain's maturity level beyond mere regulatory compliance e.g. Part-IS or NIS2 in Europe, are areas for future attention.

Cyber threat actors continue to be **predominantly financially motivated**, either directly through theft and extortion or indirectly by selling valuable information, data, or know-how. Consequently, the primary impact of cyber-attacks on aviation remains financial, with an estimated global impact still in the billions of euros annually.

The surge in ideologically-driven cyber-attacks observed last year has not only persisted but has escalated. Although the percentage dropped slightly from 12% in 2022 to 8% in 2023, the actual number of such events soared **from 318 in 2022 to 528 in 2023,** influenced by ongoing and new conflicts like those in Ukraine and between Hamas and Israel.

The preferred methods for conducting cyber-attacks — **fraudulent websites, phishing, DDoS, malware, hacking, and ransomware** — have remained largely unchanged. Certain patterns emerge, revealing that specific categories of stakeholders are more affected by particular attack vectors. e.g. **DDoS on airports** (64% of DDoS on aviation), **ransomware on the Supply Chain** (63% of ransomware on aviation), fraudulent websites on Airspace Users (98% of aviation fraudulent websites), malware on Airspace Users (57% of aviation malware), hacking (84% of aviation hacking). Though others are more evenly distributed e.g. phishing.

However, the frequency of occurrences alone does not tell the whole story. The severity of the impact is equally crucial. For instance, a ransomware attack can lead to extremely costly repercussions, not just for the victim but also for its customers or service users. The severity of incidents targeting the aviation industry has risen, with 35% now falling under Medium, High, or Critical categories, a notable increase from the 23% in 2022. Notably, there were **7 Critical** events reported. However, it is important to note that **no reported cyber events have impacted flight safety.**

This report underscores **the necessity of vigilance against cyber threats**, which show no signs of diminishing. The key questions remain: **Is the associated risk acceptable, and are investments in people, processes, and technology sufficient to achieve and sustain that goal?**

Planning ahead is vital: **It was not raining when Noah built his ark!**

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

Behind the Screens: **Understanding the Motivations of Cyber Threat Actors**

In the process of preparing this annual report on cyber in aviation, various biases can come into play, potentially influencing the objectivity and accuracy of the analysis.

One of the most significant biases is the **Field of View Bias**. This bias occurs when an analyst's perspective is limited by their specific focus or area of expertise, causing them to overlook or undervalue information outside their immediate field of view. This can lead to a narrow interpretation of data, missing out on broader trends or connections.

Other biases include **Confirmation Bias**, where analysts may favor information that confirms their pre-existing beliefs or hypotheses, and **Anchoring Bias**, where initial information, impressions, or data disproportionately shape the subsequent analysis.

There is also the **Availability Bias**, which is the tendency to rely on immediate and readily available information, rather than seeking out a more comprehensive data set.

EATM-CERT intelligence analysts being fully aware of these biases strive to mitigate their effects to ensure the most accurate and objective reporting. This includes continually broadening one's field of view to encompass a wider range of information and perspectives.

The aviation industry, a critical node in the global infrastructure, is confronted with an evolving cyber threat landscape teeming with challenges. Identifying the threat actors behind these cyber-attacks and understanding their motivations is a critical step in formulating robust defense strategies. The threat actors in this volatile cyber threat environment range from **state-sponsored** entities to sophisticated **cyber criminal** organizations, **hacktivists, insider threats,** and **ransomware operators**, each possessing diverse and often intricate motivations.

This section of the report provides an in-depth analysis of the threat actors targeting the aviation sector, categorizing them based on their identities and examining the driving forces behind their malicious activities. Our objective is to shed light on these elements, thereby providing a comprehensive overview that enables the aviation industry to better anticipate, respond to, and mitigate these threats. This, in turn, will enhance the resilience and security of the aviation ecosystem.

The Faces of Cyber Deception: a Closer Look at Cybercrime Actors

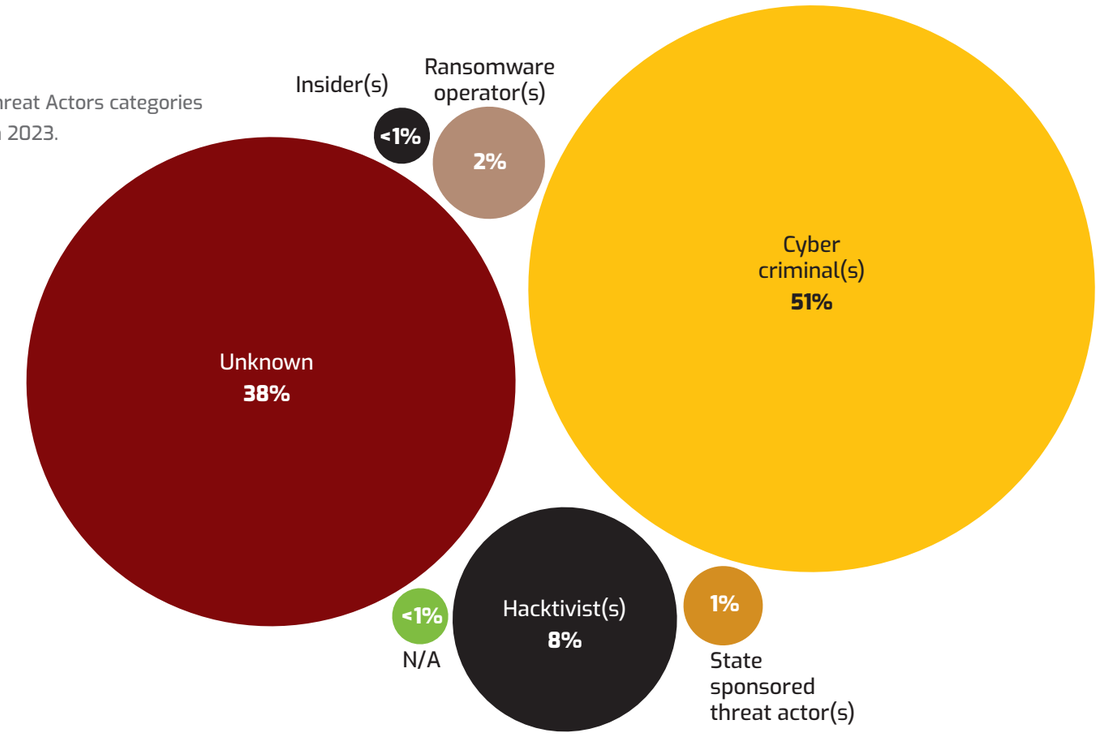
Cyber criminal organizations emerge as the **most significant category of adversaries.** These organizations have been responsible for **3.209** attacks, accounting for approximately **50.8%** of the total 6.320 incidents recorded.

Upon analysing the motivations of these threat actors, it becomes evident that financial gain is a significant driving force, with **2.667** attacks (**42%** of the total) being **financially motivated**. This underscores the potential profitability of exploiting the aviation industry's critical systems.

The **aviation** industry is particularly **vulnerable to financial fraud and identity theft** attacks orchestrated by cyber criminals, largely due to its complex network of payment systems, booking platforms, and supply chain dependencies. Cyber criminals can manipulate booking and ticketing systems to issue fraudulent tickets or vouchers, which are then sold to unsuspecting customers for illicit profit.

Moreover, the industry's intricate **supply chain** can be exploited by cyber criminals, introducing vulnerabilities that can lead to financial theft or fraud through activities such as payment redirection or false invoicing.

Figure 4: Threat Actors categories observed in 2023.



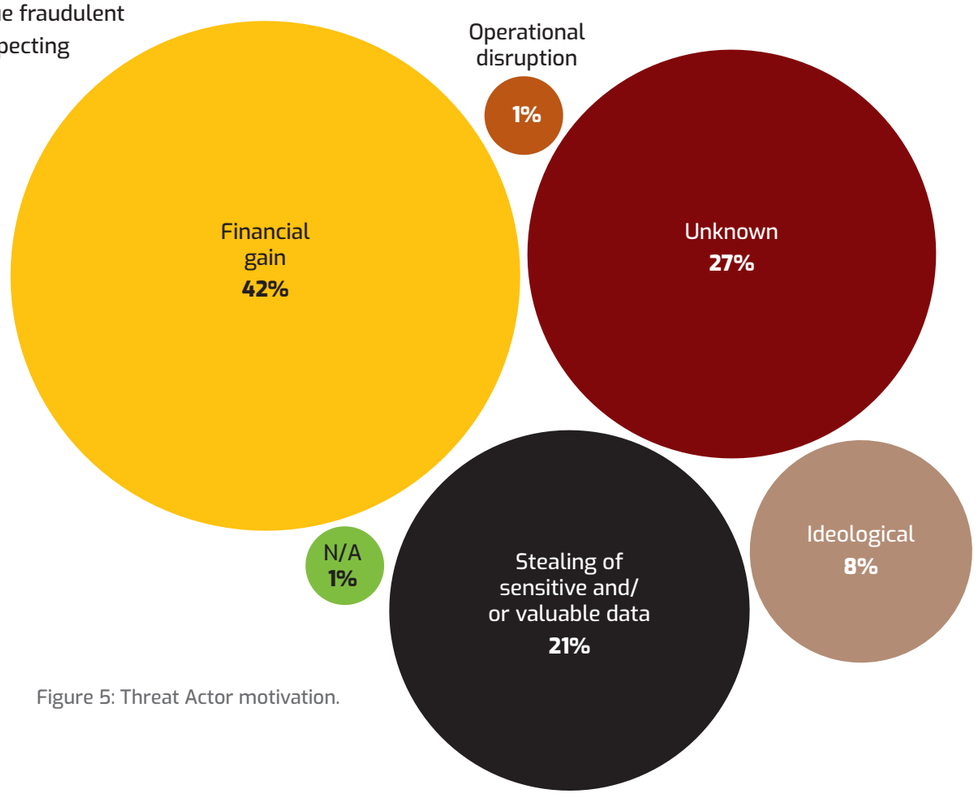


Figure 5: Threat Actor motivation.

Cyber criminal organizations often **target more than just financial systems**; they also seek to acquire sensitive data, primarily to leverage this information for various fraudulent activities. The **theft of sensitive or valuable data accounts** for **1.306** attacks (**21%**), highlighting the aviation industry's vulnerability to information theft.

While cyber criminals often exploit these systems to steal credit card and banking information, or personal data that can be used to create fraudulent identities for various illegal activities, the threat landscape is not limited to these actors. State-sponsored groups and other actors with strategic interests may also conduct cyber espionage operations within the aviation sector. In such instances, the exfiltration of sensitive data can serve broader political or economic objectives, such as gaining insights into proprietary technologies, gathering intelligence on strategic infrastructure, or monitoring the movements and activities of individuals.

Digital Protest: Exploring the Landscape of Hacktivism

Hacktivist groups emerge as **the next major category of threat actors** targeting the aviation industry. They have orchestrated **501** attacks, which account for approximately **8%** of the total recorded incidents. These groups often **exploit the high visibility of the aviation sector to magnify their messages and influence public opinion or government policies.**

These attacks are typically carried out by groups guided by political, social, or religious ideologies, utilizing the cyber domain to advance their causes. Hacktivists employ cyberattacks as a tool to advocate or protest specific political, religious, or other ideologies, and they are known to engage in **DDoS** and other disruptive activities.

Significant events in the political and military spheres have prompted various threat actors to launch ideologically driven attacks against targets within the adversaries of the conflict. This trend has been further reinforced and peaked following **the Russian invasion of Ukraine**, illustrating the intricate relationship between global events and cyber warfare.

The surge in hacktivist attacks since 2022 can be attributed to the Russian invasion of Ukraine, an event that likely spurred these groups to target the aviation industry as part of their wider political agenda. Another significant event that led to the increase in cyberattacks concerning ideologically motivated hacktivism was a **Hamas attack on Israel in October 2023**.

Nation vs. Nation: Exploring the Landscape of State-Sponsored Cybercrime

State-sponsored cyber-attacks on aviation stakeholders constitute a strategic and intricate aspect of the broader cyber threat landscape. These attacks, often motivated by political and economic factors, can have extensive implications. Efforts to gather intelligence aim to reveal **proprietary technologies** and crucial i**nfrastructure insights,** potentially providing the attacking state with a technological edge. Simultaneously, the intentional disruption of the aviation industry can result in significant economic consequences, both by directly affecting trade and travel and by extracting valuable technological innovations.

In understanding the strategic motivations behind state-sponsored cyber threats, the aviation industry must also contend with the complex and often opaque relationships these actors may establish. State-sponsored threat actors, responsible for **47** attacks and making up **1%** of the total incidents, **operate with complexities that go beyond mere numbers.**

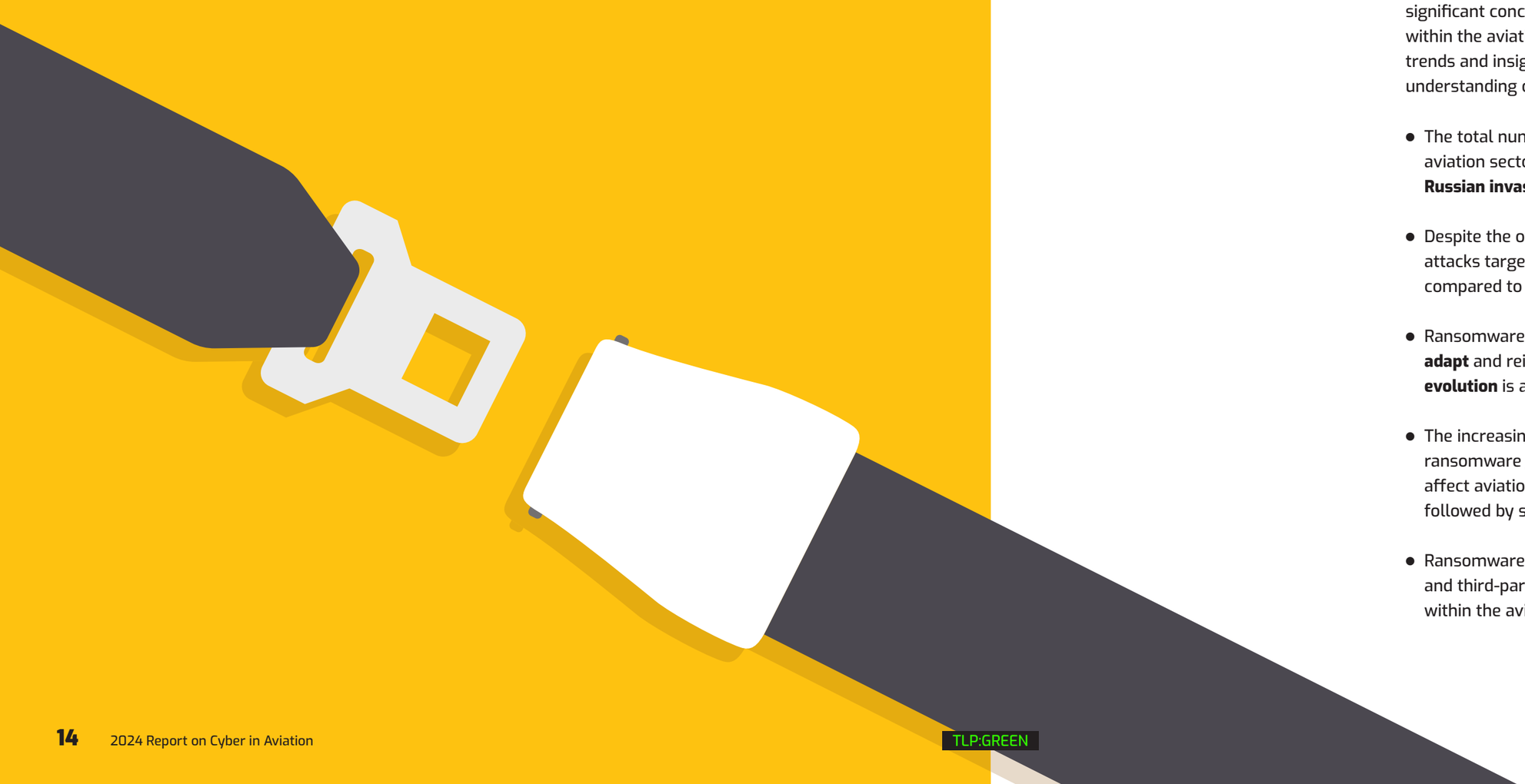
However, it is important to note that **attribution is challenging**, particularly for state-sponsored groups, and **is not the responsibility or burden of an aviation stakeholder.** This results in a limited number of cyber-attacks truly attributed to such groups of threat actors. The potential widespread impact of these attacks is amplified by their strategic targeting, serving broader political or economic agendas that can have industry-wide effects.

A subtle aspect to consider is the **alliances state-sponsored actors may form with cyber criminal gangs**, using them as proxy forces. Furthermore, state-sponsored operations might strategically align with or support non-state proxies, such as terrorist organizations, hacktivist groups, and cyber criminal organizations reflecting shared objectives or adversaries. **This intersection of interests adds a sophisticated layer to their motivations and complicates attribution.**

It is also crucial to emphasize that state-sponsored actors do not solely target the aviation industry; they conduct operations against various sectors, with the aviation domain being one of many areas of interest.

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

Turbulence Ahead:
The Impact of Ransomware on the Aviation Sector



Ransomware operators were involved in **108** incidents, accounting for **2%** of the total figure. The situation with ransomware groups is **complex and may go beyond simple financial motivations**. There are signs that some **ransomware operators may form alliances with states,** collaborating with them when their objectives align. Involvement in ransomware attacks has been observed even among state-sponsored actors and hacktivist groups. This multi-dimensional alignment and potential collaboration have led to the classification of ransomware operators as a distinct group, acknowledging their unique and often ambiguous role within the broader cyber threat landscape. Given these considerations, we have included a **dedicated section in this report on ransomware groups** to provide a more in-depth understanding of these cyber criminals.

In the intricate world of cybersecurity, ransomware remains a significant concern. As we delve into the dynamics of this threat within the aviation sector, the year 2023 offers several notable trends and insights. This context is vital as we deepen our understanding of the ransomware landscape impacting aviation.

- The total number of **ransomware incidents** reported in the aviation sector has returned to the **level observed before the Russian invasion of Ukraine in 2022.**
- Despite the overall growth, the proportion of ransomware attacks targeting Airspace Users remains at a similar level compared to 2022.
- Ransomware groups demonstrate a **chameleon-like ability to adapt** and reinvent themselves to their environment. **Constant evolution** is a characteristic of their operations.
- The increasing adoption of a **multi-extortion strategy** by these ransomware groups observed in other sectors appears to also affect aviation, involving covert extraction of sensitive data, followed by system encryption.
- Ransomware groups are **exploiting supply chain vulnerabilities** and third-party risks, targeting interconnected organizations within the aviation sector.

The aviation sector, a vital component of global connectivity, commerce, and defense, is confronted with the challenge of a complex and rapidly evolving cybersecurity landscape, which includes threats like ransomware attacks. In 2020, there were **62 reported** ransomware incidents. This number increased to **119 in 2021**. However, by **2022**, the incidents decreased to **97**, indicating a reduction in these types of attacks. Returning to **108 in 2023**.

In this dynamic landscape, it is essential to comprehend the specific ransomware groups behind these incidents. This understanding not only aids in identifying their tactics and strategies but also empowers stakeholders to devise more effective defenses. A variety of threat actors have been identified as conducting ransomware attacks against aviation industry stakeholders.

In the context of ransomware attacks against the aviation industry, particular attention must be given to the activities of three active groups. **LockBit** leads the pack, accountable for 27 out of the 108 known attacks, or approximately 21% of the total. **ClOP** follows with 14 attacks, constituting roughly 13% of the overall figure. **BlackBasta's** 7 known incursions represent around 6% of the identified attacks. Collectively, these three groups alone have orchestrated nearly **41%** of the detected ransomware attacks against aviation systems.

All of the mentioned ransomware groups, including Lockbit, ClOP, and BlackBasta, display certain common characteristics that highlight their significant threat to global cybersecurity. These groups are **not confined by geography or sector**, demonstrating a global reach with sophisticated attack techniques. They are capable of launching attacks **against both Windows and Linux systems**, reflecting a wide and adaptable technological proficiency. Unlike some cybercriminal entities that focus on specific industries, these groups target a **diverse range of sectors**, from healthcare to manufacturing and beyond.

Moreover, their potential association with other groups indicates a complex and interconnected network of criminal alliances. A significant commonality among these groups is their operation as **Ransomware-as-a-Service** (RaaS) providers. RaaS is a business model where the developers of ransomware offer their malicious software to affiliates or partners, who then execute the attacks. The proceeds from successful ransom payments are typically divided between the developers and the affiliates.

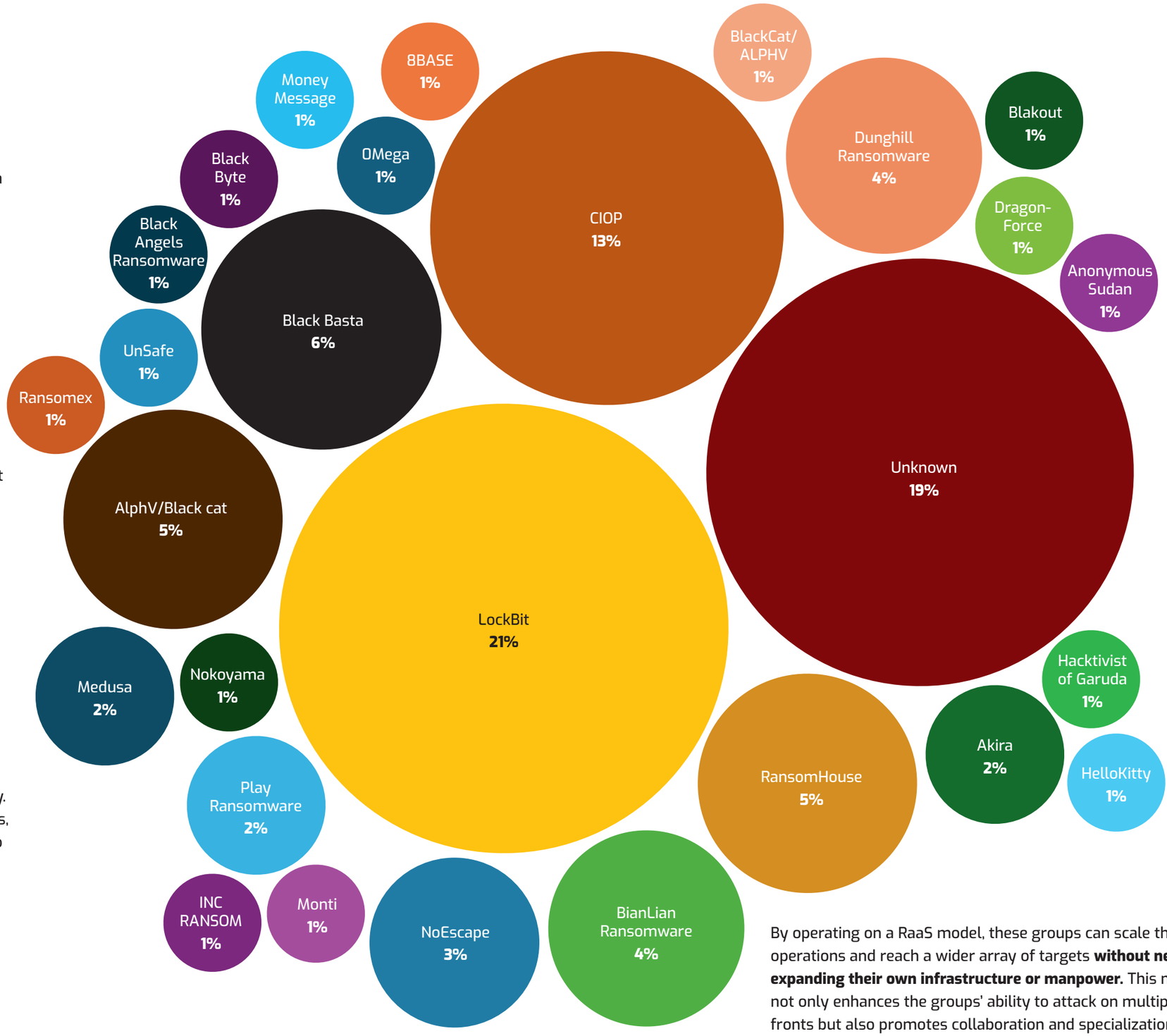


Figure 6: Ransomware groups in 2023

By operating on a RaaS model, these groups can scale their operations and reach a wider array of targets **without necessarily expanding their own infrastructure or manpower.** This model not only enhances the groups' ability to attack on multiple fronts but also promotes collaboration and specialization within the cybercriminal community, making defenses against such coordinated threats even more challenging.

