International Civil Aviation Organization

WORKING PAPER

AN-Conf/14-WP/136
30/6/24
Revision No.1
30/7/24

FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

Agenda Item 4: Hyper-connectivity of air navigation system
4.2 Cybersecurity and information system resilience

INFORMATION SHARING USING MALWARE INFORMATION SHARING PLATFORM (MISP) AND ITS CONTRIBUTION TO IMPROVE CYBERSECURITY AND INFORMATION SYSTEM RESILIENCE

(Presented by Brazil, supported by 20 Members States[1] of Latin American Civil Aviation Commission (LACAC))

REVISION NO. 1

EXECUTIVE SUMMARY

This working paper highlights Brazil's efforts in aviation cybersecurity regarding the sharing of cybersecurity information through the Malware Information Sharing Platform (MISP), aligning with ICAO's Cybersecurity Panel (CYSECP) proposals. It emphasizes that this solution requires no additional cybersecurity expenses and fosters collaboration among states, organizations, and industry to enhance cyber safety.

Action: The Conference is invited to:
a) note that the use case of MISP by Brazilian Department of Airspace Control (DECEA) as a platform for sharing cybersecurity information has been positive so far;
b) encourage Member States to adopt the MISP as a platform for sharing cybersecurity information; and
c) bring the topic of this paper to the Cybersecurity Panel (CYSECP) and create a Working Group to address the standardization of cybersecurity information sharing and the potential use of the MISP platform by the Member States.

1. INTRODUCTION

1.1 ICAO continually improve its standards and regulations to address the constantly changing global threat landscape, aligning with United Nations Security Council resolutions that emphasize States' obligation to safeguard air services within their jurisdiction. These resolutions urge all States to collaborate with ICAO to assess, enhance, and implement international security standards. The Cybersecurity Action

[1] Argentina, Aruba (Kingdom of the Netherlands), Belize, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Dominican Republic, Uruguay and Venezuela (Bolivarian Republic of).

Plan (CyAP) is formulated to effectively pursue the goals outlined in the seven pillars of the Aviation Cybersecurity Strategy and establish a robust cybersecurity environment.

1.2 DECEA's primary duties encompass overseeing airspace control, flight protection, search and rescue services, as well as managing telecommunications in Brazilian civil aviation. Additionally, DECEA offers logistical support and maintains cybersecurity systems essentials for executing these tasks.

2. DISCUSSION

2.1 Cybersecurity Information Sharing

2.1.1 Global threats are increasingly concerning. To ensure safe and continuous flight operations, air navigation and surveillance systems must be protected in their global information exchanges. Identifying and supervising these systems is crucial to prevent vulnerabilities from being exploited, causing service failures or outages. Additionally, the emergence of new systems from air navigation hyper-connectivity will be a significant issue by 2030. In this context, knowing the threats in a timely manner is an essential factor so that cybersecurity assets can more effectively protect the systems that provide aviation services.

2.1.2 Thus, the practice of exchanging cybersecurity threat information is in perfect alignment with Brazilian National Cybersecurity Policy (PNCiber), established through Decree No. 11,856, dated 26 December 2023, which establishes as one of its objectives:

— Art. 3, Inc. XI - "implementing collaboration strategies to develop international cooperation in cybersecurity."

2.1.3 In the context of ICAO, cybersecurity information sharing is outlined in its Cybersecurity Action Plan (CyAP), Second edition, January 2022. Information sharing is specifically described in Item 3.1.1 as one of the pillars of the CyAP Aviation Cybersecurity Strategy.

2.2 Malware Information Sharing Platform

2.2.1 Malware Information Sharing Platform (MISP) is a crucial cybersecurity tool for sharing threat information. Its adoption has grown due to the many benefits it offers organizations and cybersecurity professionals. Key advantages include:

a) MISP facilitates collaboration between organizations, enabling secure sharing of threat information. This is crucial in a landscape where cyber threats are constantly evolving. The ability to share indicators of compromise and threat information in real-time allows for a more robust and effective defence.

b) By centralizing and sharing threat information, MISP allows organizations to access real-time threat intelligence. This accelerates the detection and response to incidents, improving overall security posture.

c) MISP is highly customizable and extensible, allowing organizations to tailor the platform to their specific needs. This includes the ability to add custom attributes, create specific threat models, and integrate MISP with other security tools.

d) MISP connects users to global cybersecurity communities, enabling the sharing of information withother professionals and organizations. This expands the available knowledge base and strengthens defence against large-scale threats, understanding the tactics, techniques, and procedures (TTPs) of cyber adversaries.

e) MISP incorporates advanced access control and privacy features, ensuring that organizations can selectively and securely share information. This is crucial for protecting sensitive data and complying with privacy regulations.

2.2.2 In summary, MISP is crucial for managing cyber threats, offering an effective platform for cybersecurity information sharing. Its adoption enhances organizational defence and strengthens cybersecurity at national, regional, and global levels.

2.3 Use of MISP by DECEA

2.3.1 DECEA began implementing MISP in 2021 and has been utilizing and enhancing the use of this tool ever since. The continuous refinement of MISP usage underscores DECEA's commitment to staying in line with the evolving cybersecurity challenges.

2.3.2 The adoption of MISP enables DECEA to collaborate effectively with other Brazilian stakeholders, including the Network Incident Treatment Center of Brazilian Air Force (CTIR.FAB), Brazilian Petroleum Corporation (Petrobras), National Telecommunications Agency (ANATEL) and Brazilian Federation of Banks (FEBRABAN), in sharing critical threat intelligence. This collaboration not only strengthens DECEA's own defence mechanisms but also contributes to the overall security posture of the Brazilian Air Space Control System (SISCEAB).

2.3.3 The threat indicators and alerts received through MISP from others are processed and serve as the foundation for composing block lists or for crafting firewall rules. These indicators provide crucial insights into potential security threats, allowing organizations to proactively protect their networks and systems from malicious activities, staying ahead of emerging threats and strengthen their cybersecurity posture.

2.3.4 The rules associated with a threat is determined by its risk level over time. This risk level for each threat is continuously updated based on indicators received through MISP. By dynamically adjusting the risk level associated with each threat, organizations can ensure that their firewall rules remain effective and responsive to ensure more secure landscapes. This approach allows for more adaptive and precise threat mitigation strategies, enhancing overall cybersecurity resilience.

2.3.5 To exemplify, Figure 1 shows some of the top ten types of threats among the most received through MISP by DECEA, in the last year, were Trojan Zeus, Phishing URL Finding, emotet IOC update, Trojan Citadel and phishing pages.

2.3.6 Figure 2 presents the daily quantity of malware blocks from indicators received by the MISP platform over a one-week period. From the graph shown, it can be observed that MISP contributes to approximately 40,000,000 malware blocks per year.