Ransomware has emerged as an extremely profitable enterprise for cybercriminals. The primary initial vectors for most ransomware operators continue to be **spear phishing and stolen credentials**. Equally alarming is the evolution of tactics used by ransomware groups to maximize their leverage on victims. A notable trend observed is the increasing adoption of a **double and even triple extortion strategy,** which essentially involves three stages of victim exploitation.

The first stage involves the cybercriminals infiltrating the victim's network to covertly extract sensitive data. They often target the most critical and confidential information to maximize the potential impact. This extraction phase is usually conducted with surgical precision, with the threat actors aiming to remain undetected.

In the second stage, the perpetrators initiate the encryption of the victim's systems, paralyzing their operational capacities. With their data held hostage and their systems rendered inoperative, the victims find themselves under immense pressure. The final stage introduces an additional layer of extortion.

The criminals' bargaining power may be strengthened by the triple threats of persistent system downtime, the risk of sensitive data exposure, and the threat of public data leak. In exchange for the ransom, victims are promised a decryption key to restore their encrypted systems and an assurance that the extracted data will not be leaked on the internet.

Ransomware threat actors are **increasingly exploiting vulnerabilities in supply chains and third-party service providers.** These organizations, often involved in handling sensitive data, are becoming attractive targets due to their interconnectedness with larger entities within the aviation sector. It is speculated that these organizations are perceived as more likely to pay the demanded ransom due to the high stakes' nature of their data and their associations.

In addition to direct attacks, third-party and supply chain vulnerabilities also provide a backdoor for threat actors to the larger entities they service. This trend underscores the growing prevalence and success of supply chain attacks in the current threat landscape.

The impact of ransomware attacks extends far beyond the immediate disruption of systems. Such incidents can potentially lead to significant financial losses, unauthorized acquisition of sensitive information, damage to an organization's reputation, and even legal repercussions.

Their effects are not only confined to the immediate disruption of operations but can, in some cases, extend to a variety of interconnected stakeholders and systems. An illustrative example of this was when several flights were grounded following a ransomware attack, causing significant service disruptions and economic loss.

Even without paying the ransom, organizations still face **substantial costs after a ransomware attack**. These expenses include lost revenue due to operational downtime, costs for restoring or replacing compromised systems and data, and additional investments in cybersecurity enhancements. Potential legal and regulatory costs may also arise in the event of data breaches.

From a strategic perspective within the aviation industry, it is crucial to note that there are **not any cyber threat actors who exclusively target aviation stakeholders.** Rather, ransomware groups operate with an opportunistic approach, targeting a variety of organizations across diverse sectors. However, it is essential to highlight that these groups often **select their targets based on potential profitability,** seeking out organizations from which they can extract substantial ransoms. Their approach is fundamentally pragmatic, and the aviation industry, with its vital infrastructure, large service, and extended financial resources, is undeniably a part of their potential target pool.

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

The Anatomy of Aviation Cybersecurity:

A Breakdown of Attacks and Threat Patterns

Comprehending the **adversaries** that **attack** the aviation sector offers **crucial knowledge** about the **'who' and 'why' behind the attacks.** However, it is equally **important** to investigate **'how'** these actors **initiate** their **attacks**. Various stakeholders in the aviation industry, such as Airspace Users, Aviation Supply Chain providers, Airports, Air Navigation Service Providers (ANSPs), and Civil Aviation Authorities (CAAs), are subject to a broad range of advanced methods. This section examines the specific attack vectors and techniques used against these diverse stakeholders.

As we **shift** our attention **from identifying** the threat **actors to understanding the strategies** they use, it **becomes clear** that the **tactics** employed to **target aviation** stakeholders are as **diverse** and **intricate** as the actors themselves. Threat **actors** have **taken advantage** of these **vulnerabilities** through a broad array of **attack vectors**, including Ransomware, Phishing, Misuse, Malware, Hacking, Fraudulent Websites, Errors, DDoS, Web Application Attacks, Business Logic Abuse, and Physical Access.

In 2023, EATM-CERT **detected and reported** a total of **6.320** cyberattacks affecting various aviation stakeholders. The spread of these attacks was extensive, with:

- **Airspace Users** experiencing **3.762** incidents,
- **Airport Operators** suffering **1.220,**
- **Aviation supply** chain providers facing **225**,
- **Air Navigation Service Providers** (ANSPs) dealing with **1.011,**
- **Civil Aviation Authorities** (CAAs) encountering **88.**

The **distribution** of **attacks** detected by EATM-CERT and reported by stakeholders in **2022** and **2023** shows considerable **differences** among various aviation **stakeholders**.

- **Airspace Users** bore the brunt, with the attack percentage **dropping** from **76% in 2022** to **60% in 2023**.
- Attacks on **airports grown** from **15% in 2022** to **19% in 2023.**
- **ANSPs** also saw a growth, from **2% in 2022** to **16% in 2023**.
- The least impacted were the **CAAs - 1%** of attacks in **2022** and in **2023.**
- The attacks on **Aviation Suply Chain** providers **dropped** from **6% in 2022** to **4% in 2023.**

A detailed **analysis** of these **attack vectors** offers a glimpse into the **diverse strategies** used. **Fraudulent Websites** topped the list with **2022 attacks (~32% of the total),** followed by **Phishing** with **1.458** incidents **(~23%)**, **Malware** related attacks with **741 (~11%)** and **DDoS 562 (~9%)**. **Ransomware** was accountable for **92** incidents **(~1.5%)**, and **Web Application Attacks** were reported in **5** cases **(0.08%). Errors** led to **33** incidents **(0.5%)**, with **Hacking** at **385** incidents **(6%), Business Logic Abuse** in **2** incidents **(0.03%),** and **Misuse** in **16** cases **(0.25%). Unknown** vectors accounted for **1.039** attacks **(~16.5%).**

The sheer volume of these attacks highlights the intricate and evolving nature of cyber threats in the aviation industry, and a closer look at the data reveals the distribution of these attacks among various stakeholders over the past year.

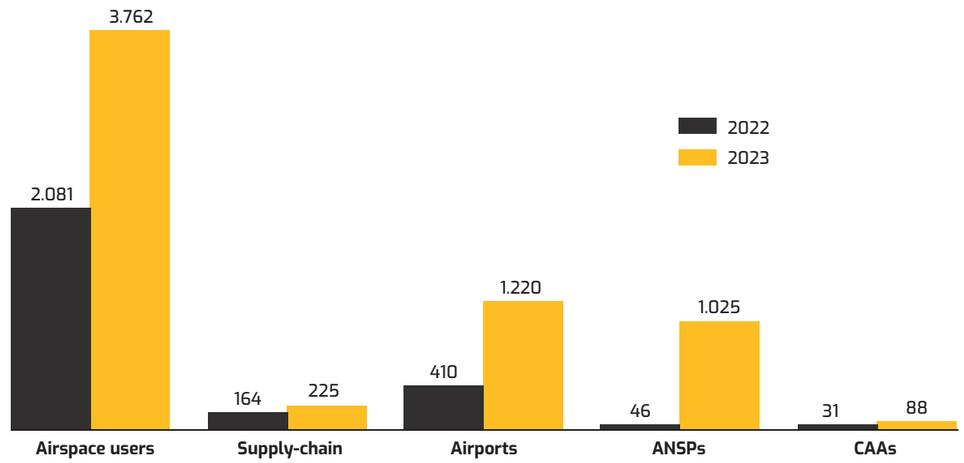


Figure 7: 2022 and 2023 threat attack surface comparison

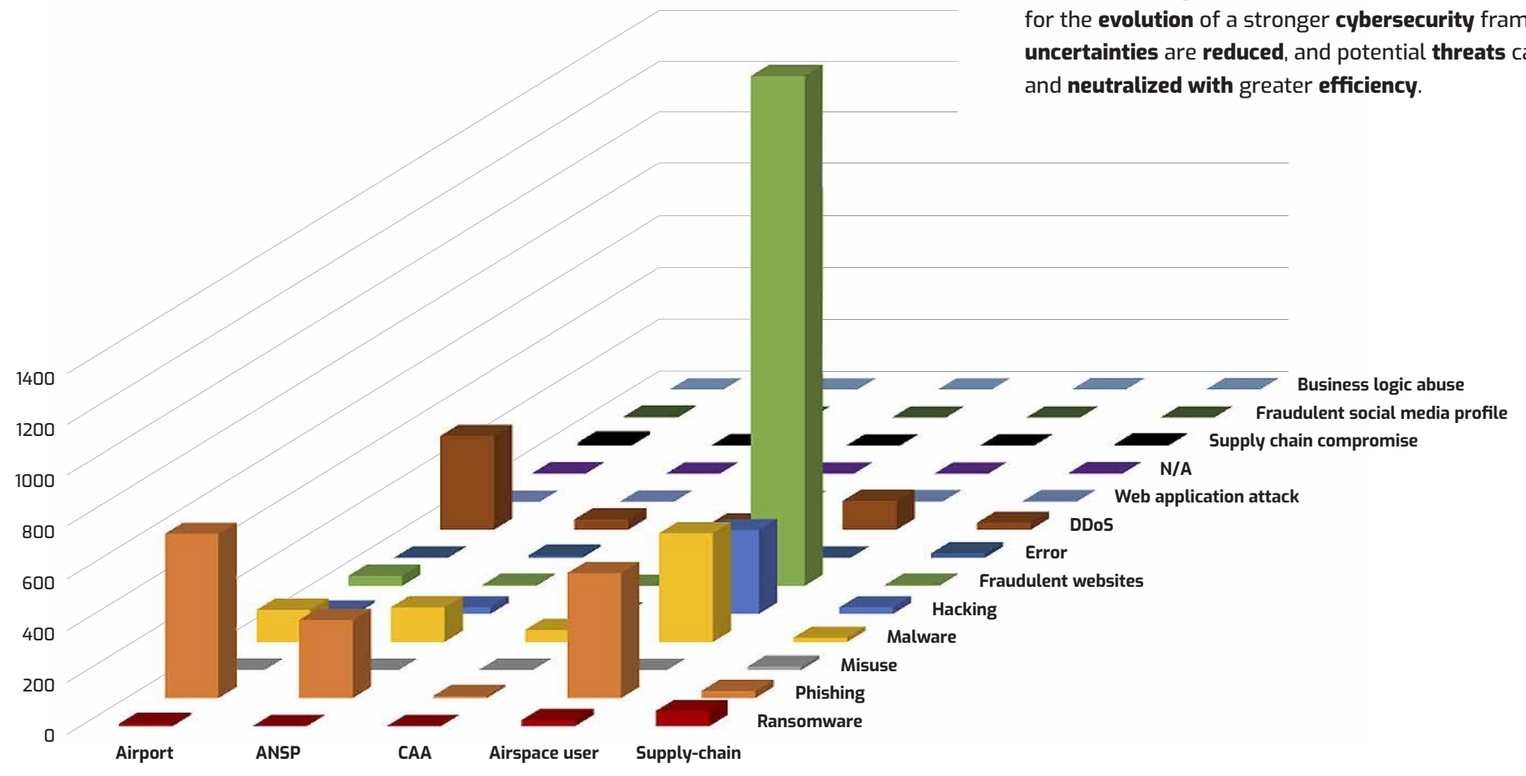


Figure 8: 2023 Attack type distribution

The Enigma of Airspace: Deciphering the Unknowns in Aviation Cybersecurity

Cybersecurity events are often shrouded in **uncertainty. EATM-CERT compiles** information from **diverse sources**, such as the **dark web, digital marketplaces, messaging apps, and various social and news media outlets**. Yet, the **specifics** of cyber incidents **are rarely divulged** by those impacted, with the **bulk of information** typically **limited** to a **press release** or **emerging** in yearly **summaries** shared with EATM-CERT. This **leads** to a **substantial number of uncertainties**, which **EATM-CERT** is **dedicated** to **diminishing by refining** the **data** through different strategies. Nonetheless, there's an **encouraging sign** of progress, with the **steady enhancement in the** exchange of **information** each year, reflecting an **increased** consciousness and **readiness to communicate details of incidents** among network members. This **advancement** is **vital** for the **evolution** of a stronger **cybersecurity** framework where **uncertainties** are **reduced**, and potential **threats** can be foreseen and **neutralized with** greater **efficiency**.

Fraudulent Websites Spearheaded Cyber Theft Against Airspace Users

In **2023**, **Airspace Users** in the aviation sector were **exposed** to a wide variety of **cyberattack vectors**. Among these, **Fraudulent Websites** emerged as the most common type of incident, with **1.975** instances. This provides valuable insight into the threat **actors** who specifically **target Airspace Users**, highlighting that **fraudulent websites are a particularly preferred tool.** While **fraudulent websites** make up **32%** of the total attacks across all aviation stakeholders, a closer look at the attacks on **Airspace Users** reveals an astonishing **52%** were carried out using this method. This disparity clearly **demonstrates** that threat actors **attacking Airspace Users** employ **fraudulent websites** at a **rate nearly double** the overall industry **average**. You can find additional details about the strategy employed by the adversaries in chapter Unmasking the Fraudulent Websites.

Phishing schemes were **responsible** for **484** incidents, constituting **13%** of the **total**. **Malware** was the next most common method, with **442** incidents, while **DDoS** attacks accounted for **112** cases. Surprisingly this year we have noted an **increase** in hacking attempts **324 comparing to 2022** which was only **1**. **Ransomware**, though **less frequent**, was still identified in **23** incidents, contributing to **1%** of the cases. **Unknown vectors** were **associated** with **418** attacks, making up **11%** of the total. Additionally, **single incidents of Errors, Supply chain compromise and Business logic abuse** were recorded.

Continue your exploration on the effects of Airspace Users in Costly Clusters: Financial Loss and Data Theft in Airspace Users.

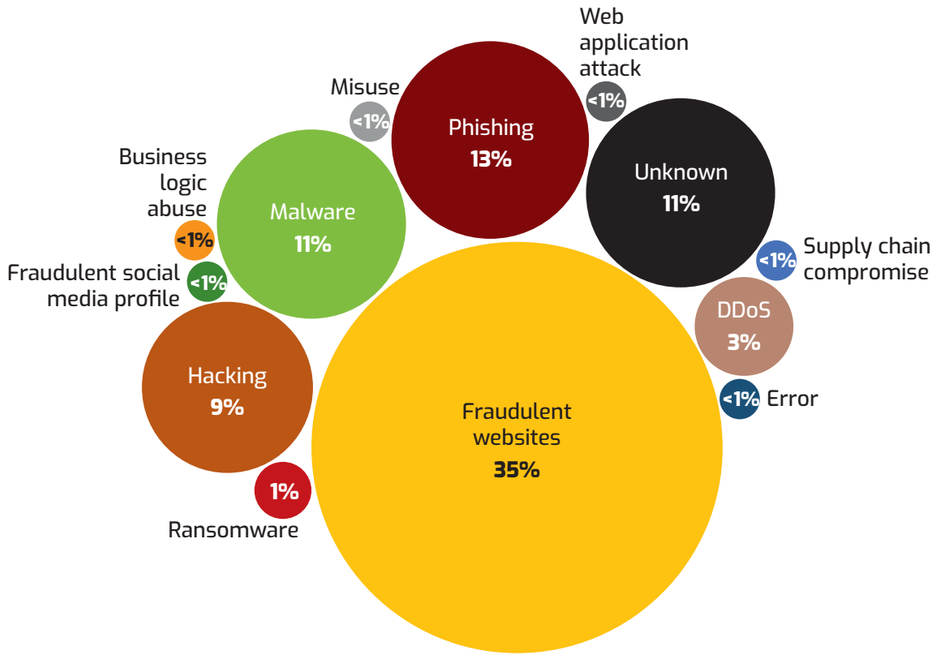


Figure 9: Airspace users attack vector

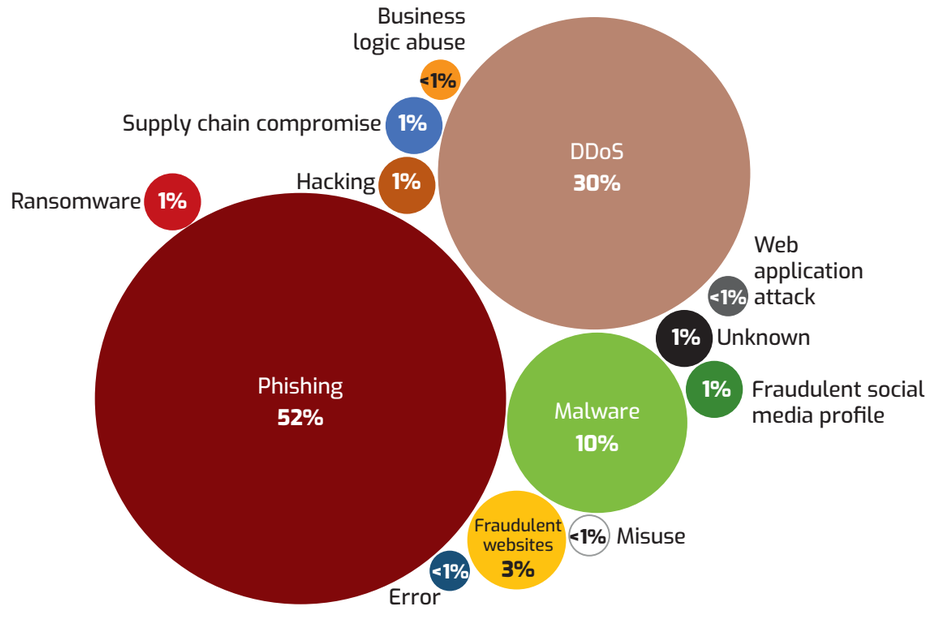


Figure 10: Airports attack vector

Airports at the Intersection of Ideologically Driven Cyber Attacks and Phishing

After examining the primary threat vectors targeting Airspace Users, it is equally important to delve into the specific attack patterns encountered by another key element of the aviation ecosystem: airports. As crucial nodes connecting different parts of the globe, airports have a unique threat profile that highlights their strategic significance. The complex nature of their operations and their pivotal role in the global transportation network make them appealing targets for various cyberattacks. The data indicates a particular emphasis on disruption-oriented attacks, with DDoS attacks at the forefront, reflecting a distinct threat profile for airports within the aviation industry.

In the context of **airports**, the analysis of **cyberattacks in 2023** uncovers a **unique pattern** in the threats they face. The **most prominent** attack vector was **Phishing**, accounting for **636** incidents which reflects **52%**. **Unlike** the **wider landscape of the aviation** industry, **airports** have been specifically **targeted** by **DDoS** attacks **(363)**, which make up an impressive **30%** of the total attacks against them.

Given the increasingly acknowledged but not yet fully established link between **DDoS** attacks and **hacktivist activities**, often **driven** by **ideological** or **political motives**, it is plausible to suggest that airports may be a significant target for such cyber attackers. The disproportionate **number** of **DDoS** attacks against **airports, suggests** a potentially **targeted strategy** that might align with the **hacktivist agenda. Airports**, as **critical infrastructure** and **symbols** of **global connectivity may** naturally **attract** these ideologically driven **attackers**. Their **targeting** of **airports** could serve **various purposes**, including causing highly visible **disruptions, spreading their messages, or protesting** specific policies or global events.

Malware is also present, with **124** incidents **(10%)**. Fraudulent websites and hacking were less common but still significant, with **39** cases **(3%)** and **9** cases **(1%)**. In **2023** we have also observed **12** incidents **(1%)** related to a **supply chain compromise**. The current **trends** in the cyber **threat landscape** are **suggesting** that the **growth** in this area is inevitable and more attacks of this type should be observed in the future.

Continue your exploration on the effects of Airports in A Reputation at Risk: Airports' Cyber Impact Analysis.

Navigating a Distinctive Landscape: Threats on Aviation Supply Chain providers

The examination of **cyberattacks** on **Aviation Supply Chain** providers unveils a **unique** assortment of attack vectors, reflecting the specific vulnerabilities and potential threats that this segment of the aviation industry faces. In **2023, Aviation Supply Chain providers** were subjected to a total of **225 cyberattacks** spread across various methods. **Ransomware** surfaced as the **primary** type of attack, accounting for **58** incidents or **26%** of the total.

Phishing attacks were the second most frequent type, with **28** instances, making up **12%** of the total. **DDoS** were the third most frequent type, leading to **27** attacks **(12%)**. **Hacking** attempts with **25** occurrences **(11%)** become fourth. **Malware** was associated with **16** incidents **(7%)**. **Errors** and **Misuse** seems to be subject of concern for the **Aviation Supply Chain** providers with 17 and **13** occurrences **(7%)**. **Errors** were documented in **4** instances, contributing to **2.4%** of the total cyber incidents faced by Aviation Supply Chain providers.

Unknown vectors were accountable for **47** attacks, constituting **28.7%** of the incidents.

The occurrence of business logic abuse, misuse, and error as attack vectors in the portfolio of incidents targeting Aviation Supply Chain providers underscores a unique facet of the cyber threat landscape in this sector. While these methods are seldom documented across other aviation stakeholders, their presence in attacks against Aviation Supply Chain providers may highlight specialized tactics or vulnerabilities unique to this part of the industry.

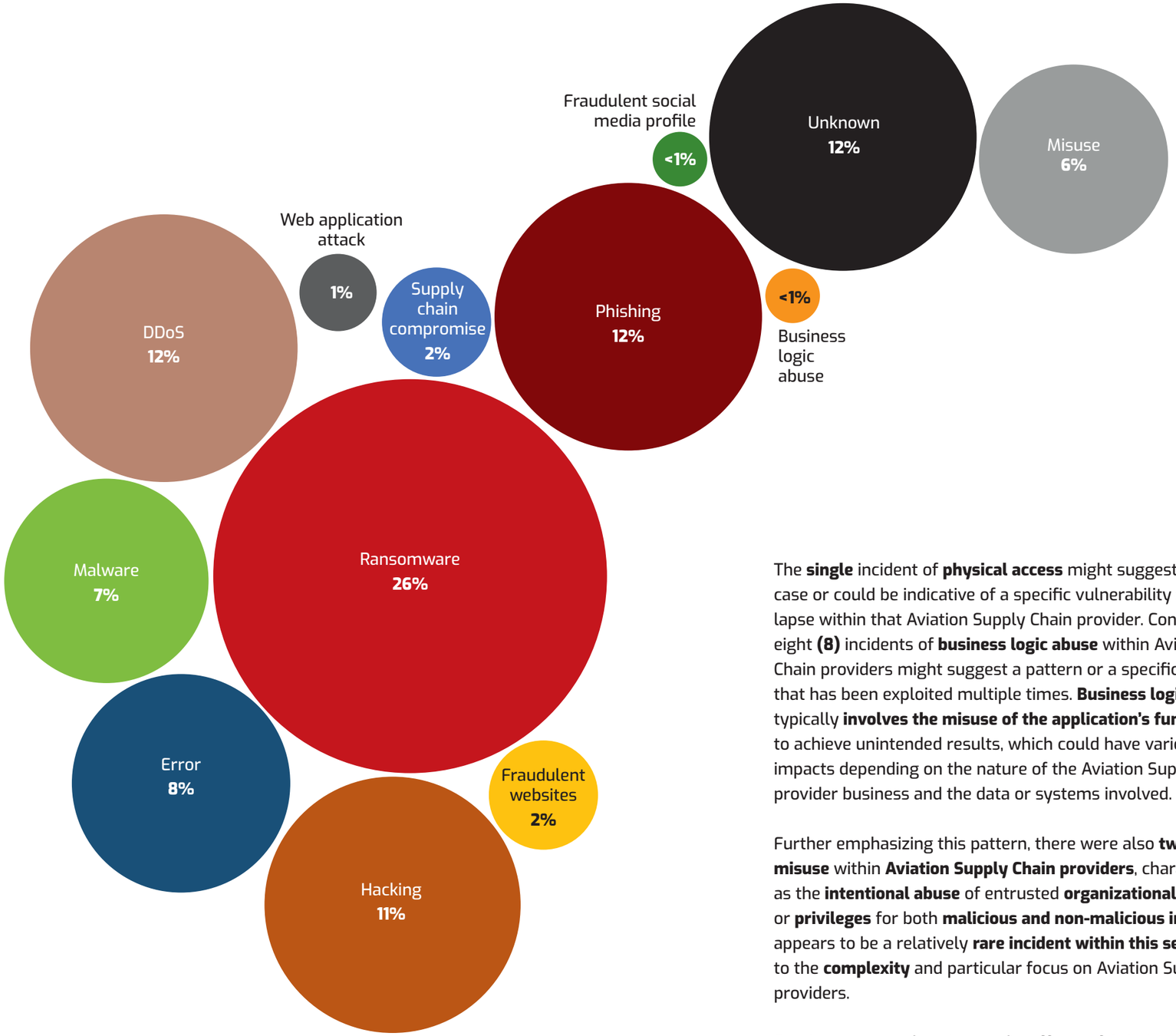


Figure 11: Aviation supply chain attack vector

The **single** incident of **physical access** might suggest an isolated case or could be indicative of a specific vulnerability or security lapse within that Aviation Supply Chain provider. Conversely, the eight **(8)** incidents of **business logic abuse** within Aviation Supply Chain providers might suggest a pattern or a specific vulnerability that has been exploited multiple times. **Business logic abuse** typically **involves the misuse of the application's functionality** to achieve unintended results, which could have various harmful impacts depending on the nature of the Aviation Supply Chain provider business and the data or systems involved.

Further emphasizing this pattern, there were also **two cases** of **misuse** within **Aviation Supply Chain providers**, characterized as the **intentional abuse** of entrusted **organizational resources** or **privileges** for both **malicious and non-malicious intent**. This appears to be a relatively **rare incident within this sector** but **adds** to the **complexity** and particular focus on Aviation Supply Chain providers.

Continue your exploration on the effects of Aviation Supply Chain in Stolen Bytes: Data Theft and Its Impact on Aviation Supply Chain providers

A Deep Dive into ANSP Threat Landscape: Anomalies and Trends

The landscape of threats and the strategies of attackers can significantly differ across various sectors of the industry. **Phishing** was observed in **302** instances, constituting **30%** of the total. **Malware** was associated with **134** incidents, accounting for **13%** of the cases. **DDoS** attacks, though less common, were reported in **40** instances, representing **4%** of the cases. **Hacking** was observed in **25** attempts while **Errors** and **Web Application** Attacks were reported in 9 and 4 instances. Worth mentioning are **supply chain compromise** attacks that for ANSP were highlighted **2** times.

Unidentified vectors were implicated in **506** incidents, making up **49%** of the total. Learn more about unknowns in chapter: The Enigma of Airspace: Deciphering the Unknowns in Aviation Cybersecurity

Interestingly, there were **only few** incidents of **fraudulent websites (4)**, which are **typically linked to financially motivated** threat **actors**. This, along with the notably low occurrence of ransomware (1) attacks on ANSPs (Air Navigation Service Providers), may suggest a trend. These **observations could indicate a reduced interest** from cybercriminal **groups** primarily **motivated** by illegal **financial gains**. A **possible explanation** for this lack of interest could be that **ANSPs do not provide commercial services**, making them less appealing targets for fraudulent activities from the viewpoint of cybercriminals.

The unique profile of this sector, marked by the absence of certain common attack vectors and the presence of specific threats, may reflect the unique value or risk associated with ANSP operations. It highlights a complex and multi-dimensional threat landscape, suggesting that financial incentives may not be the primary motivator for cyber attackers targeting ANSPs.

Continue your exploration on the effects of ANSP in Data Heists in the Sky: ANSPs' Cyber Struggle

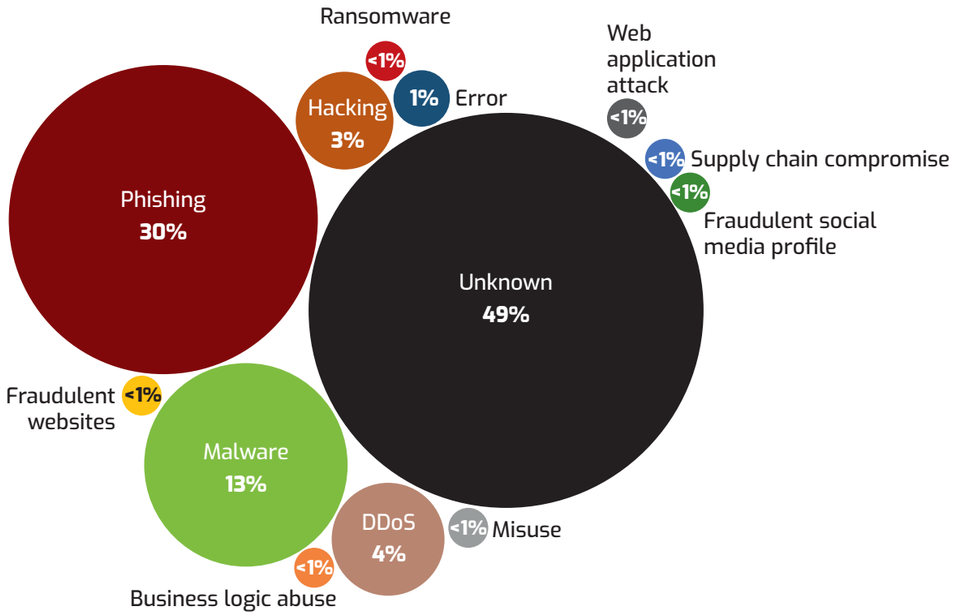


Figure 12: ANSP attack vector

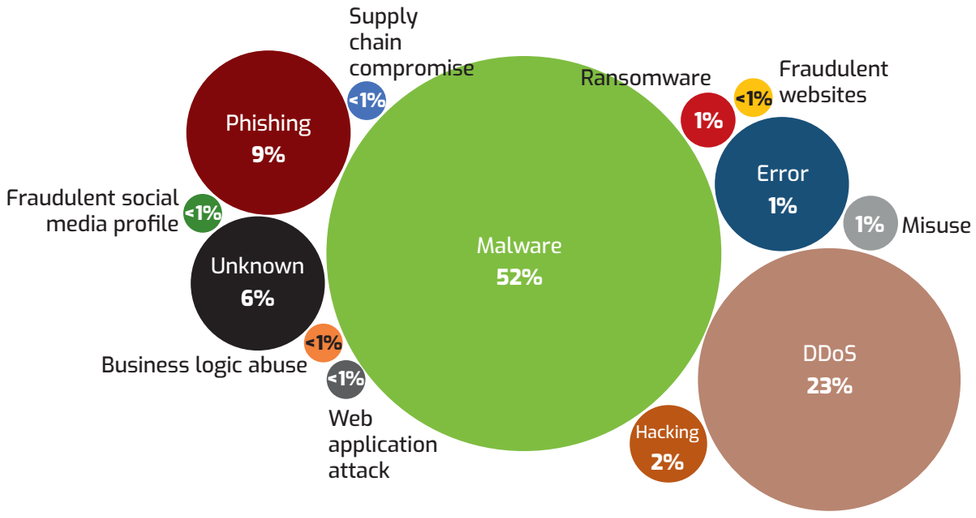


Figure 13: CAA attack vector

Facing the Unknown: CAAs and the Puzzle of Unidentified Threats

In the complex network of aviation security, the domain **of Civil Aviation Authorities experienced** a variety of **cyber threat vectors** over the year, albeit in lesser numbers. Out of a **total** of **88** recorded incidents, the **majority** were ascribed to **Malware** related attacks, making up **46** cases or **52%** of the total.

Subsequently, **DDoS** attacks were recorded in **20** instances, representing **23%** of the overall threat landscape. **Phishing** was less common – **8** occurrences **(9%)** while **Ransomware** was associated only with **1** incident or **1%** of the total.

Continue your exploration on the effects of ANSP in The Trust Equation: CAAs' Battle with data stealers.

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

Unlocked Secrets:
Understanding Password Leaks

EATM-CERT offers a service dedicated to detecting credential leaks associated with the domain names of aviation stakeholders. It is key to understand that those leaks are split into three distinct categories:

1. Corporate Records: 3rd party websites (like games forum, News websites, etc.) that got breached and aviation stakeholders used their professional email address (ex. account@eurocontrol.int on News Website).

2. Infected Employees Records: Malware-infected systems, using aviation professional accounts (ex. account@eurocontrol.int).

3. Infected Consumer Records: Malware-infected systems of consumers accessing corporate websites (ex. account@gmail.com accessing service@eurocontrol.int)

The first category, **Corporate Records**, poses a risk for the affected company due to the phenomenon of **password reuse**, where individuals often use the same or similar passwords across multiple services. The danger lies in an employee using identical or comparable passwords for both a breached third-party website and professional services.

The second category, **Infected Employee Records**, presents a greater risk because an **infected system with malware can capture professional credentials.** This can occur either on a corporate system or a personal computer used to log in to professional services, such as VPN.

The third category, **Infected Consumer Records**, is less critical since it involves **consumers accessing corporate services**. However, it should still be considered, depending on the sensitivity of the affected service.

This service has garnered increasing trust and subscription from various entities: Air Navigation Service Providers (ANSPs), Airport Operators (AOs), Airspace Users (AUs) and Civil Aviation Authorities (CAAs).

By the end of 2023, this service covered **179** domain names, serving **88** constituents.

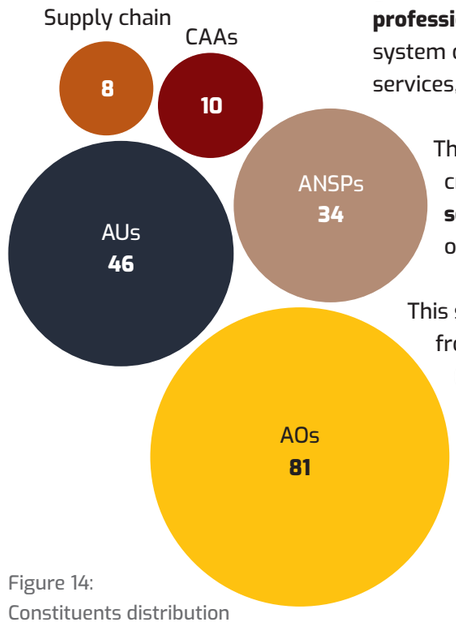


Figure 14:
Constituents distribution

The following figures provide an overview of the number of leaked credentials during 2023, pertaining to aviation stakeholders. These leaks are correlated against the number of affected domains, as it allows to draw certain observations.

In the figure 15, we can see that Airspace Users were more heavily affected by Corporate Leaks. Despite having a large number of domains impacted, the volume of leaked credentials is significantly higher compared to ANSPs and Airport Operators which have a similar or greater number of domains.

This result is expected when considering that Airspace Users typically have a larger workforce and therefore, a higher risk of credentials leaks from their users.

Another interesting observation is that CAAs also have a large amount of leaked credentials despite the very low number of affected domains and a generally smaller workforce compared to Airports and Airlines.

The Corporate Records Leaks highlight poor hygiene among Aviation stakeholders' employees that use their professional email address for non-professional services. This practice can be reduced by raising awareness about the proper and professional usage of corporate email addresses.

An important distinction in this category concerns **"Sightings"**. A sighting refers to the number of times the exact same credentials were observed across leaked records. This is crucial because hackers often combine and re-publish already leaked credentials, in new, so-called combo-lists.

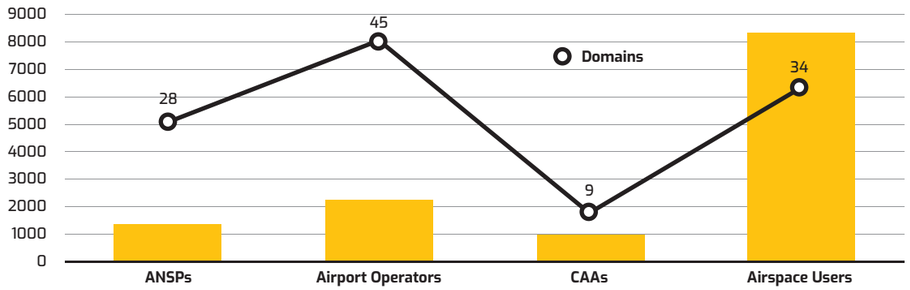


Figure 15: Corporate leaks per constituent type

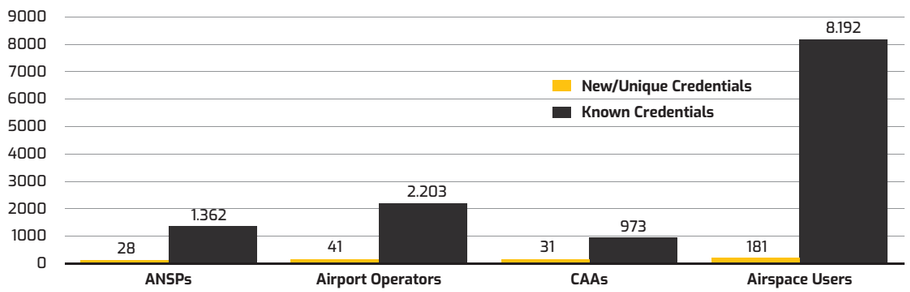


Figure 16: Corporate leaks per constituent type

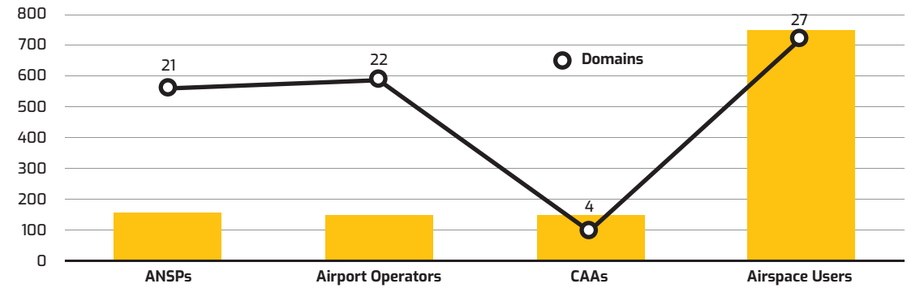


Figure 17: Infected Employee per constituent type

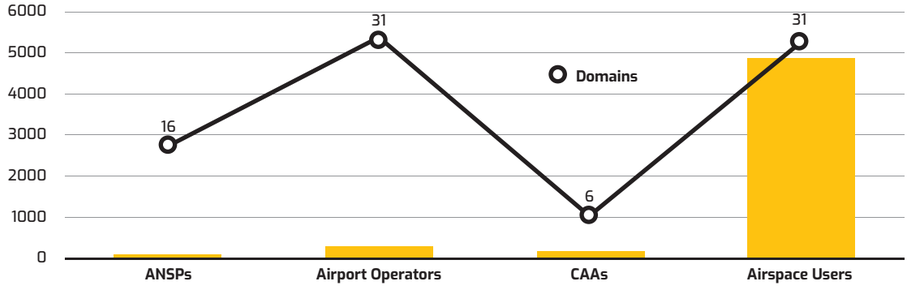


Figure 18: Infected Consumer per constituent type

The figure 16 shows the first-time-seen (Sighting equal to 1) leaks compared to already known credentials.

One can assume that most of the leaked credentials concern already known (potentially stale) credentials but the issue is that there is no way to distinguish between re-used credentials and stale/old ones.

For example, for ANSPs we see that in 2023, only 28 new credentials were identified while 1.362 were already known. However, it is impossible to know whether these 1.362 known credentials concern passwords re-used across distinct (breached) services.

The figure 17 provides the same overview for the second category of leaked credentials **(Infected Employee Records)** for 2023.

Here we see again that Airspace Users are more heavily affected than ANSPs and Airport Operators even though they have the same number of domains. Once more, this makes sense considering that Airspace Users typically have a larger workforce than the other categories.

More importantly, CAAs have a very large amount of leaked credentials from infected employees' systems, compared to the very low number of affected domains.

In the figure 18, the same overview is provided for the third category of leaked credentials (Infected Consumer Records) for 2023.

It is clear that Airspace Users are by far the most affected. This is expected, as Airlines have the most consumers compared to other Aviation stakeholders. Moreover, the consumers of Airspace Users also include Frequent Flyer accounts, which are considered prime targets for hackers due to their easy monetization.

Concerning the sources of all the leaks for 2023, the figure 19 depicts the percentage distribution.

Only newly seen, unique credentials for 2023 are taken into account for this figure. Otherwise, huge combo lists that include previously leaked credentials dominate the statistics and do not allow a good reading.

Regarding the 8% that concerns malware sources, the figure 20 depicts the distribution between the main malware families.

It should be noted that, these malware sources depend on the credential leaks service's capability to monitor and extract information from infected machines. Malware families that are not susceptible to such monitoring cannot be represented.

Further delving into the actual leaked passwords, it is noteworthy that while complexity requirements and awareness have increased, we still observe bad practices leading to weak passwords.

A very visual representation of a **password's complexity** is its length, and the figure 21 shows that most Aviation personnel employ 6 to 10 characters long passwords, based on 2023 data.

Of course, length is not the only requirement for a complex and hard to guess password.

Defining a complex password as one that is:

- Longer than 8 characters.
- Including alpha and numeric characters.
- Including capital and lower case.

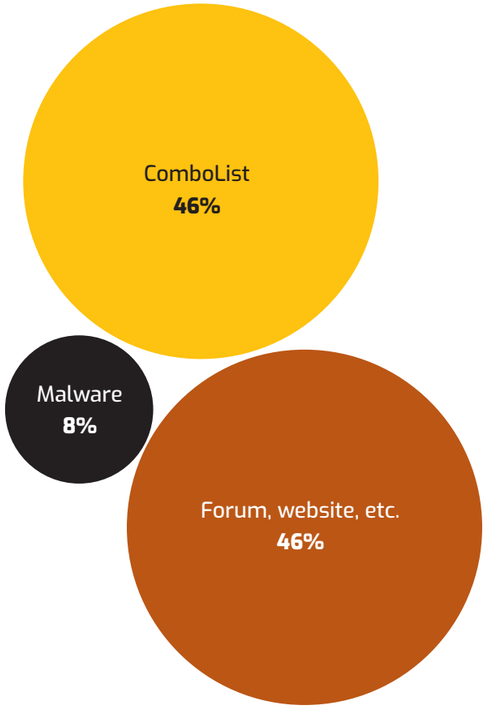


Figure 19: Unique Passwords sources

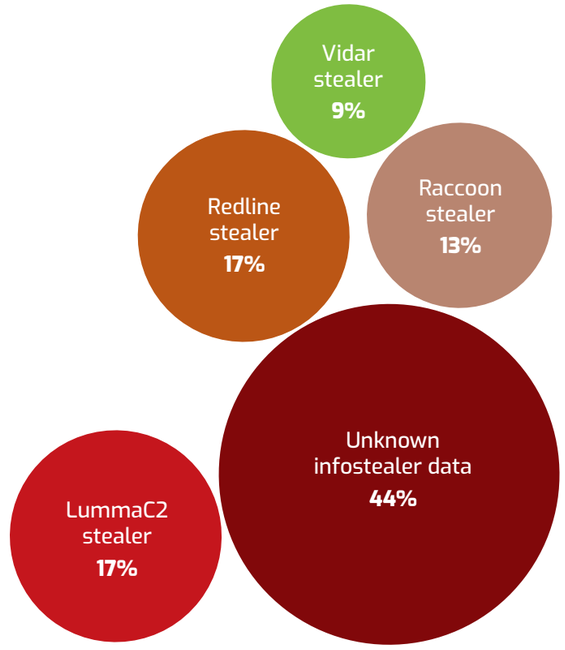


Figure 20: Main malware families stealing passwords

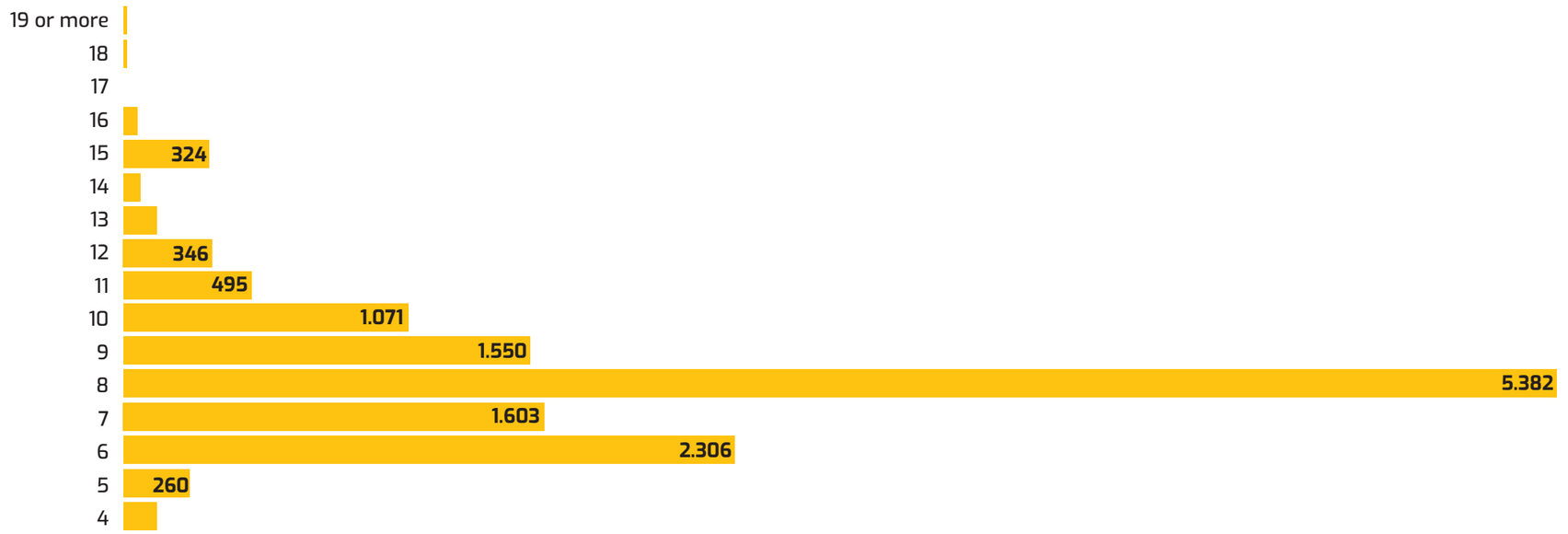


Figure 21: Password length distribution

It is then possible to visualize the percentage of complex and non-complex leaked passwords for 2023.

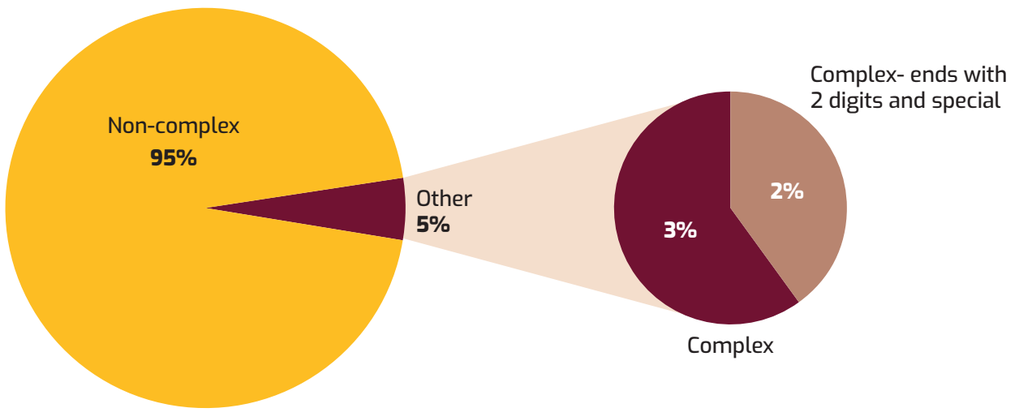


Figure 22: Password complexity

It clearly appears that **Aviation personnel do not follow best practices for password complexity when not required to**, and even the few (5%) that do, are using very common patterns among hackers. For example, as shown in the figure 22, a very common pattern is to use 2 digits and a special character at the end of the password. This is an easy way to make a password "complex", but hackers are aware of these patterns and can easily exploit them to guess even complex passwords.

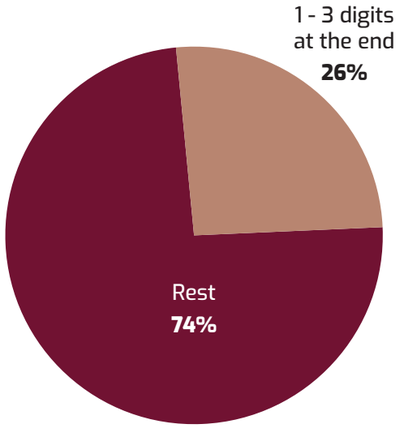


Figure 23: Passwords with digits at the end

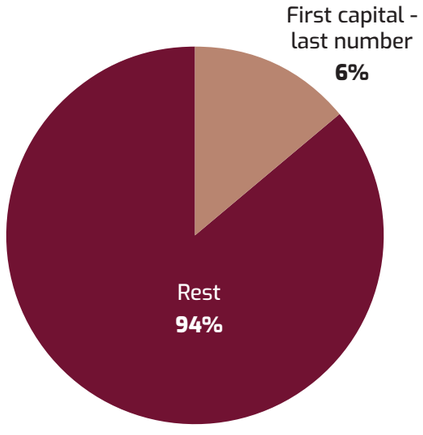


Figure 24: Password with capital letter and number

Likewise, using digits at the end of the password, is a very common pattern, as shown in the figure 23.

Or leaked passwords of Aviation stakeholders that start with a capital letter and end with a digit (Figure 24).

As another illustrating example (Figure 25), a common pattern is for people to use year of birth in their password. Checking Aviation stakeholders' leaked passwords that include a year, we can see a noteworthy 6% that includes dates from 1960 to 2023.

What is more interesting, is that checking the actual year employed in the leaked password, we see that almost the double amount of leaked passwords, includes a year between 1960-1979 than a year between 1980-1999 (Figure 26).

A potential indicator that older Aviation stakeholders employ more predictable patterns for their passwords.

Taking these weaknesses into account, the adoption of **multi-factor authentication** (MFA) – whether through SMS, one-time password apps, or device confirmations – emerges as a potent solution. It acts as a significant line of defence, even when password choices are less than optimal.

While technological solutions offer a safeguard, the cornerstone of cybersecurity remains the **awareness and education of users**. The recurrent oversight in password management underscores an enduring weakness in IT security.

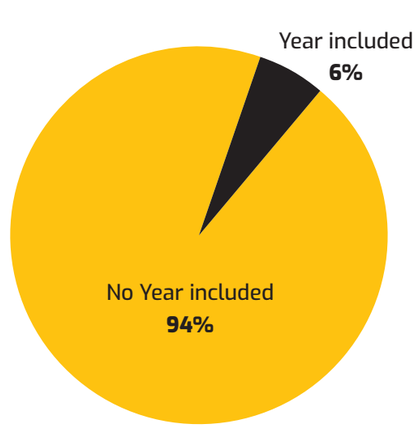


Figure 25: Passwords including year

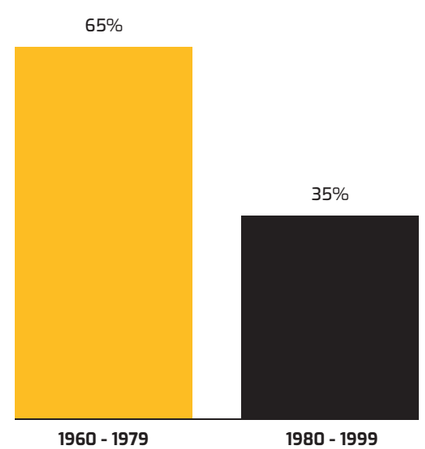


Figure 26: Passwords with birth year

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

Navigating the Dark Storm

The aviation industry continues to be a popular topic of discussion on underground forums, ransomware leak sites, and both private and public Telegram channels due to the sensitive nature of its data and the potential impact of disruptions.

EATM-CERT monitors the dark web to protect stakeholders from operational disruptions, financial loss, and reputational harm resulting from data theft. Stakeholders receive prompt alerts about mentions in hacking communities, along with imminent threats and covertly planned attacks on forums and other platforms frequented by threat actors.

The analysis below provides a comprehensive overview of various threats detected in the Dark Web over the 2023, including discussions on underground forums, Initial Access Broker (IAB) auctions, data leaks, ransomware leak sites, insider threats, supply chain attacks, and hacktivist activities.

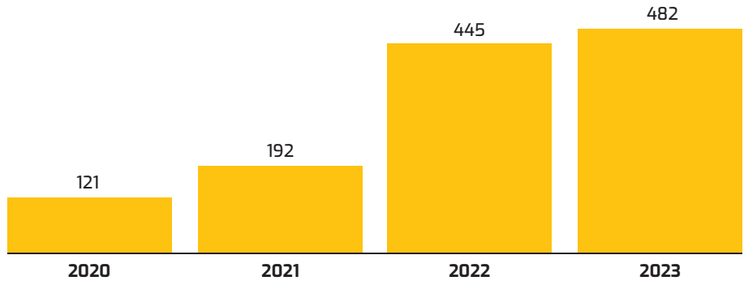


Figure 27: Number of detected dark web posts

Initial Access Brokers (IABs) in the Aviation Industry

The aviation industry is a high-value target for Initial Access Brokers (IABs) due to the critical nature of its data. The year 2023 saw 9 posts on underground forums offering initial access to the networks of aviation entities, encompassing airlines, airports, aerospace manufacturers, and associated service providers. These offers included various levels of access, such as network credentials, administrative privileges, email server access, **RDP access, VPN access,** and **direct server access.** Methods of acquisition often include phishing attacks, exploiting software vulnerabilities, insider threats, or using previously compromised credentials.

Data Leaks discussion on the underground

Personally identifiable information (PII) of customers and employees makes the airspace users a **prime target** for cybercriminals. **During 2023**, there were **35 instances** of posts on underground forums **discussing data breaches** in the aviation industry, encompassing airspace users, CAAs, airports, aerospace manufacturers, and related service providers.

Cybercriminals focus on airspace users due to the vast amounts of sensitive data they handle, including personal passenger information and financial details. Data leaks are advertised on dark web forums, where small samples are posted to entice buyers.

Insider

In **2023**, there was a **single post** on underground forums **indicating insiders** involved in **selling personally identifiable flight booking data.** Additionally, **another post** highlighted a **misconfiguration** by airspace users, which **exposed** environment files containing **database and email configuration details**. These databases were exposed to the underground, meaning anyone could potentially use these credentials to access sensitive information stored in the databases. This exposure implies that malicious actors could have accessed user information without the need to exploit any vulnerabilities. Attackers could log in, read, and copy the contents or, if user privileges allowed, modify, or delete the data.

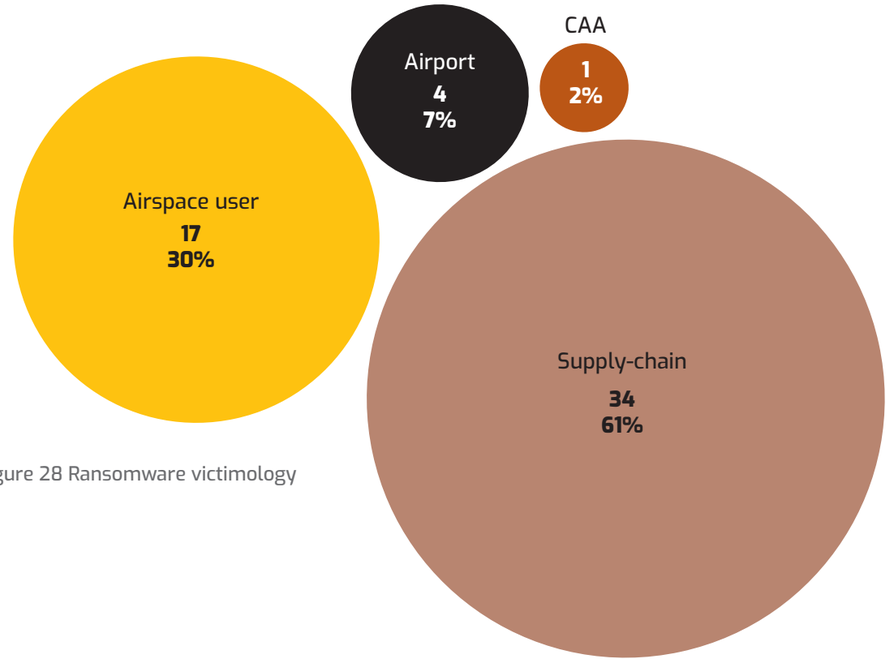


Figure 28 Ransomware victimology

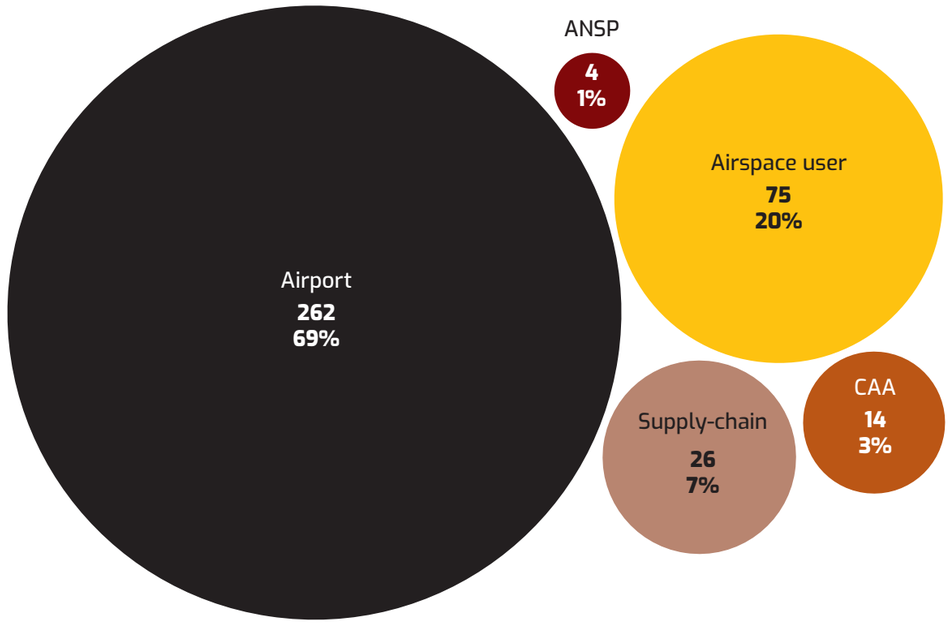


Figure 29 Hacktivist victimology

Supply Chain Attacks

Supply chain companies are frequent victims of ransomware operators who aim to infiltrate internal environments or gain access to customer information. Ransomware groups often use leak sites on the dark web to publicly shame compromised victims, displaying countdowns, data samples, and screenshots of compromised documents. In **2023, 61% of ransomware victims** were supply chain companies. Supply chains are attractive targets because infecting a single compromised supplier can impact multiple organizations, maximizing profits for the attackers.

No specific threat actor singularly focused on targeting the aviation sector was identified.

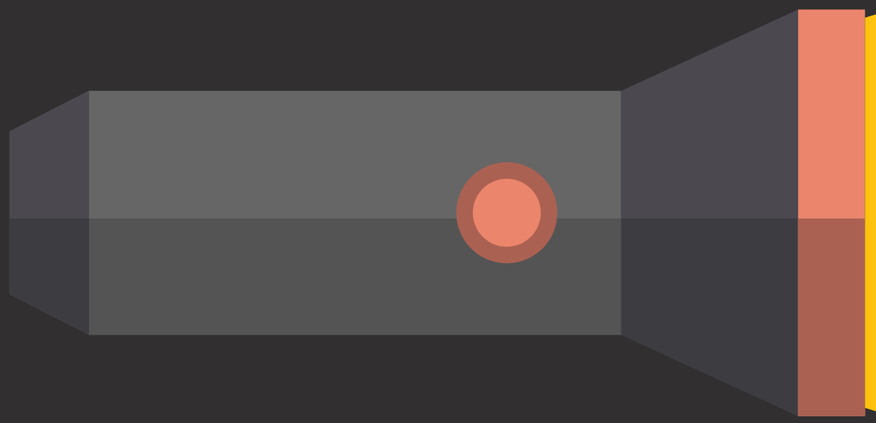
Hacktivist Activities

Hacktivists mainly target airports, aiming to cause disruption through DDoS attacks. The increasingly fragmented geopolitical landscape, reshaped by conflicts such as the war in Ukraine and hostilities in the Middle East, has fuelled more underground discussions about aviation as critical infrastructure. **In 2023, 69%** of the targets mentioned on Telegram channels regarding DDoS attacks were airports.

DDoS attacks remain relatively easy to execute. In many cases, adversaries do not need to own infrastructure as it can be purchased from various “service providers.” A DDoS attack is a highly efficient method to gain media attention. Often, adversaries use this opportunity to deliver different statements.

No specific threat actor singularly focused on targeting the aviation sector was identified.

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team



Points Lost in the Darkness

Loyalty programs are increasingly becoming targets for cybercriminals who compromise accounts. The detection stands out this year, with the number of compromised accounts rising from **5.348** (representing **4.303.498 miles**) in **2022**, where approximately **36%** of the compromised accounts did **not** contain **miles**, to **18.670** (representing **11.367.190 miles**) in **2023**, where **29%** of the compromised accounts did **not** contain **miles**.

It is estimated that the value of frequent flyer miles outstanding (i.e., miles that have been issued but not yet redeemed) could be worth around US$200 billion (all airlines, worldwide).

Frequent flyer programs represent substantial and attractive assets that can be monetized quickly and discreetly on dark markets, making them highly profitable targets.

In 2023, frequent flyer miles averaged **1.20 US cents per mile**, depending on the program and how they are redeemed. Based only the number of miles and points detected in 2023, the potential market value runs into **US$136,406.28.**

Frequent flyer miles hold significant monetary value in underground market where stolen frequent flyer miles are worth approximately **0.80 US cents per mile** on the dark markets according to our dataset.

In 2023, the average price of a compromised account dropped to **$11.78**, a significant decrease from **$15.19 in 2022**. This decline can be attributed to several factors.

As cybersecurity risks evolve, more accounts are being compromised, leading to a **higher supply on the black market**. The increased availability of compromised accounts drives down their price. The cybercrime market has become **saturated** with numerous sellers offering compromised accounts. This competition among sellers leads to l**ower prices as they strive to attract buyers.**

Some dark markets changed their policies regarding returns and refunds for compromised accounts. Stricter return policies or the elimination of refunds have made buyers more cautious, leading to decreased demand and lower prices.

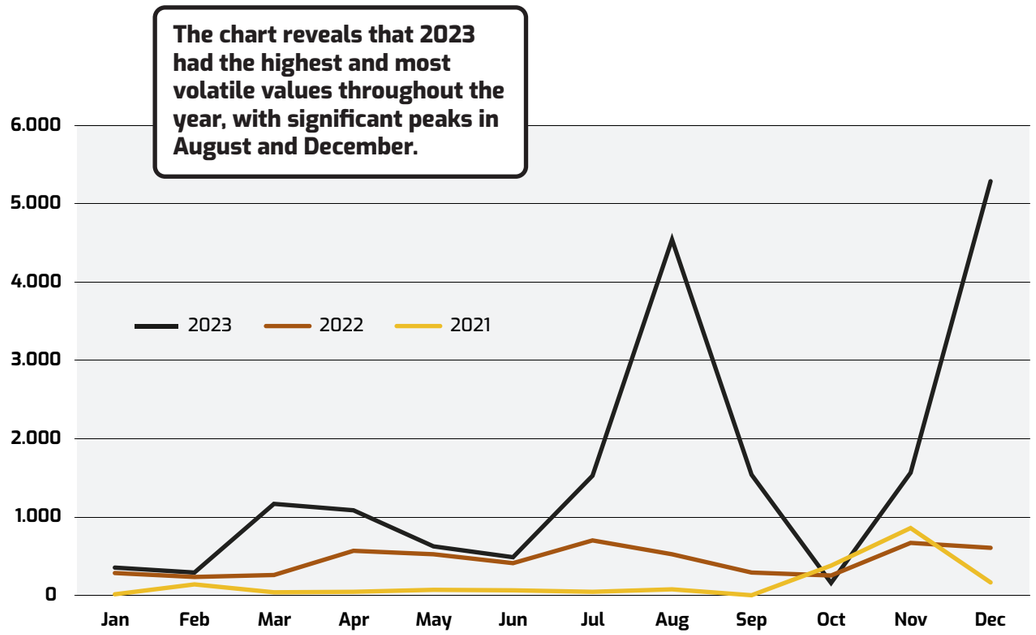


Figure 30 Highest and most volatile values throughout the year

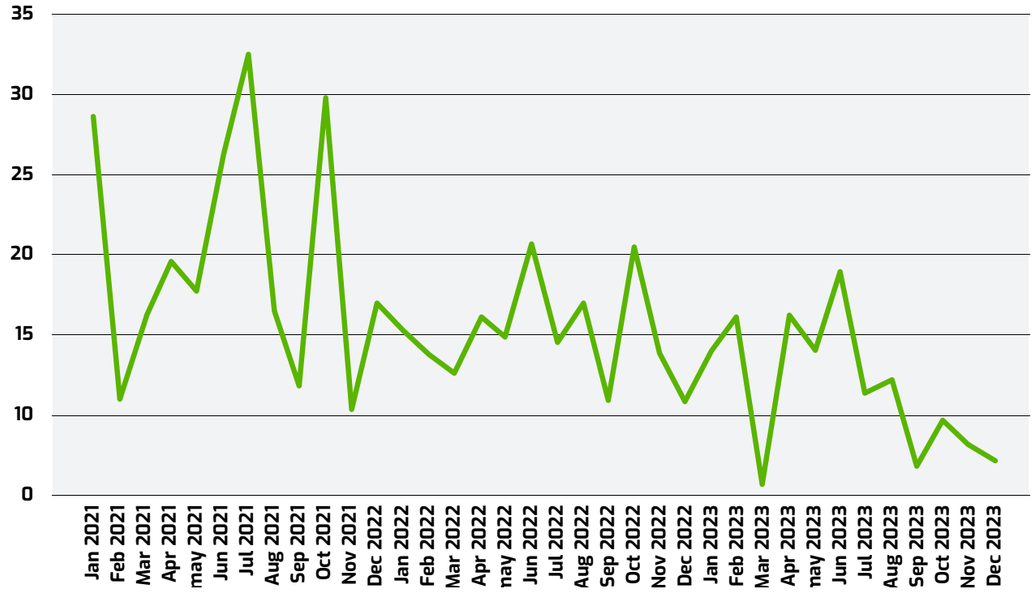


Figure 31 Stolen Frequent flyer program data price evolution.

Following the exploration of underground forums, another critical aspect is why the price of compromised accounts is decreasing while the price of miles remains stable. This is due to the sale of personally identifiable (PI) data. Notably, **29%** of the compromised accounts detected in 2023 do not contain miles, they are likely **solely selling PI data** from the accounts. These accounts are usually sold at a **lower price.**

The **price of session cookies** sold on the **dark market** can vary significantly based on several factors, such as the type of session cookies. The **cheapest session cookies**, which contain basic session data, **login credentials**, or minor personal information, are priced between **$1 to $5 each.**

Detection of fraudulent websites impersonating airlines has highlighted how cybercriminals often compromise frequent flyer programs, posing a significant threat to travellers. Cybercriminals use various methods to perform **account takeover** (ATO) attacks, often through phishing and spear phishing. They mimic websites to appear as if they are from legitimate airlines, **tricking users into revealing their login credentials.** Once inside an account, they can quickly use or sell the miles, often on the dark web.

Another method discovered on underground marketplaces involves the sale of "cookies" by cybercriminals that have infected victims' devices through malware or account takeover attacks. Cybercriminals on these dark markets s**ell access to all the data** harvested from the infected devices, such as saved logins from airline profiles and autofill form data.

The year 2023 marked the rise of Telegram as a fresh frontier in the dark market for selling access to loyalty programs. Cybercriminals have been flocking to Telegram channels and groups, hoping to benefit from **better visibility to buyers and enhanced anonymity.** This approach grants them **continuity** because dark web sites are sometimes suspended and require time to be promoted again with a new source.

Unmasking the Fraudulent Websites

In **2023**, EATM-CERT observed a significant surge in the detection of fraudulent websites impersonating **aviation stakeholders.** This alarming trend highlights the efforts of cybercriminals targeting the aviation sector. The number of these fraudulent sites grows each year, underscoring the need for continuous advancements in detection technologies and methodologies.

EATM-CERT analyses fraudulent web sites schemes and outlines techniques used by fraudsters at each stage outlined in Figure 32.

Reconnaissance	Domain Registration	Resource development	Campaign	Monetization
Collect data about the impersonation victim Copy the content (including images), structure, and design elements from the legitimate website	Typosquatting: Register a domain name that closely resembles the legitimate one (e.g., using similar characters or slight misspellings) Free Subdomain: Scammers use services like Weebly, Wix, WordPress, or other platforms that offer free subdomains to create a website.	Use the gathered website content, images, and design elements to create a clone of the legitimate site. Use website builders like Wix, WordPress, or Weebly to quickly create a professional-looking clone of the legitimate site, leveraging templates and drag-and-drop functionality. Use services like Cloudflare to protect obscure the hosting provider's IP address, making it harder for the site to be taken down. Using SEO techniques to make fraudulent websites rank highly in search results.	Refund Cancellation Scams (Scammers pretend to be from an airline offering refunds for cancelled flights.) Fake Customer Service Numbers (Scammers set up fake customer service numbers that mimic those of legitimate airlines.) Fraudulent Book Flight Forms (Scammers create fake flight booking forms to steal personal and financial information) Prize Flight Tickets Scams (Scammers notify victims that they've won free flight tickets in a contest or lottery they never entered.) Fake Anniversary Tickets Offers (Scammers offer discounted or free tickets to celebrate an airline's anniversary.)	Credential Capture (Scammers capture login credentials for airline accounts, email, or other services.) Theft of Personal Identifiable Information (PII) (Scammers steal personal information that can uniquely identify an individual.) Theft of finacial data (Scammers target financial information, especially credit card details.) Sell accounts to third-party scammers on specialized darkmarket shops

Figure 32 The Fraudulent Websites attack anatomy

In 2023, a total of 2,024 fraudulent websites were identified as targeting IATA members, and 37 were found to be targeting ACI Europe members. **Fraudulent websites** aimed at IATA members are **primarily used for selling scam tickets,** making victims complete payments through fraudulent websites, or stealing credentials, which are then used to steal frequent flyer miles. However, our detailed analysis of **fraudulent websites** impersonating ACI Europe members **revealed** that they are often used for the same goal, impersonating airspace users, but for this activity they use **watering hole attacks**. Specifically, **attackers create** a single **website impersonating** an ACI Europe member with several subdomains to impersonate various IATA members, redirecting victims to these fraudulent airline sites.

Only **fraudulent websites** that **contain clear fraudulent content** and **explicitly impersonate** IATA members or ACI Europe members a**re detected and reported,** excluding domains without active websites.

Figure 34 visualizes the distribution of fraudulent website detections across different continents for the year 2023. North America has the highest percentage of detections, accounting for more than half of the total detections at 57.6%, followed by Europe with 20.9%. Asia also has a significant share at 12.5%. Other regions such as the Middle East, Africa, South America, and Oceania have smaller shares.

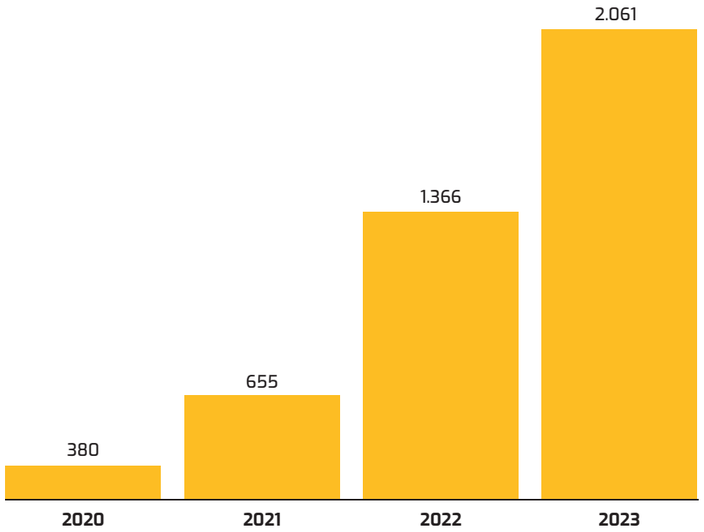


Figure 33: Number of detected websites impersonating aviation stakeholders

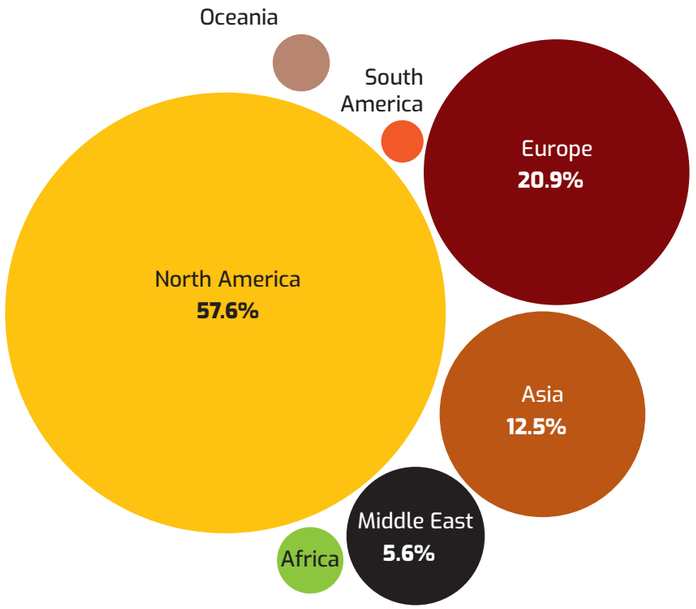


Figure 34: Victim distribution

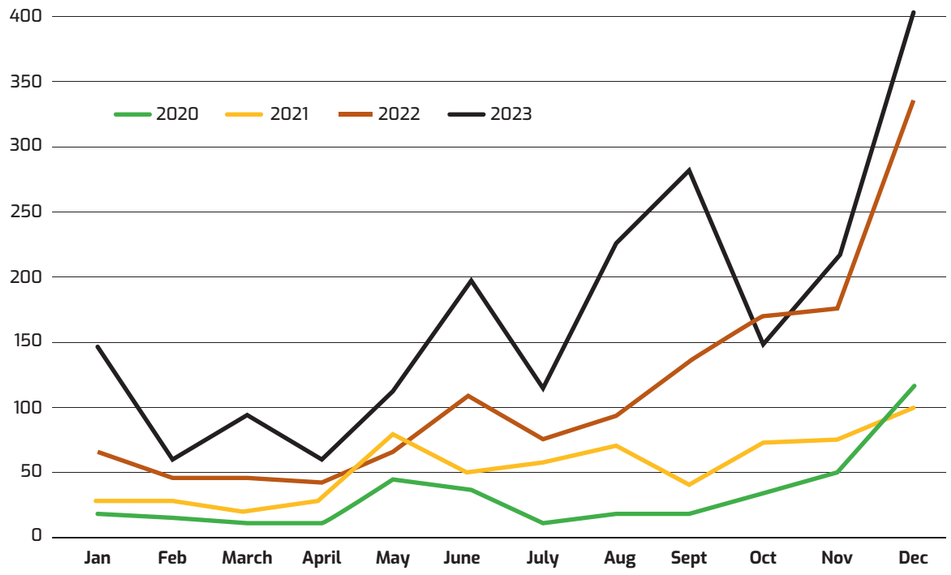


Figure 35 Fraudulent activities detections over the year

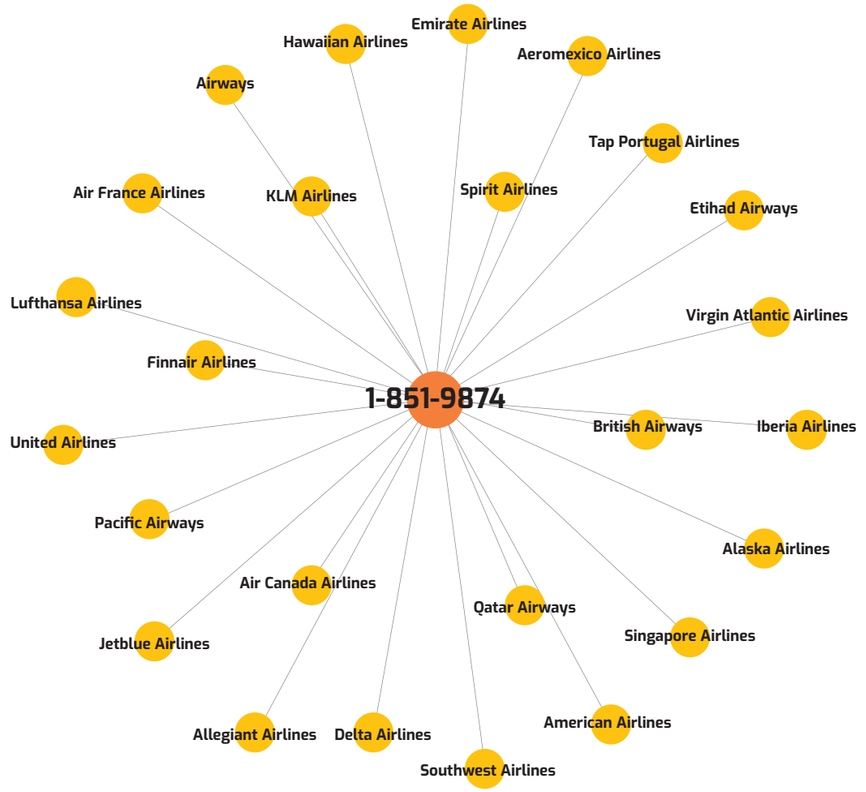


Figure 36 Single point for contact

The analysis, consistent with previous years, reveals a distinct seasonal pattern in fraudulent website activity, with **significant surges occurring during peak travel seasons.** Cybercriminals intensify their efforts, creating deceptive fraudulent websites particularly during **summer vacations** and the **Christmas holidays**. This aligns with times when flight ticket purchases are at their highest, demonstrating the opportunistic nature of these actors.

Data reveals a **51%** increase in detected fraudulent websites **from 2022 to 2023,** showcasing both the evolving tactics employed by cybercriminals and improvement in our detection capabilities.

The previous approach involved the use of approximately 300 typo keywords for each constituent. Now, the keyword database was enhanced to **include phone numbers** frequently **used by cybercriminals**. This enhancement significantly improved ability to identify fraudulent activities.

Figure 36 serves as a visual representation of how a **single phone number** can be central **to multiple fraudulent websites** across various airlines.

Cybercriminals Changing their TTPs with a Focus on Masking Activities

The rise in detected fraudulent websites impersonating IATA members and ACI Europe members is a growing. The increasing sophistication of these sites and their evolving techniques, tactics, and procedures (TTPs) focused on masking activities make them harder to detect and combat. Cybercriminals are using various methods, such as website builders, to create professional-looking fraudulent sites, leveraging services like Cloudflare to protect these sites from detection, and automated scraping. Additionally, Non-Lookalike Domain phishing tactics, which direct victims to fraudulent websites, are becoming more prevalent.

Typo squatting

Typo squatting in **2023 continues** to be a highly utilized technique for fraudulent websites, with **1,060 detections reported**. This technique involves registering domains that are slight variations of legitimate websites.

Figure 37 illustrates that typosquatting is still the most used technique, similar to the previous year, but with a slight decrease from 61.6% in 2022 to 51.4% in 2023.

This is followed by Website Builders, which show a slight increase, from 38.3% in 2022 to 47.1% in 2023.

Additionally, Non-Lookalike Domain Websites emerged as a new technique in 2023, accounting for 1.4% of the total.

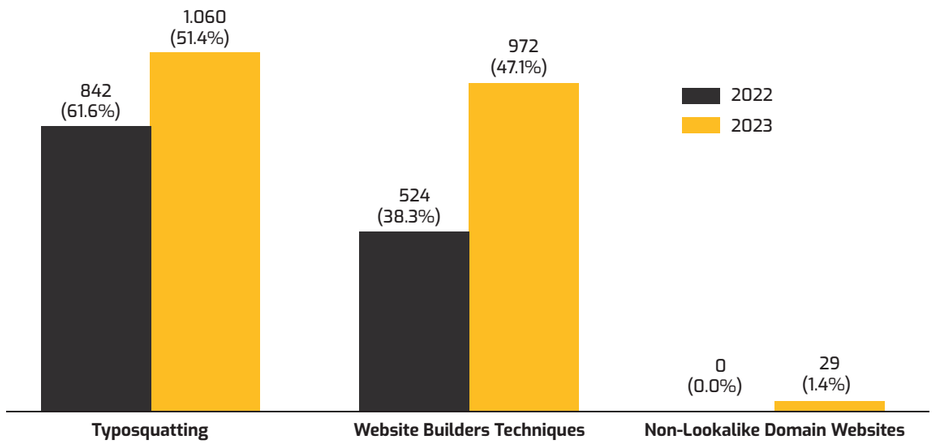


Figure 37 Fraudulent websites adversaries techniques in 2022 and 2023

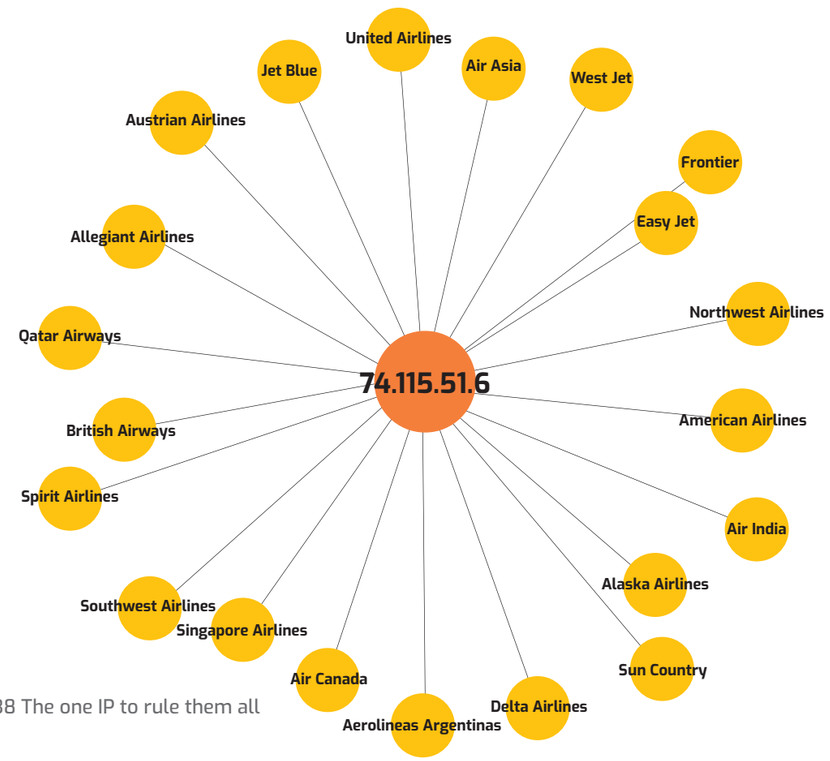


Figure 38 The one IP to rule them all

Website Builders option for Masking Cyber Criminal Activities

The rise in fraudulent websites created using Website Builders is growing. The increasing usage of these sites makes it easy to produce and develop fraudulent websites by the cyber criminals.

The year 2023 saw the detection of 972 fraudulent websites that leveraged Website Builders such as weebly.com, yola.com, wordpress.com, wix.com, and site123.com. This represents an increase from 524 in 2022 to 972 in 2023.

The growing detection capability highlights the ongoing battle against these threats and the need for persistent and evolving detection measures.

Cybercriminals **using Black Hat Search Engine Optimization (SEO) techniques** are employed to manipulate search engine rankings and increase the visibility of malicious sites. By optimizing these sites to rank higher in search results, attackers can lure more victims into visiting their fraudulent pages. This tactic enhances the credibility of phishing and other types of attacks by making malicious sites appear as legitimate top search results.

Cybercriminals often use legitimate website builders to create convincing, professional-looking websites that host malicious content. This can help them bypass security filters that might block suspicious or lesser-known domains. Using reputable domains also adds a layer of legitimacy to their sites, increasing the likelihood that users will trust and interact with them.

Cybercriminals Leveraging Cloudflare to protect Automated Scraping and Data Harvesting

The use of Cloudflare by cybercriminals to protect automated data scraping and screenshot activities presents a significant challenge. Continuous advancements in detection technologies, proactive security measures, and close collaboration with service providers such as Cloudflare are essential to effectively combat this evolving threat. This strategy highlights the ongoing battle against threats and the need for persistent and evolving detection measures. **The 2023, saw a detection of 241 fraudulent websites behind Cloudflare.**

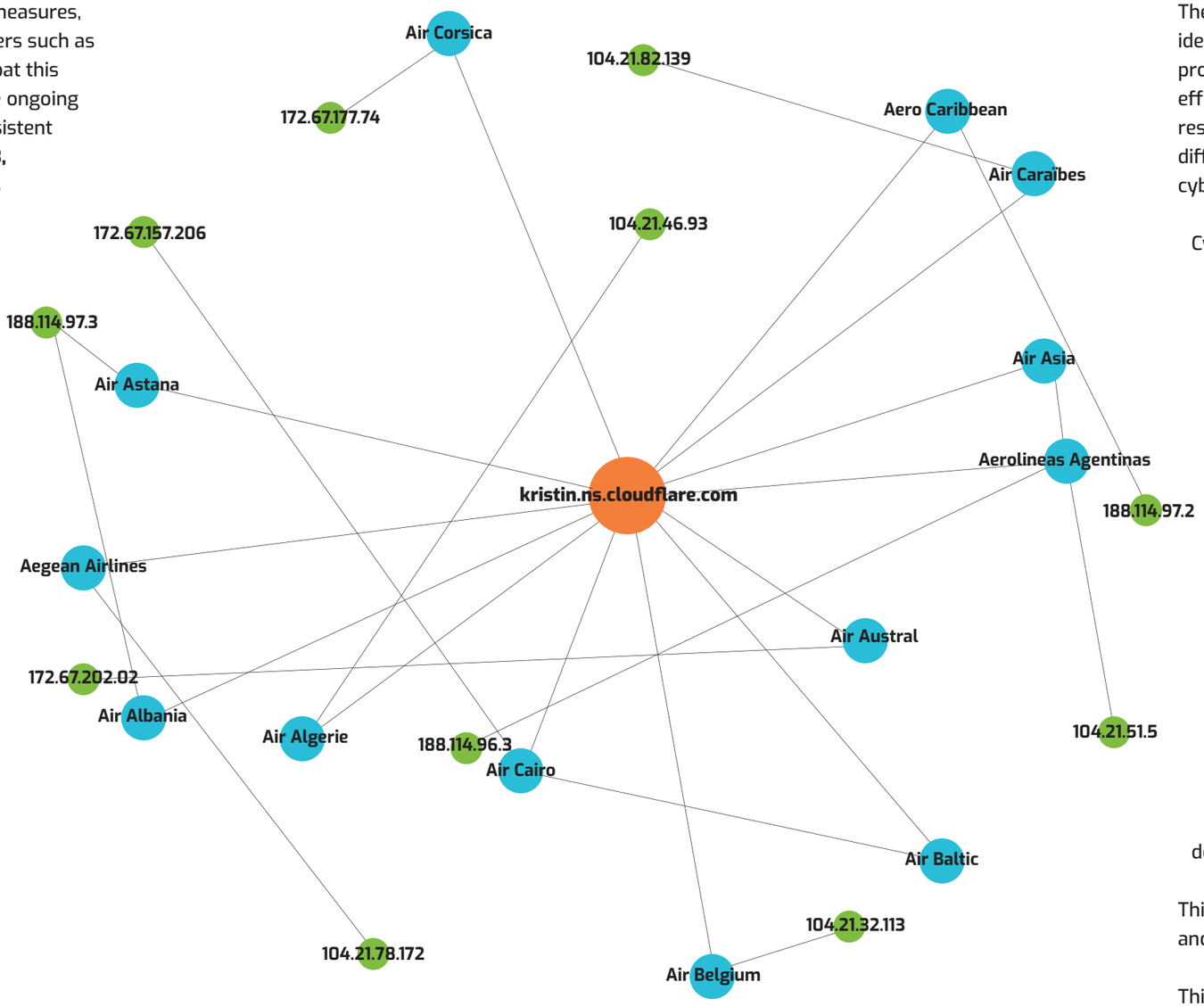


Figure 39: Different websites hidden behind Cloudflare

Non-Lookalike Domain Websites

The ongoing enhancement of detection capabilities has led to the identification of a critical challenge in fraudulent website detection processes. Current tools and keyword detection strategies effectively pinpoint fraudulent websites involving domains resembling those of airspace or airport users. However, significant difficulties arise when dealing with non-lookalike domains used by cybercriminals.

Cybercriminals are employing domains that bear no resemblance to the legitimate airspace or airport domains, such as **random strings of letters and numbers** (e.g., cgtaopsjdn.net). These domains do not trigger our existing keyword detection algorithms, making it challenging to identify and report such fraudulent websites.

By using **Non-Lookalike Domain Websites** to frequently update or change content, which helps them avoid detection. These dynamic changes can include altering page elements or rotating airline logos.

Only a small percentage of this activity is currently detected, with a concerning trend identified This necessitates rapid detection of these fraudulent websites because cybercriminals frequently change their tactics. Specifically, they keep the fraudulent domains active for a limited time. For example, a domain might be used to impersonate **Airline X for 2-3 days** and then, **after 3-5 days, the same domain might be repurposed to impersonate Airline Y.** This constant change in content further complicates detection and mitigation efforts.

This tactic allows cybercriminals to bypass detection mechanisms and thereby prevent for taking takedown action.

This increases the risk of monetizing their efforts by having victims complete payments through fake websites or by using stolen credentials, which are then used to steal frequent flyer miles.

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

Traps in the Route Charges, Impersonating EUROCONTROL

This year continues to show a steady presence of deceptive tactics used by entities masquerading as EUROCONTROL representatives. This year, we continue to observe a persistent occurrence of deceptive tactics employed by individuals posing as EUROCONTROL representatives. These cunning fraudsters have refined their methods, utilizing their skills of reconnaissance to uncover leaked invoices published by airspace users on social media platforms. Subsequently, they weaponize these invoices to craft communications that closely mimic authentic ones, making them increasingly difficult to discern. Upon receiving reports of fraudulent attempt, EATM-CERT promptly engages affected parties, urging them to provide original fraudulent email directly from the attacker they've received. This evidence serves as a crucial step in initiating the necessary measures for takedown and taking proactive steps by creating a MISP event.

Throughout 2023, EUROCONTROL received **198 notifications** regarding attempted scams, with **160** instances backed by tangible evidence. 2023 marked a significant milestone in our monitoring efforts, as stakeholders, for the **first time, provided** a remarkably **high percentage of original emails**, reaching up to **81%** reports with an email comparing to reports without. This uptick underscores an enhanced level of awareness and exemplary cooperation in combating these attacks.

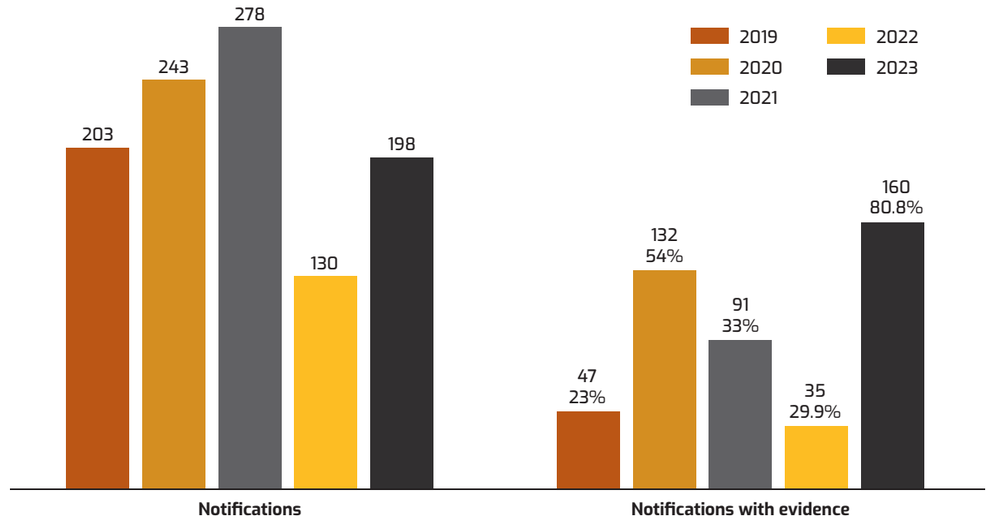


Figure 40: Reported fraudulent email distribution

TLP:GREEN

90 events, led to the discovery of **94 fraudulent domain** names or email addresses. Among these findings, **34 were email addresses** from various providers, while **60 were domain names**. It is worth noting that a single event might involve the utilization of multiple email addresses.

Out of the **total 94 deceptive domains and email addresses** identified, each one was **successfully suspended,** marking the first time achieving such a high rate of suspending fraudulent emails, thus demonstrating an outstanding success rate.

In addition to the year-on-year trend, our analysis of Scams Impersonating EUROCONTROL activity reveals specific peaks or attractive months for this type of cybercriminal activity. For example, in June, 75 notifications for scams impersonating EUROCONTROL, and in December, 36. It tends to surge during specific summer and winter periods. This pattern underscores the specific nature of these actors, who strategically amplify their fraudulent activities during vacation periods when targets stakeholders are with staffing reduced and awareness of this type of activity may be lower.

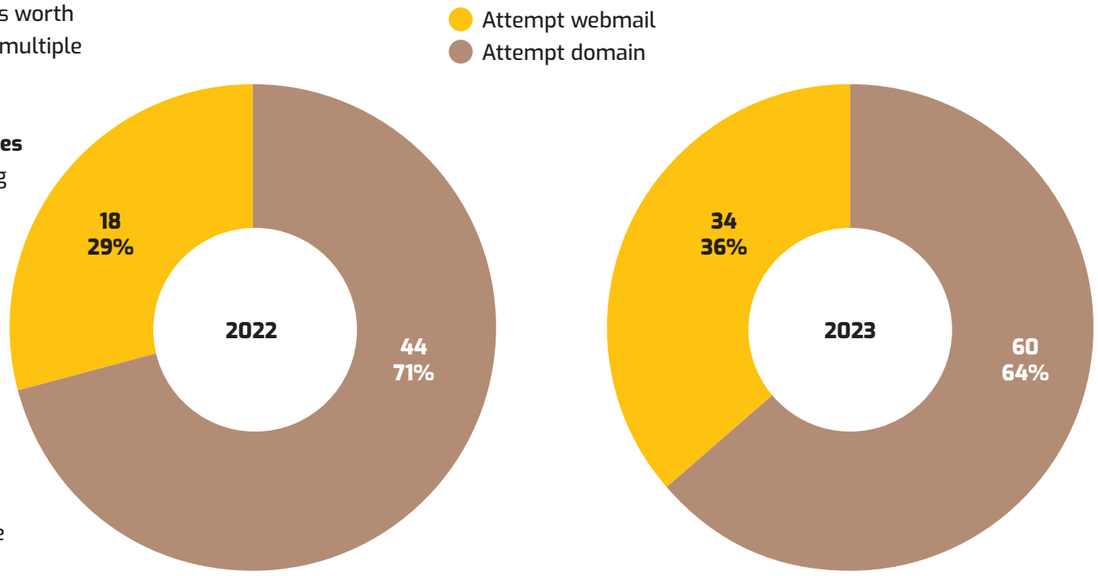


Figure 41: Attack type distribution in 2022 and 2023

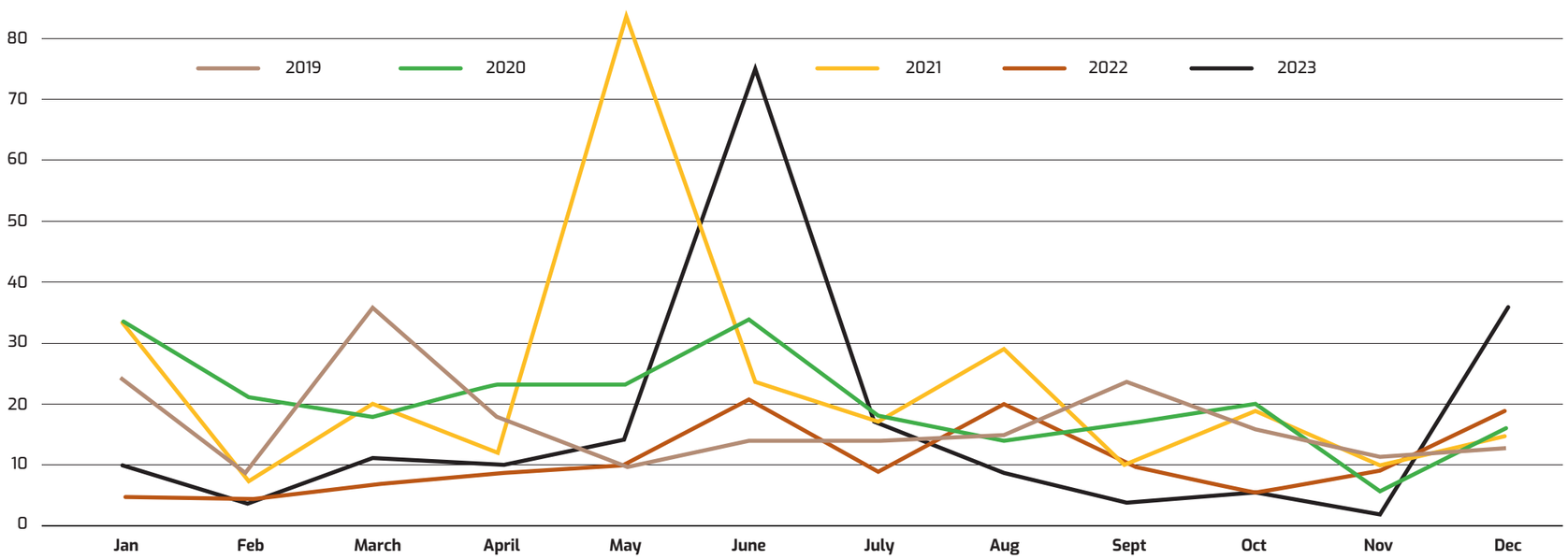
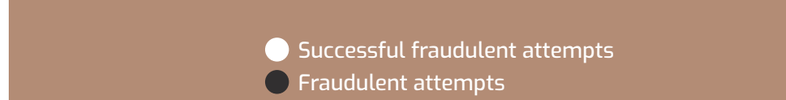


Figure 42: Scams Impersonating EUROCONTROL

Unfortunately, this year cybercriminals have successfully executed two fraudulent attempts. One resulting in a loss of 49,175 euros and another one with a loss of unknown amount.



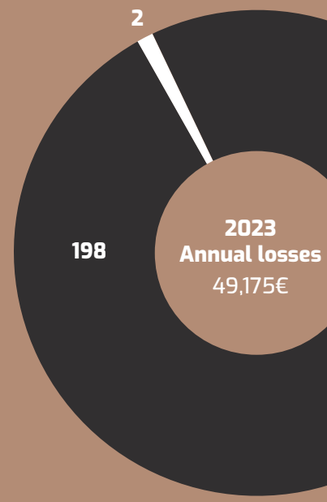


Figure 43: Payments to fraudsters

TLP:GREEN

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

Navigating Uncharted Threats:

MITRE ATT&CK Framework Findings

The MITRE ATT&CK framework is a globally recognized knowledge base of adversary tactics and techniques based on real-world observations. It provides a comprehensive matrix that maps out the various stages of an attack lifecycle, detailing specific methods and tools used by attackers. Organizations can use the MITRE ATT&CK framework to enhance their cybersecurity strategies by understanding and anticipating potential threats. It serves as a valuable resource for threat modelling, assessment, and mitigation, allowing security teams to identify vulnerabilities, improve detection capabilities, and develop robust defences tailored to the techniques most likely to be used against them. By leveraging the insights provided by the MITRE ATT&CK framework, organizations can stay one step ahead of adversaries and strengthen their overall security posture.

Actors Attacking Aviation

Our analysis focused on specific Advanced Persistent Threats (APTs) and cyber threat groups that attacked the aviation, aerospace, and transportation sectors in 2023.

The updated list of the most active cyber threat groups attacking aviation is presented in the following table:

APT10	APT39	HEXANE	UNC2420
APT15	APT41	Ke3chang	UNC2565
APT18	Axiom	LazyScripter	UNC2589
APT2	Chimera	Leafminer	UNC3318
APT27	Cleaver	Leviathan	UNC3810
APT28	Conference Crew	Molerats	UNC4214
APT29	Dragonfly	MuddyWater	UNC4697
APT3	Equation	Roaming Tiger	UNC4705
APT33	FIN6	TA2541	UNC4713
APT35	FIN7	Tropic Trooper	UNC4841
APT37	FIN11	UNC1543	UNC5111

Table 1: APT groups attacking aviation

Through the analysis of threat actors and the modeling of their behaviors using the MITRE ATT&CK matrix, we can derive the most common attack patterns and Tactics, Techniques, and Procedures (TTPs) employed by these actors.

2023 Aviation Heatmap

Based on an analysis of the tactics, techniques, and procedures (TTPs) employed by these cyber threat groups using the MITRE ATT&CK framework and on the 2023 dataset, the 2023 MITRE ATT&CK® **aviation heatmap** has been generated.

We utilized the latest version of the MITRE ATT&CK Enterprise matrix (v15.1), which includes sub-techniques and an expanded set of techniques for analyzing TTPs. Notably, this version incorporates tactics that model attackers' behavior before an actual attack occurs (formerly known as PRE-ATT&CK). Specifically, tactics such as **Reconnaissance** and **Resource Development** are included in the framework to capture this pre-attack behavior. Understanding these early-stage activities is crucial because it allows us to gather sufficient data about potential attackers, potentially preventing their actions before they execute an actual attack.

By using the 2023 dataset, we ensure that the analysis is relevant and reflects the most up-to-date threat landscape.

The colour schema used is based on a temperature chart:

- **red** is the most common techniques used by adversaries.
- **orange** is the second most common.
- **yellow** is rarely used by adversaries.
- **green** represents the least used techniques.

Additionally, the darker the colour in its group, the more often the technique is used. For instance, the "T1078: Valid Account" tactic is more widely used than the "T1070.001: Clear Windows Event Logs" one.

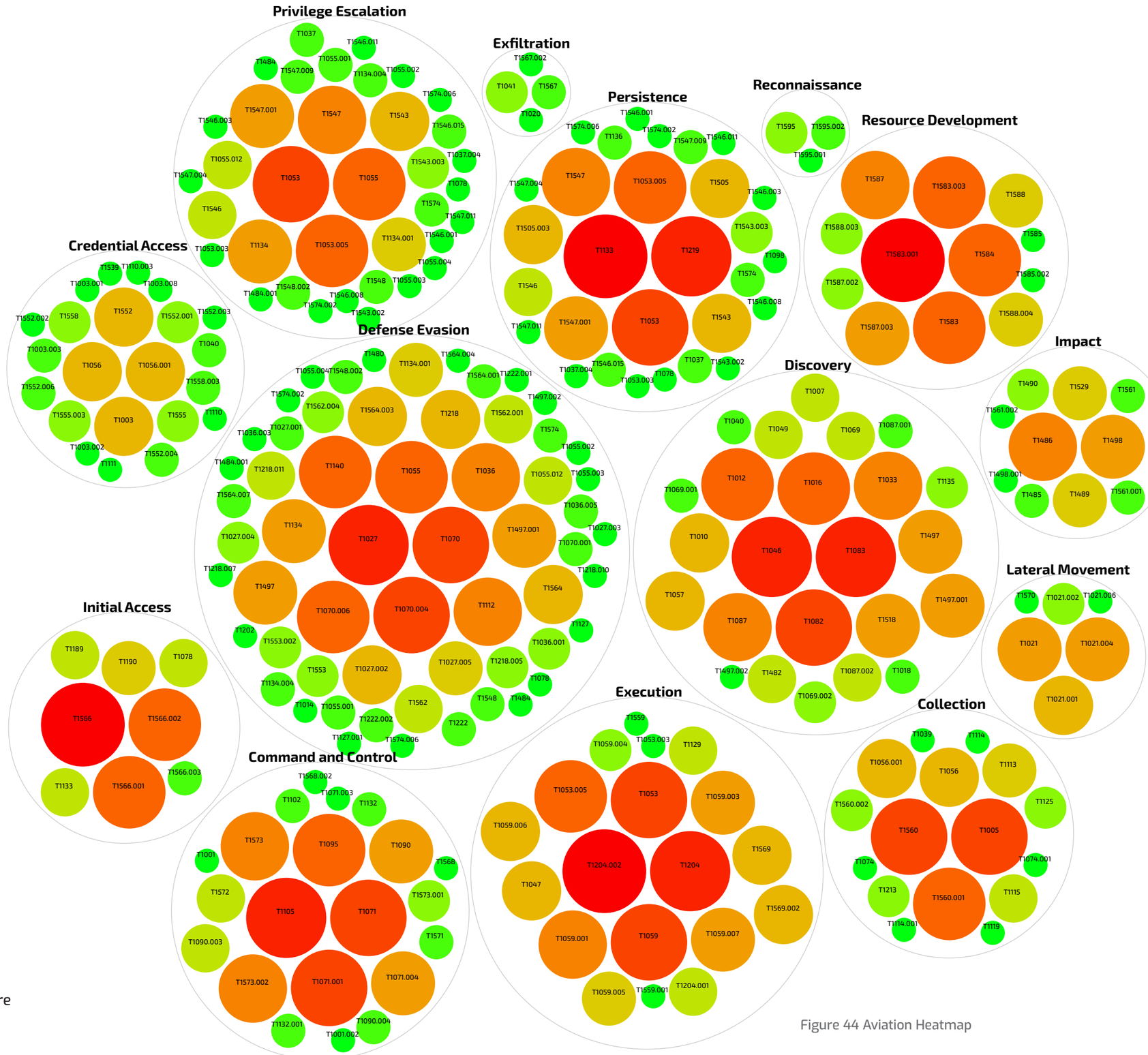


Figure 44 Aviation Heatmap

Understanding the prevalent attack techniques allows us to prioritize our defence activities effectively. In the following figure, we present a list of the **Top 10 Mitigation Means** measures related to the most used techniques for attacking aviation.

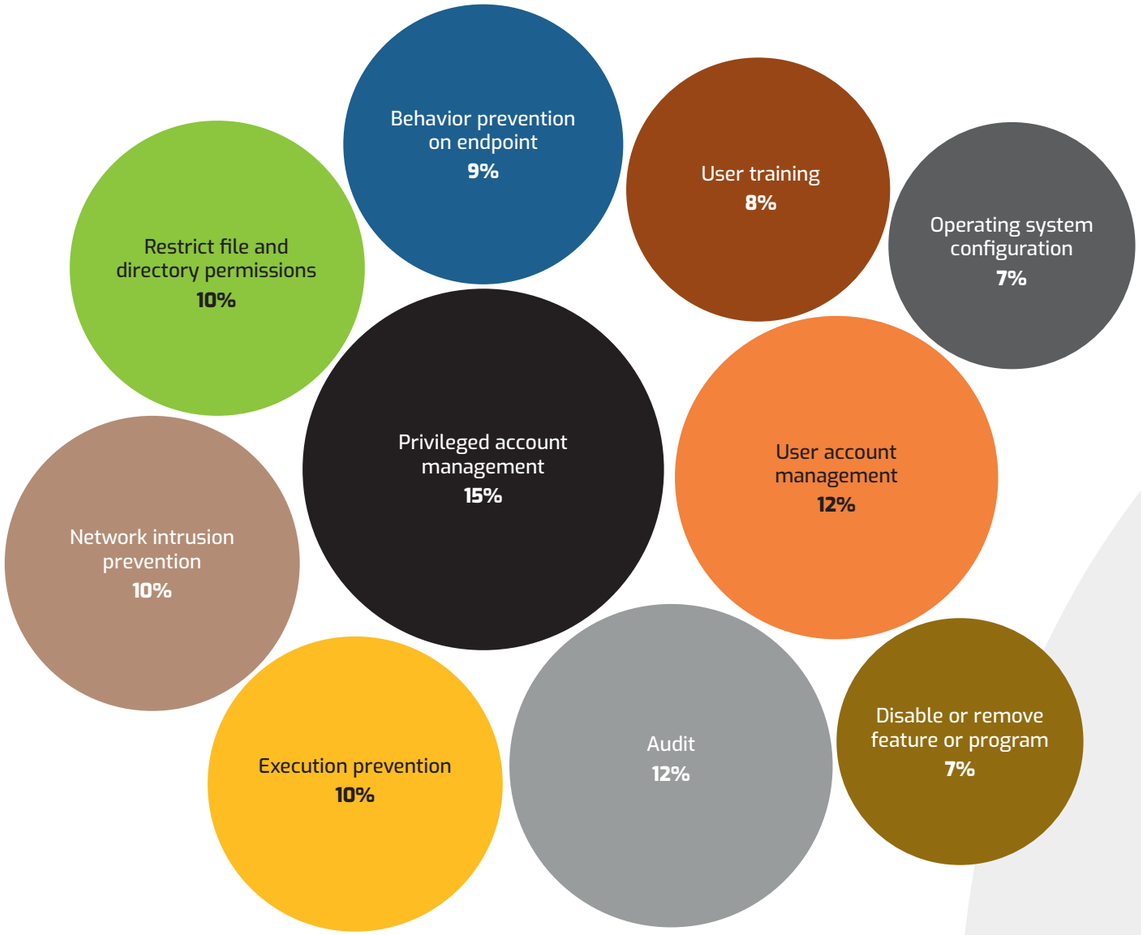


Figure 45: Identified mitigations

The aviation heatmap helped us also derive the **top 10 Detection Means,** the most needed means to detect the techniques which are most used to attack aviation.

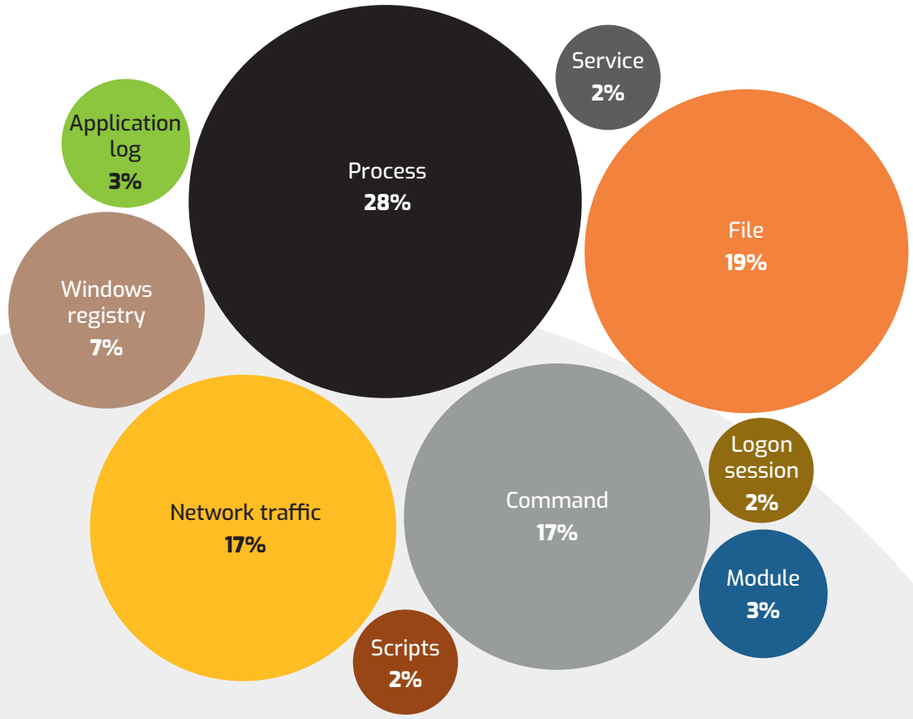


Figure 46: identified detections

Top 10

TOP 10 Findings based only on 2023 dataset

This year, we conducted an additional analysis based solely on 2023 dataset, which includes information provided by stakeholders and data generated by the EATM-CERT and excluding APTs TTPs mentioned in section above. This analysis enables a more accurate assessment of threats affecting our industry.

The 2023 dataset reveals that 81% (5.126 of 6.320) of the cyber events description included MITRE ATT&CK TTP information. This substantial percentage underscores the high use rate of the MITRE framework within our stakeholders.

Figure 47 presents the distribution of the top 10 most critical techniques, derived exclusively from 2023 data.

The analysis of the top 10 MITRE ATT&CK framework techniques highlights several critical attack methods used by adversaries, emphasizing the need for robust cybersecurity measures. In 2023, only 14% of techniques used against aviation lacked mitigation means, and all of the top 10 techniques had mitigation means in place.

Here is breakdown of top 10 techniques based on their frequency:

1. **Compromise Infrastructure: Domains (T1583.001):**
   This is the most frequently observed technique. This involves attackers compromising domain names to facilitate their malicious activities, such as hosting phishing sites or command-and-control servers. The prevalence of this technique underscores the importance of securing domain infrastructure and monitoring for unauthorized changes.

2. **Phishing (T1566):**
   "Phishing" (T1566) remains second most significant threat. Attackers use phishing to deceive individuals into divulging sensitive information, such as login credentials or financial data. This technique's high frequency highlights the need for continuous user education and advanced email filtering solutions to detect and block phishing attempts.

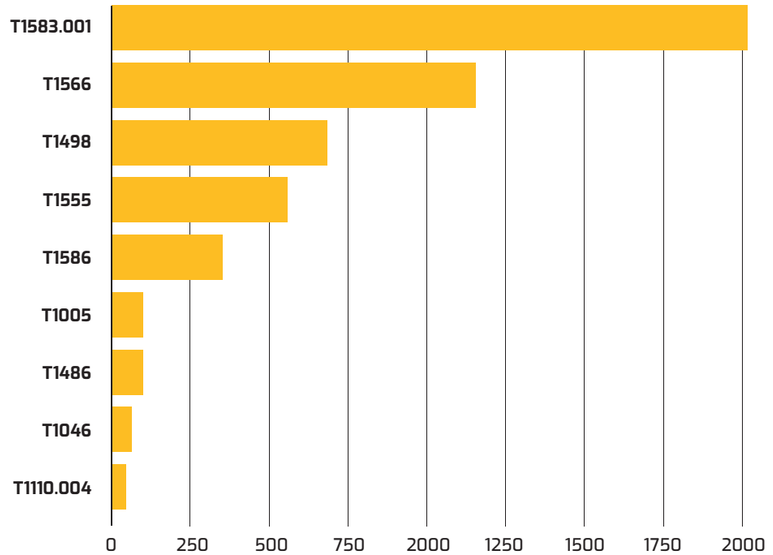


Figure 47: Top 10 techniques used by adversaries

3. **Network Denial of Service (T1498):**
   "Network Denial of Service" (T1498) is the third most common technique. Attackers use this method to overwhelm network resources, rendering services unavailable and causing significant disruptions. Implementing robust DDoS protection measures is crucial to mitigate the impact of such attacks.

4. **Credentials from Password Stores (T1555):**
   Extracting credentials from password stores is a common method attackers use to gain unauthorized access to systems. Securing credential storage and implementing multi-factor authentication are vital countermeasures.

5. **Compromise Accounts (T1586):**
   Attackers often target user accounts directly to compromise them. Ensuring strong account security practices is essential to mitigate this risk.

6. **Exploitation for Credential Access (T1212):**
   This technique involves exploiting system vulnerabilities to gain access to credentials. Regular patching and vulnerability management are crucial to protect against this technique.

7. **Valid Accounts (T1078):**
   Using valid accounts to gain access is a method that bypasses many security mechanisms. Monitoring for unusual account activity can help detect such intrusions.

8. **Command and Scripting Interpreter: PowerShell (T1059.001):**
   PowerShell is a powerful scripting language often exploited by attackers. Restricting and monitoring its use can help mitigate associated risks.

9. **Account Manipulation (T1098):**
   Manipulating account properties to gain elevated privileges is a common technique. Ensuring proper account management and audit trails are essential defenses.

10. **Windows Management Instrumentation (T1047):**
    WMI is used for remote management and can be exploited by attackers. Limiting WMI use and monitoring for suspicious activity can reduce this risk.

Conclusion

The most important events against aviation highlighted by this analysis are those that involve **compromising infrastructure, phishing, and denial of service.** These techniques not only occur frequently but also have the potential to cause significant disruption and damage. Therefore, organizations should prioritize strengthening defenses (prevention, mitigation, and detection) against these techniques by implementing robust security measures, educating users, and maintaining vigilant monitoring practices.

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

The Cyber Impact Landscape: **Insights and Implications**

The ever-changing **dynamics** of the **aviation** industry necessitate a thorough comprehension of the **specific effects of attacks** on stakeholders. After analyzing the threat actors, scrutinizing the affected targets, and studying the various attack methods used, this section delves into the repercussions faced by the industry and its stakeholders.

The **effects** can be **divided** into several unique **categories**, each with its own significance and potential for devastating consequences. These include:

- **financial loss,**
- **operational disruption,**
- **service interruption,**
- **leaks of confidential data,**
- **theft of sensitive data,**
- **reputational impacts,**
- **legal implications,**
- **impacts that are still unknown.**

These factors combine to depict a complicated scenario of vulnerability and risk within the aviation sector. It is crucial to understand that the total of individual impact categories surpasses the total number of reported attacks on aviation stakeholders. This discrepancy is due to the intricate nature of cyberattacks, where a single attack often leads to multiple outcomes. For example, a breach could simultaneously result in financial loss, theft of sensitive data, and damage to reputation.

Throughout the aviation sector, stakeholders classified a total of **6.320** cyber incidents based on their perception of each threat's severity. Their evaluations showed that the majority of these, specifically **3.600** cases or **57%** of the total, were perceived as **'Low'** severity attacks. **'Medium'** severity incidents followed, with stakeholders identifying **2020** such cases, making up **32%** of all recorded threats.

While **'High'** severity threats were less common, they were still recorded **193** times, accounting for **3%** of the classifications. The most severe category, **'Critical'**, was identified only **7** times.

Furthermore, this year we have introduced a category known as 'Informational'. Even though it is ranked below 'Low', it can still contribute value to the evaluation.

None of the scrutinized incidents that were categorized to offer essential value had any effect on safety.

At first glance, one might infer that the overall **impact of cyberattacks** on aviation is relatively minor, as the **'Low'** severity category significantly **dominates**. However, this can be **deceptive**, as the **cumulative impact of all** those 'Low' events **is not insignificant**. For instance, the impact of a single fraudulent website impersonating an Airspace User is categorized as 'Low,' but the cumulative effects of all these fraudulent website impersonations are quite substantial from a financial perspective.

A closer look at the specific impacts on each stakeholder will offer a more detailed understanding of how different types of impacts have affected various participants within the industry.

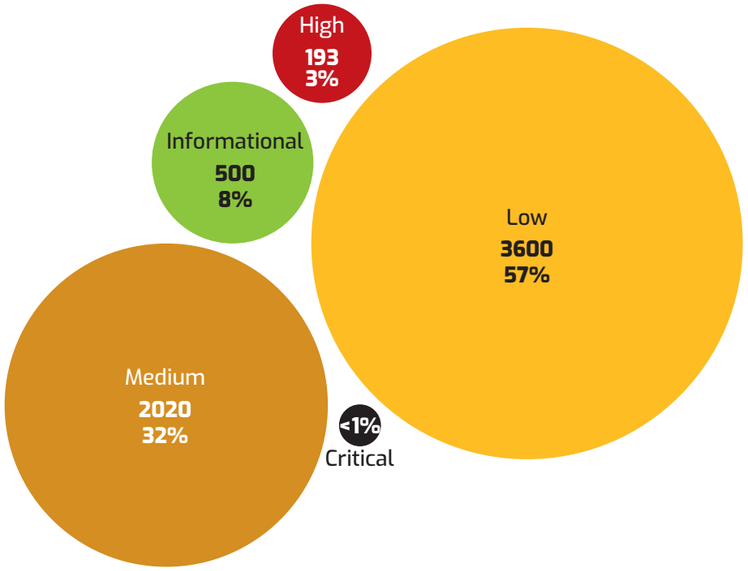


Figure 48: 2023 attacks severity

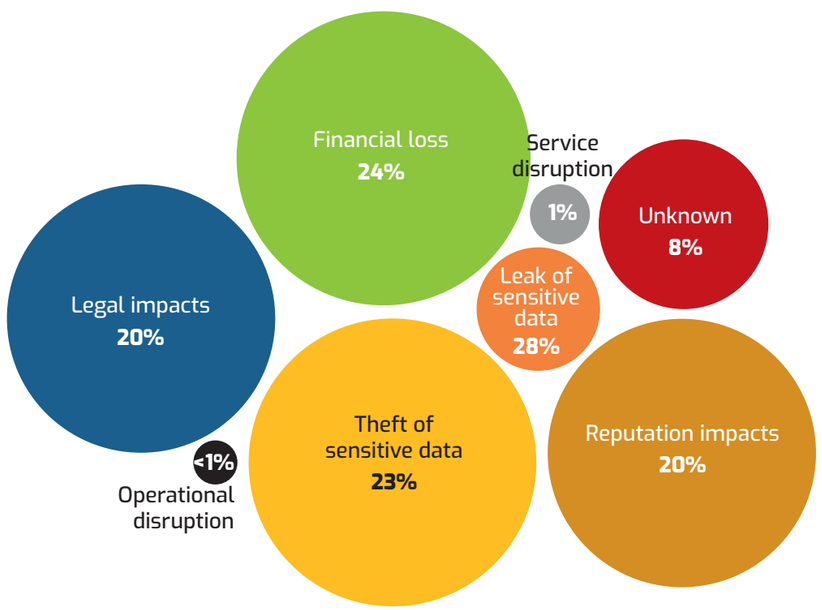


Figure 49: Airspace Users attack impact

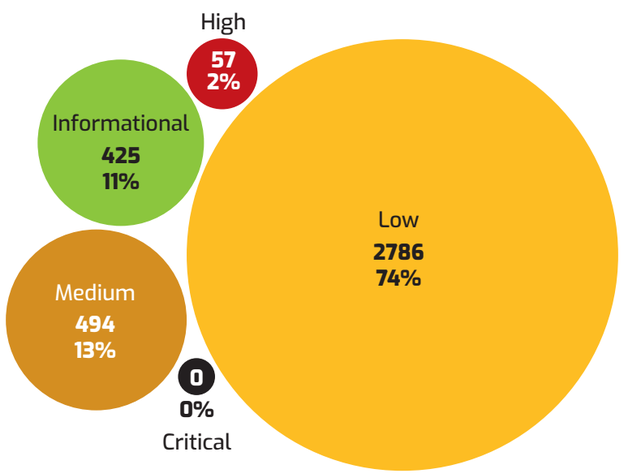


Figure 50: Airspace Users attack severity

Costly Clusters: Financial Loss and Data Theft in Airspace Users

In **2023, Airspace Users** in the aviation industry encountered a notably difficult cyber environment. **Financial motivations**, as demonstrated by the **24%** of impacts related to financial loss (**2.309** incidents), were a significant driving force for threat actors targeting this sector. However, the theft of **sensitive data** was even more prevalent, accounting for **23%** (**2.247** incidents). This underscores both the worth of the information possessed by Airspace Users and the unyielding efforts by adversaries to obtain it. Impacts on **reputation** were also significant, constituting **~20%** (**1.946** incidents), shedding light on the extent of harm an attack can cause to an organization's reputation and credibility. **Legal** consequences were also considerable, representing **~20%** (**1.900** incidents), underscoring the potential regulatory and legal issues that can emerge from cybersecurity breaches. **Service disruptions (1%), leaks of sensitive data (4%)**, and **operational disruptions** further illustrated the diverse nature of cyber threats. Lastly, **8% (796) unknown** impacts served as a stark reminder of the h**idden risks** that might not be immediately apparent but can have long-term implications for the industry.

For **Airspace Users**, out of the reported **3.762** incidents, the vast majority, amounting to **74%** or **2.786** cases, were of **'Low'** severity. This dominant trend is contrasted by the **'Medium'** severity attacks, which made up only **13%** with **494** instances. **'High'** severity attacks, while less common, constituted **2%** of the total with **57** instances. The **'Informational'** severity was assigned to **425** occurrences which translates to **11%.**

The intricate nature of the repercussions of cyberattacks is nowhere more evident than in the impacts against **Airspace Users**. A closer look at the figures reveals close numbers across **different impact categories**, including **financial loss, theft of sensitive data, reputation damage, and legal impacts.** These numbers not only illuminate the immediate consequences of cyber threats but also shed light on the complex network of secondary and even tertiary effects that can ripple through an organization. Such impacts often intertwine, where a data theft might lead to both immediate financial losses and long-term reputation damage, with ensuing legal complications.

Continue your exploration on the effects of Airspace Users in Airspace Users: Websites and Social Media as the Prime Targets.

A Reputation at Risk: Airports' Cyber Impact Analysis

Airports, crucial connectors of global travel, grappled with a wide array of cyber challenges in **2023**. Among the impacts, **damage** to their reputation emerged one of the most significant, accounting for **19% (414)** of the total repercussions. This highlights the critical role of maintaining trust and confidence with the traveling public.

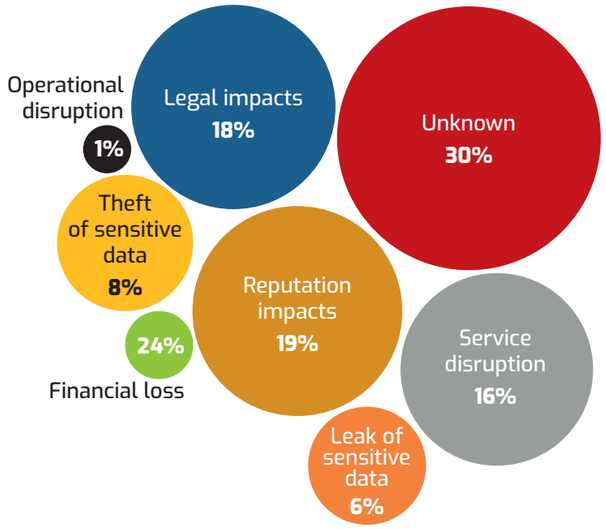


Figure 51: Airports attack impact

Legal implications were a close second, making up **18% (396)** of the impacts, indicating potential regulatory challenges and litigations. **Service disruptions** also surfaced by **350 (16%)** reflecting the difficulties airports faced in maintaining consistent operational efficiency amidst cyber threats.

The combined **theft (8% or 176)** and **leak of sensitive data (6% or 130)** are underscoring the ongoing threats to airport data integrity. **Financial losses** were less prominent but still present, accounting for **2% (47)** of the impacts.

Operational disruptions and **unknown** impacts completed the list, at **1% (11)** and a significant **30% (666)** respectively. Upon analysing the dataset, it is clear that **airports face** considerable **repercussions** in terms of **reputational damage**. This is primarily **due to** each **Distributed Denial of Service (DDoS)** attack being categorized as **having** a significant **impact** on **reputation** due to the **public attention** related to the attacks performed by the hacktivists. **In reality**, as the data shows, those **attacks** have almost no **operational impact** on the airports. Furthermore, with a variety of incidents involving website compromises and the theft of sensitive data, it is not surprising that the 'reputation impact' metrics are high.

For **Airports**, out of a total o**f 1.220** incidents, the primary concern was **'Medium'** severity attacks, which were reported **1.090** times, accounting for **89%** of all cases. **'Low'** severity attacks were the next most common, with **96** instances, representing 8% of the total. **'High'** severity threats, though less frequent, were still present, with **21** instances, making up 2%. Meanwhile, the **'Critical'** category was reported on **1** occasion.

Continue your exploration on the effects of Airports in Main Targets: An Analysis of Airport Attack Patterns and Their Prime Targets.

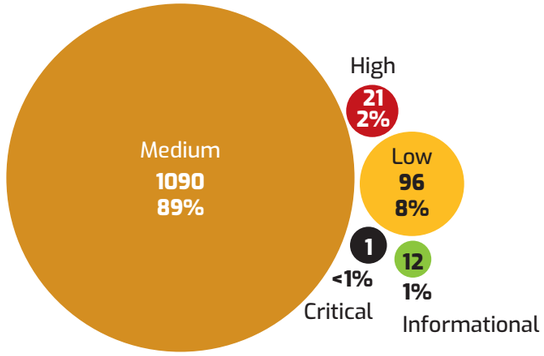


Figure 52: Airports attack severity

Data Heists in the Sky: ANSPs' Cyber Struggle

In the aviation sector, **Air Navigation Service Providers (ANSPs)** faced a diverse range of cyber impacts in **2023**. **Service and operational disruptions** are representing **45% (204)** and **1% (4)** of the impacts, emphasizing the tactical vulnerabilities within the operational environment of ANSPs. **Theft of sensitive data (17% or 75 occurrences)** combined with **leaked (17% or 73 occurrences)** showing an importance of the data protection within ANSP, especially those that consider Intellectual Property or Personal Identifiable Information. **Reputational consequences**, accounting for **6% (67)**, further highlighted the delicate balance ANSPs must uphold between operational excellence and public trust.

The sphere of legal **implications,** capturing **5% (24),** points to the complex network of regulatory complications that can follow a security breach. Notably, **financial losses,** which amounted to a mere **1% (5),** suggest that monetary motivations might not always be the primary driver behind attacks on ANSPs.

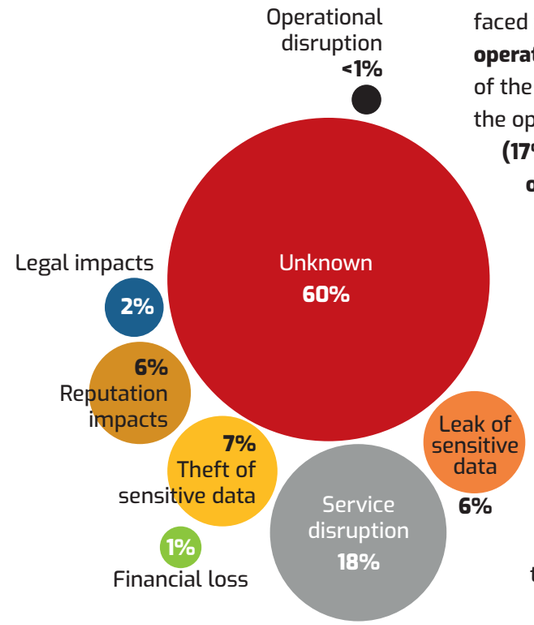


Figure 53: ANSP attack impact

For **ANSPs**, among the **1.025** reported incidents, the majority, representing **64% or 659** cases, fell into the **'Low'** severity category. '**Medium'** severity attacks, which were reported **260** times, accounting for **25%** of all cases. '**High'** severity threats, though less frequent, were still present, with **42** instances, making up **4%**. While most threats were of lower severity, the presence of **6** 'Critical' attacks, constituting **1%** of the total, was also noted.

Continue your exploration on the effects of ANSP in End Users as ANSPs' Top Cyber Concern.

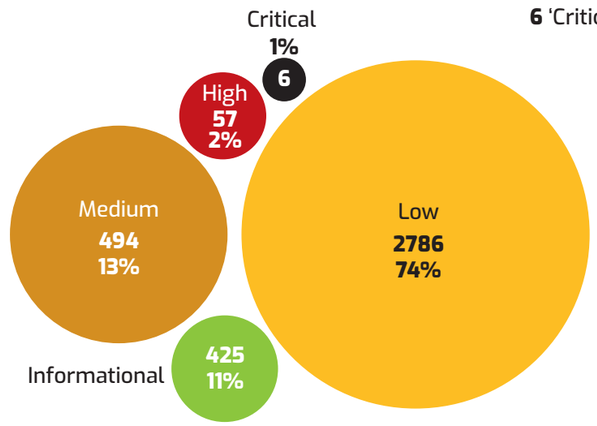


Figure 54: ANSP attack severity

Stolen Bytes: Data Theft and Its Impact on Aviation Supply Chain providers

In the aviation industry, **Aviation Supply Chain** providers navigated a complex cyber landscape in **2023**. The **theft and leak of sensitive data** was one of the prominent, accounting for nearly **8% (42)**, highlighting the valuable nature of proprietary information within the manufacturing sector. **Aviation Supply Chain providers** also grappled with significant reputation challenges, which made up approximately **14% (73)** of the total impacts. These figures underscore the dual burden Aviation Supply Chain providers face in protecting their invaluable intellectual assets and maintaining their public image. The **legal** aspect that is closely linked to those incidents was identified in **21%** which stands for **103** attacks. A significant number of incidents **(30%)** remains still **unknown**.

Learn more about unknowns in chapter: The Enigma of Airspace: Deciphering the Unknowns in Aviation Cybersecurity.

Out of a total of **225** cyber incidents, the **'Medium'** severity attacks took a prominent position with **108** instances, accounting for **48%** of the total. **'High'** severity attacks followed, making up **30%** or **67** instances. **'Low'** severity threats were noted in **45** cases, which constitutes **20%**.

Continue your exploration on the effects of Aviation Supply Chain in The Supply Chain Frontline: Systems and Networks as Primary Targets.

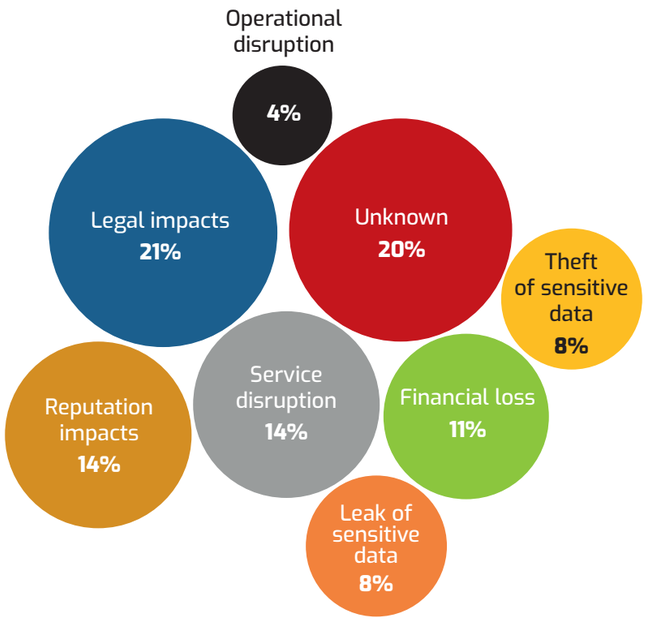


Figure 55: Aviation Supply Chain attack impact

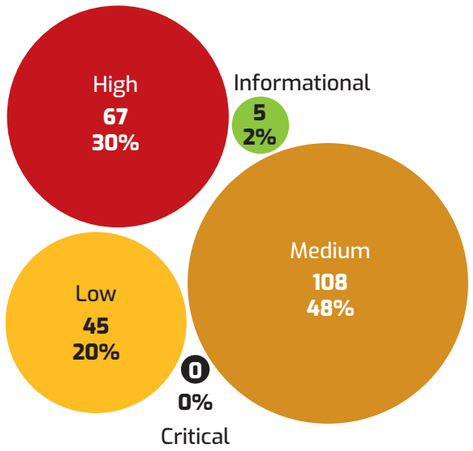


Figure 56: Aviation Supply Chain attack severity

The Trust Equation: CAAs' Battle with data stealers

In 2023, **Civil Aviation Authorities (CAAs)** found themselves navigating a complex cyber ecosystem. Each of impacts related to incidents represented a unique aspect of their cybersecurity challenges.

Sensitive **data theft (27% or 52 occurrences)** and **leak (27% or 51 occurrences)** emphasizing the ongoing efforts by adversaries to obtain valuable information from regulatory bodies.

Reputational consequences were, making up a significant **15% (29)** of the total impacts. This highlights the substantial responsibility that CAAs carry in maintaining trust and credibility with both the public and the aviation entities they regulate.

Legal repercussions, which made up **13% (25)** of the impacts, underscored the regulatory and compliance issues that can arise from security breaches.

Service disruptions, which constituted **15% (28)** of the impacts, demonstrated the vulnerabilities in the operational frameworks of the CAAs. **Financial losses**, although relatively lower **(2)**, suggested that the motives behind cyberattacks on CAAs often go beyond direct financial gains.

Out of the **88** documented cyber incidents for CAAs, the majority were classified as **'Medium'** severity, accounting for **77% or 67** instances. **'Low'** severity attacks followed, making up **16%** with **14** instances. **'High'** severity attacks, although less frequent, were still observed, making up **7%** of the total with **4** reported cases. This distribution underscores the variety of cyber threats that Civil Aviation Authorities face, highlighting the need for vigilance and comprehensive security measures across all levels of attack severity.

Continue your exploration on the effects of CAA in CAA Cyber Spotlight: Internal end user becomes important.

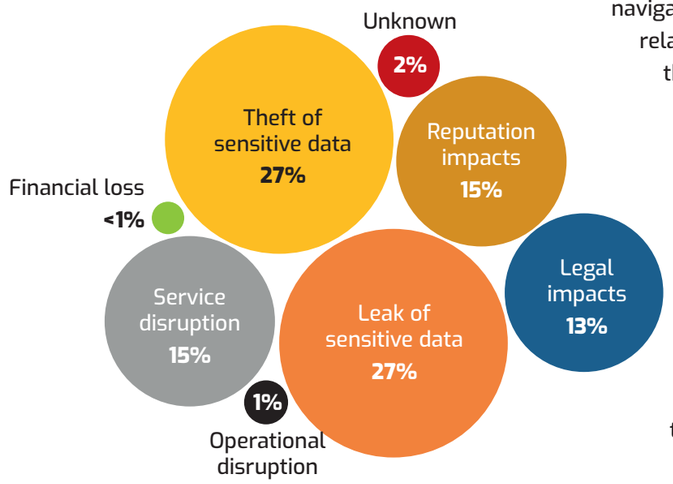


Figure 57: CAA attack impact

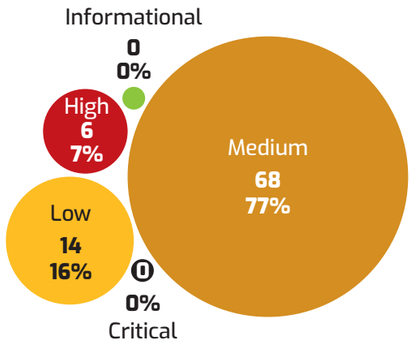


Figure 58: CAA attack severity

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

Landing on Target:

An Asset-Centric Analysis on Aviation Cybersecurity

This section transitions from examining the threat actors who have attacked the aviation industry and their motivations and methods, to **focusing on the specific digital assets** that may have been targeted in these cyber-attacks. This includes potential targets such as:

- **Credentials**
- **End users (internal – employee, external – customer)**
- **Internet presence impersonation (fake websites or social media profiles)**
- **Sensitive data**
- **Systems and networks**

The range of potential targets within the industry is extensive and intricate. This section adopts a stakeholder-centric approach, investigating which digital asset is most or least targeted among various aviation stakeholders. By analysing the complex dynamics and highlighting the actual assets and digital components at risk, this section aims to offer an in-depth view of the wider landscape of cyber threats and contribute to the guide for proactive defence in the aviation industry.

Regrettably, some targets are labelled as "Unknown" Learn more about unknowns in chapter: The Enigma of Airspace: Deciphering the Unknowns in Aviation Cybersecurity.

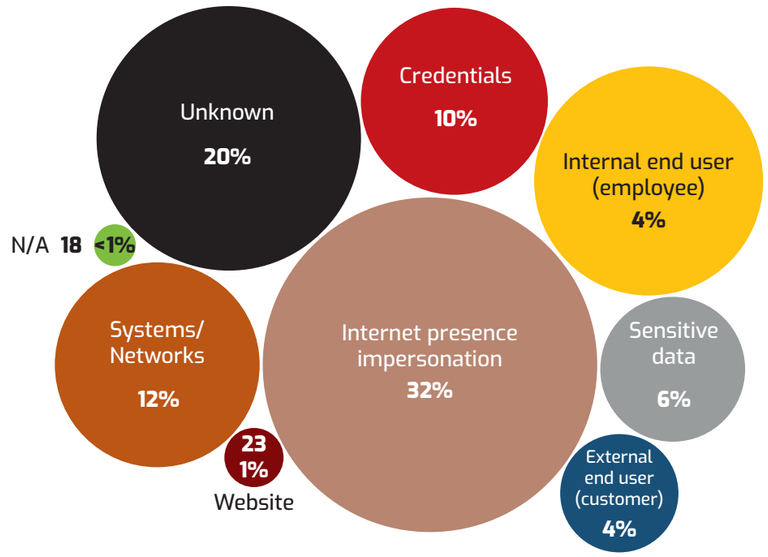


Figure 59: Aviation targets in 2023

TLP:GREEN

Airspace Users: Websites and Social Media as the Prime Targets

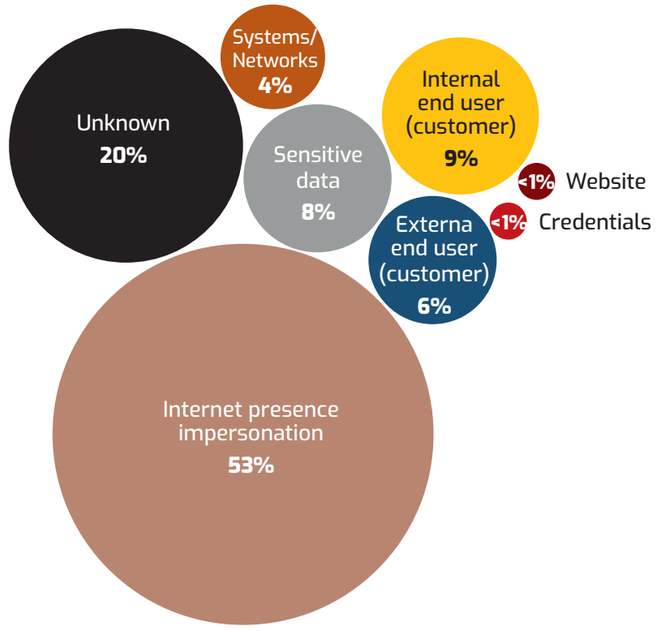


Figure 60: Attacks against Airspace Users

Internet presence impersonation appear to be the **primary targets of cyber-attacks** on Airspace Users, accounting for approximately **32%** of the total impacts with **1.974** instances. It is around **600 incidents more than last year**. The primary reason for this is that these attacks are often based on social engineering tactics, where cybercriminals impersonate airlines by creating duplicate social network accounts or websites.

It is important to note that **Airspace Users are unable to prevent** the impersonation of their websites. The **creation of a fraudulent website** that impersonates an organization does **not involve hacking, exploiting vulnerabilities, or any form of weakness abuse.** It is **only** through the c**ollaboration between aviation cyber entities** like EATM-CERT and **Airspace Users** that fraudulent **websites** can be **detected** and **taken down**, thereby **mitigating** their **impact**.

Following this, **Internal End user (employee)** has been **targeted 337** times, making up **9%** of the total victim. **External End users,** primarily **understood as** airline **customers**, have been affected **233** times, constituting around **6%** of the total impacts. **Systems and networks**, are less frequently targeted, making up about **4%** with **148** instances. There significant part of the data set are **750** instances with **unknown** impacts, accounting for **20%** of the occurrences on Airspace Users.

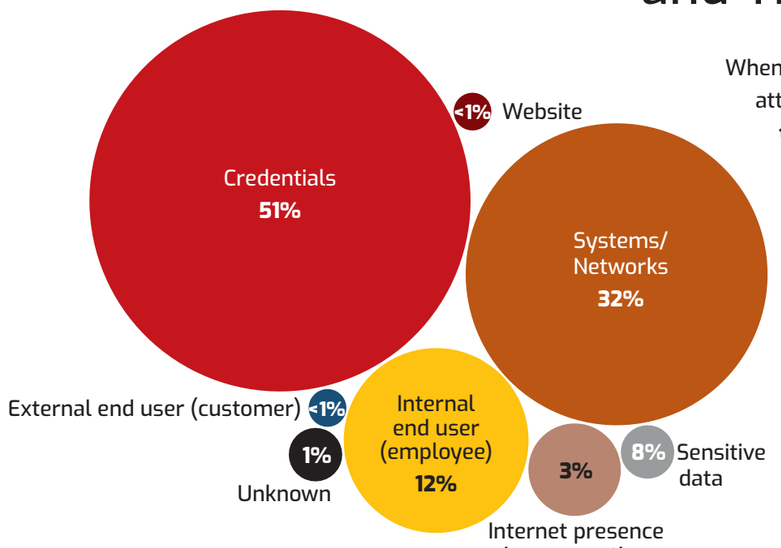


Figure 61: Attacks against Airports

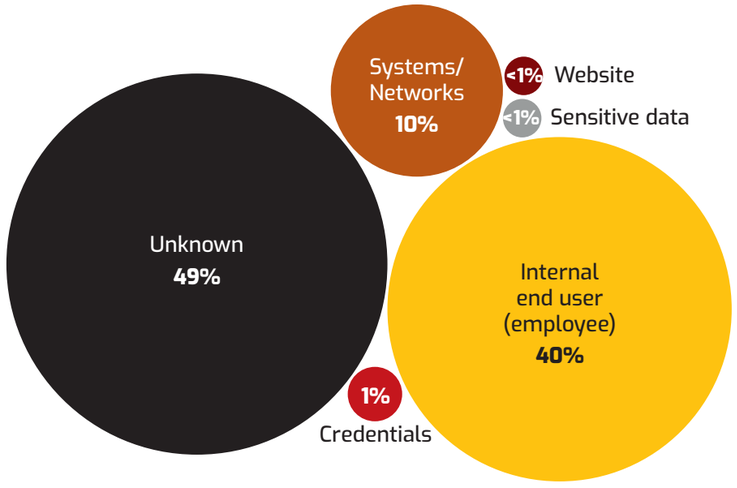


Figure 62: Attacks against ANSP

Main Targets: An Analysis of Airport Attack Patterns and Their Prime Targets

When we focus on **airports**, which experienced **1.220** attacks, it is clear that **credentials** are the **primary targets**, making up **51% (623)** of all potential targets. **Systems and networks** were the next most targeted, accounting for **32% (385)**, highlighting the crucial need for robust infrastructure security. **Internal End users (customer)** also formed a significant portion of the targets, comprising **12% (143)**, thereby emphasizing the human factor in cybersecurity risks. Finally, the category of **unknown** targets made up **1% (7)** of the total.

End Users as ANSPs' Top Cyber Concern

In the domain of **Air Navigation Service Providers (ANSPs)**, the array of potential digital assets targeted by attackers exhibits a unique pattern. Out of a total of **347 attacks, Internal end users (employees)**, appear to be the most susceptible, accounting for **34% (64)** of the attacks. **Systems/Networks** follow closely, constituting **6% (64)** of the total. **Credentials**, representing **1% (5)** of the targeted assets, underscore their strategic significance.

Websites and **External End user (customer)**, seem to be fewer appealing targets, contributing a **1% (5)** to the overall attacks. The **'Unknown'** category makes up a significant **58% (595)** of the targets. Learn more about unknowns in chapter: The Enigma of Airspace: Deciphering the Unknowns in Aviation Cybersecurity.

The Supply Chain Frontline: Systems and Networks as Primary Targets

Within the domain of **Aviation Supply Chain providers, Systems and Networks** are the **primary targets** of cyber threats, making up a substantial **48% (107) of the 225** recorded attacks. **Sensitive Data**, while not as frequently targeted, still represents a significant **23% (52)** of the total.

Credentials are also notable targets, accounting for **6% (14)** of the attacks. **Websites and Social Networks** comprising **5% (12)** of the attacks. The '**Unknown'** categories is only **4% (9)**. Learn more about unknowns in chapter: The Enigma of Airspace: Deciphering the Unknowns in Aviation Cybersecurity.

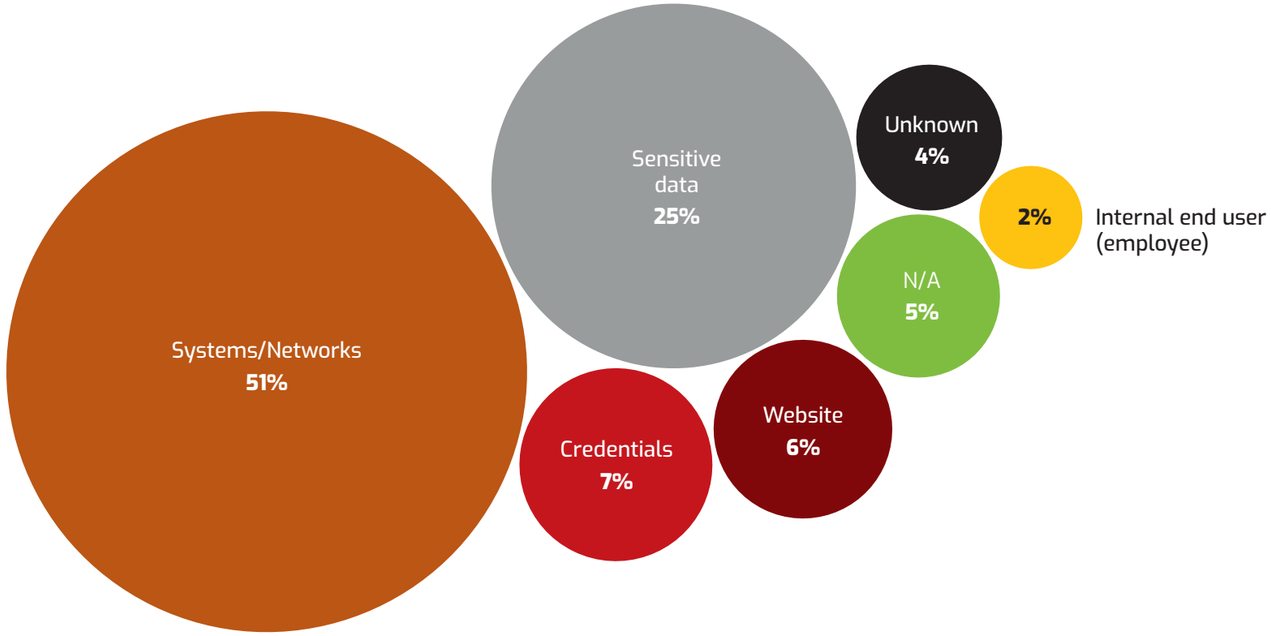


Figure 63: Attacks against Aviation Supply Chain

CAA Cyber Spotlight: Internal end user becomes important

The pattern of cyberattacks within the cyber landscape of **Civil Aviation Authorities (CAAs)** highlights specific areas of concern among targeted digital assets and offers insights into the priorities of attackers. The **'Internal End user (employee)'** category is the most significant, accounting for **55% (48)** of the total **88** recorded attacks. **System/Networks** is the next major area, making up **28% (25)** of the attacks.

Sensitive data is representing **6% (5)** of the targeted assets. Lastly, **External End user (customer)** and **Websites** seems to be the least targeted, contributing to **3% (3)** and **1% (1)** of the incidents.

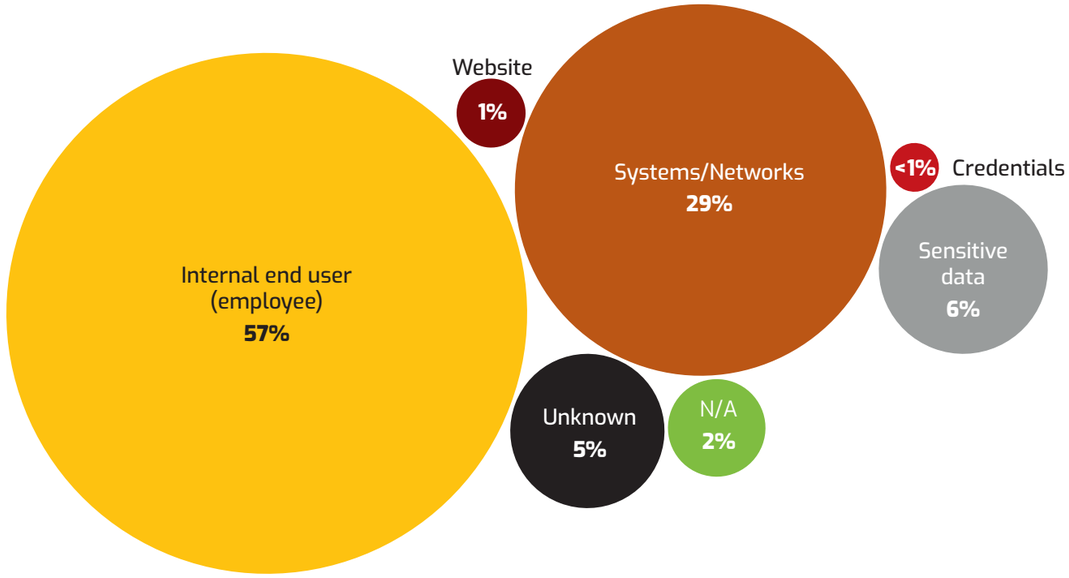


Figure 64: Attacks against CAA

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

MISP in Aviation:

The Growth of Cyber Threat Intelligence Sharing

The **MISP** (Malware Information Sharing Platform) is swiftly gaining traction as the go-to open-source tool for automated Cyber Threat Intelligence (CTI) data exchange. Its widespread adoption is due to its versatile capabilities:

- It provides various methods for intaking and processing intelligence data.
- It underscores the significant benefits of accessing shared data.
- Users can securely share their data without compromising sensitive information.
- It facilitates the correlation of new events with previously published ones, helping to identify links between current and past incidents.

By the close of 2023, EATM-CERT had established **58** connections with 21 national CERTs and 37 aviation stakeholders, showing an **increase of 2 CERT/NCSC connections and 5 aviation stakeholders** compared to 2022. Requests from constituents continue to come in annually, and efforts are ongoing to ensure coverage across all member states and their aviation stakeholders.

EATM-CERT aims to both collect and disseminate threat information, thereby heightening cyber-threat awareness in the aviation sector. This mission not only enhances EUROCONTROL's protection but also positions EATM-CERT as a pivotal **facilitating hub for aviation CTI.** However, it is worth noting that only a limited number of aviation stakeholders have contributed events to MISP so far.

Looking ahead, EATM-CERT is dedicated to sharing incident data via MISP, ensuring that all stakeholders are promptly informed of emerging cyber threats targeting the aviation industry.

TLP:GREEN

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

The Importance of Time and Automation in Cyber Threat Intelligence: How MISP Enhances CTI Effectiveness

Time and automation are crucial elements of effective Cyber Threat Intelligence (CTI), and the Malware Information Sharing Platform (MISP) excels in both areas, significantly enhancing the efficiency and responsiveness of cyber threat management.

Time:

MISP facilitates the timely sharing of CTI, allowing for progressive updates of the same event. This is a game-changer in incident analysis and response. Unlike traditional email alerts, which are limited and often delayed, **MISP can support multiple, real-time updates.** For example, during an incident analysis, an event on MISP can be updated multiple times (e.g. 20) with new information such as Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs). In contrast, the same process might involve only two or three email alerts, which would be sent out after the MISP updates have already occurred. This capacity for **continuous and timely updates** ensures that all stakeholders have access to the latest intelligence, enabling **more informed and quicker decision-making.**

Automation:

MISP's ability to automate the entry of information into security devices is another major advantage. By integrating directly with Security Operations Centres (SOC), firewalls, antivirus software, Intrusion Detection/Prevention Systems (IDP/IPS), … **resource-intensive and time-consuming human intervention**. In the event of a cyber incident, rapid response is critical. The automated sharing and updating of CTI through MISP allow organizations to quickly.

deploy defensive measures, protecting their infrastructure with the latest intelligence shared by others in the MISP "network".

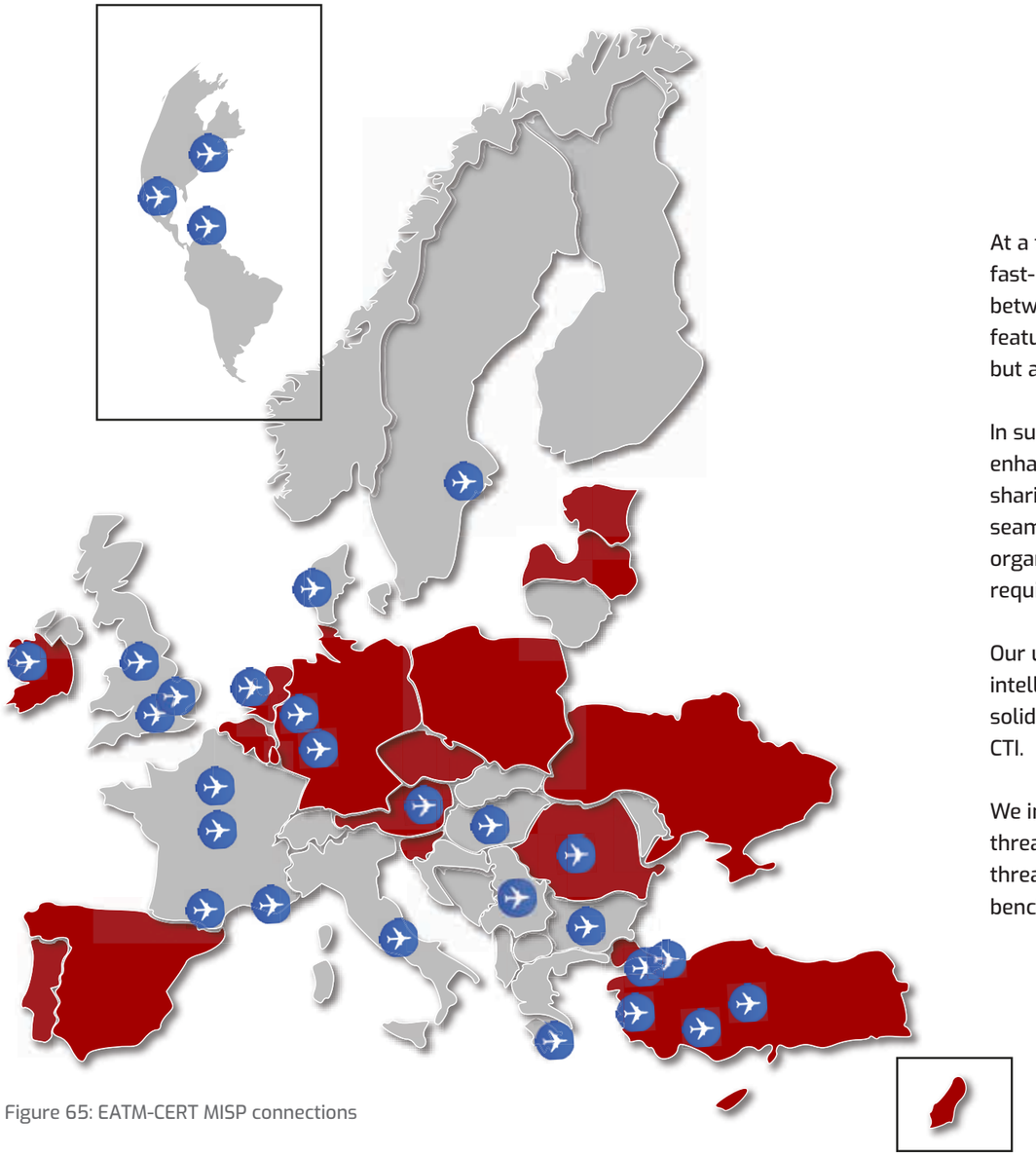


Figure 65: EATM-CERT MISP connections

At a time when cyber threats are increasingly sophisticated and fast-moving, the ability to react quickly can mean the difference between containment and widespread compromise. MISP's features ensure that organizations are not only better informed but also better equipped to act swiftly and effectively.

In summary, MISP stands out as an indispensable tool for enhancing CTI through its capabilities in time-sensitive information sharing and automation. By enabling continuous updates and seamless integration with security devices, MISP ensures that organizations can respond to threats with the speed and precision required in today's cyber landscape.

Our unwavering goal is to facilitate bi-directional sharing of threat intelligence, thereby reinforcing cyber threat awareness and solidifying our status as a leading knowledge centre for aviation CTI.

We invite all stakeholders to actively participate in bi-directional threat data sharing, which will significantly enhance cyber threat intelligence in the aviation sector and help us become a benchmark for aviation CTI.

AVIATION STAKEHOLDERS

Austria – Austrocontol (ANSP)
Belgium – DHL
Bulgaria – BULATSA (ANSP)
Denmark – NAVIAIR (ANSP)
France – CERT-AIRBUS A/C
France – Groupe ADP
France – DSNA
France – Air Caraïbes
Germany – DLH-DE – Lufthansa Group
Germany – Frankfurt Airport
Greece – HANSP
Hungary – HungaroControl (ANSP)
International – IATA
International – AMADEUS
Ireland – Shannon airport
Italy – Aeroporto Di Roma
Mexico – Aero Mexico Airlines
Netherlands – Schiphol Airport
Romania – CAA-RO
Serbia & Montenegro – SMATSA (ANSP)
Sweden – Swedavia (airports)
Turkey – CERT-THY (Turkish Airlines)
Turkey – DHMI (ANSP)
Turkey – IGA Istanbul Airport
Turkey – Celebi Ground ops
Turkey – SGIA Airport
UK – British Airways
UK – Heathrow Airport
UK – Manchester Airport Group

NATIONAL CERT/NCSC

Austria (CERT.at)
Belgium (CERT.be)
Cyprus (CSIRT-CY)
Czech republic (CSIRT.cz)
Europe .eu (CERT-EU)
Estonia (CERT-EE)
Germany (CERT-Bund)
Ireland (CSIRT-IE)
Israel (CERTGOVIL)
Latvia (CERT.LV)
Luxembourg (CIRCL)
Netherlands (NCSC-NL)
Poland (CERT.GOV.PL)
Portugal (CERT-PT)
Romania (CERT-RO)
Slovenia (SI-CERT)
Spain (INCIBE-CERT)
Spain (CCN-CERT)
Turkey (TR-CERT)
Ukraine (CERT-UA)

Data Collection Trends

Figure 66 and Figure 67 show some statistics collected from EATM-CERT MISP.

If we look at the new incidents reported by our connected partners, there was a steady increase (Figure 66) between Q1 and Q4.

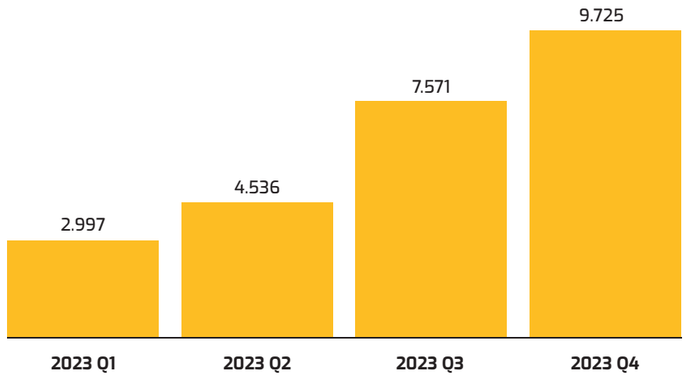
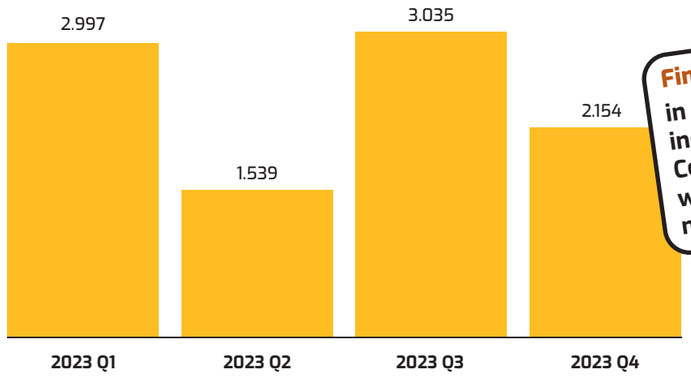


Figure 66: Total numbers of new Incidents received by the MISP in 2023

Although some variations from quarter to quarter can be observed, they are not that significant.



Finding:
in 2023, there is steady increase in new incidents. Compared with 2022, there was nearly 3 times more new events in 2023.

Figure 67: Number of new incidents received by the MISP by quarter in 2023

Examination of the Top 10 IOCs on MISP

The top10 IOCs (indicators of compromise) types shared on the MISP in 2023 are (see Figure 68):

- Source IPs
- URLs
- File hashes
- File names

Benefit:
These IOCs can be used proactively to prevent potential attacks on an environment and can be ingested automatically into SIEM products or perimeter security devices, such as IPS and firewalls.

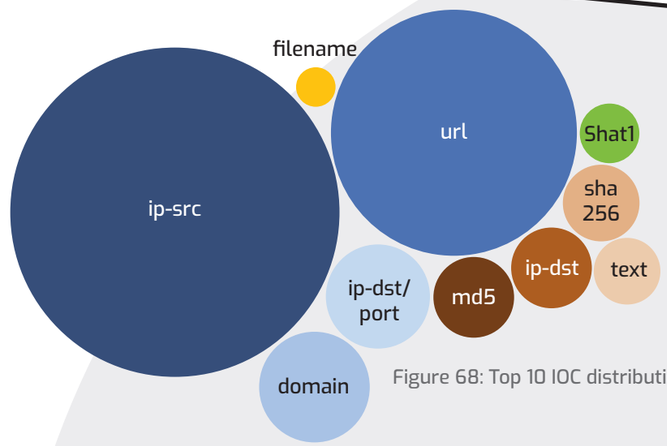


Figure 68: Top 10 IOC distribution

Insight into the MITRE ATT&CK Techniques on MISP

The MITRE ATT&CK framework is globally acknowledged as a comprehensive knowledge base and taxonomy of adversary tactics and techniques observed in real-world scenarios. Complementing this, the Malware Information Sharing Platform (MISP) acts as an essential repository for cyber threat intelligence, providing crucial insights into current cyber threats and vulnerabilities.

"T1566-Phishing" and **"T1598-Phishing for information"** and are the most used techniques in 2023 just like the past years. (see Figure 69)

The next frequently employed technique is **"T1498"** which is utilized to carry out Denial of Service attacks. This technique's prevalence aligns with the observation that DDoS attacks were a favoured method among adversary groups in 2023.

Continue your exploration of MITRE ATT&CK in Costly Clusters: Financial Loss and Data Theft in Airspace Users.

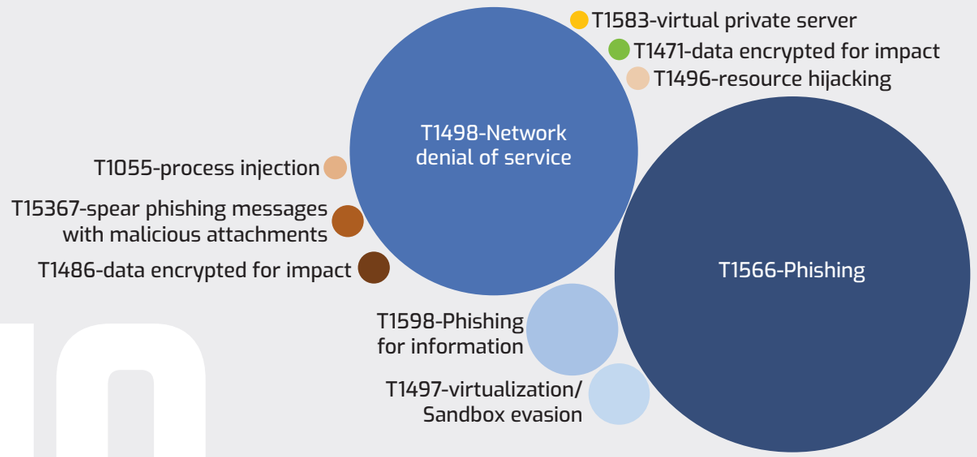


Figure 69: Top10 MITRE ATT&CK Techniques in MISP in 2023 – all sectors

Top 10

TLP:GREEN

Wall of Fame

We extend our heartfelt gratitude to the impressively numerous organizations that have generously contributed to this report by sharing their cybersecurity events and accepted to have their logo on our wall of fame.

Your collaboration and transparency are invaluable in advancing our collective understanding and resilience in the face of cyber threats.

We also recognize and appreciate the contributions of those many organizations who, while choosing to remain anonymous, have played an essential role in this endeavour. Your support is equally significant, and we are grateful for your commitment to enhancing cybersecurity in aviation.

Thank you for your dedication and partnership.

Glossary

This report study aims to provide an in-depth examination of the cyber threat landscape faced by the aviation sector in 2023. The information for this report has been sourced from EUROCONTROL/ EATM-CERT and analysed using the same methods as previous editions. Given the technical scope of this research, it is crucial to clarify the specific terminology and naming conventions used throughout to ensure clarity and precision for the readers. These definitions are used:

- Incident: a security event that compromises the confidentiality, integrity, or availability of an information asset. This event can lead to:
  - disruption of service.
  - financial loss.
- Event: an occurrence that may have affected an organization (no evidence of any direct or indirect impact but worth being considered) such as a leak of sensitive information or a disclosure of vulnerability.
- Incidents and events were classified using the following categories:
- Data theft – an intentional act of stealing sensitive data from the organization that was compromised.
- Defacement – an intentional act in which webpage content is replaced with something aligned with the actor's motives.
- Leak of sensitive documents – This can be the intentional or unintentional act of releasing sensitive documents to an inappropriate broader audience or to the public.
- Phishing – the intentional action of sending an email crafted in a way to lure the email receiver into carrying out specific actions, as desired by the threat actor.
- Error – This is understood to be anything done incorrectly or left undone inadvertently without any malicious intent.

List of Tables & Figures

Acronyms & Abbreviations

A/C	Aircraft
ACI	Airports Council International
AI	Artificial Intelligence
A-ISAC	Aviation Information Sharing and Analysis Center
ANSP	Air Navigation Service Provider
AO	Airport Operator
API	Application Programming Interface
APT	Advanced Persistent Threat
ATC	Air traffic Control
ATM	Air Traffic Management
AU	Airspace User
AV	Antivirus
AWS	Amazon Web Services
BIOS	Basic Input/Output System
C&C	Command&Control
CAA	Civil Aviation Authority
CANSO	Civil Air Navigation Services Organisation
CERT	Computer Emergency Response Team
CIRCL.LU	The Computer Incident Response Centre Luxembourg
CPU	Central Processing Unit
CRCO	Central Route Charge Office
CSIRT	Computer Security Incident Response
CTI	Cyber Threat Intelligence
CYBERG	Cybersecurity Group`
DLL	Dynamic Link Library
EASA	European Union Aviation Safety Agency
ECCSA	European Centre for Cyber Security in Aviation
EDR	Endpoint Detection and Response
ENISA	The European Union Cybersecurity Agency
EVAIR	EUROCONTROL Volunteering ATM Incident Reporting
FMS	Flight Management System
IANS	Institute of Air Navigation Services
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
ID	Identification/Identity/Identifier
IMT	Information Management Team
IOA	Indicator of Attack
IOC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
ISMS	Information Security Management System
IT I	nformation Technology
MBR	Master Boot Record
MISP	Malware Information Sharing Platform
ML	Machine Learning
MUAC	Maastricht Upper Area Control Centre
NDA	Non-Disclosure Agreement
NDTECH	Network Directors of Technology Working Group
NID/PS	Network Intrusion Detection/Prevention System
NIS Directive	Network and Information Security Directive
NM	Network Management
NOP	Network Operations Portal
OEM	Original Equipment Manufacturer
OS	Operating System
OT	Operational Technology
OWASP	Open Web Application Security Project
PC	Personal Computer
PPD	Personal Privacy Device
RAT	Remote Access Tool
RDP	Remote Desktop Protocol
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOC	Security Operation Centre
SSL	Secure Socket Layer
TF-CSIRT	Task Force – Computer Security Incident Response Teams
TLS	Transport Layer Security
TTP	Tactics, Techniques and Procedures
URL	Universal Resource Locator
VBS	Visual Basic Script
WMI	Windows Management Instrumentation

SUPPORTING
EUROPEAN
AVIATION

www.eurocontrol.int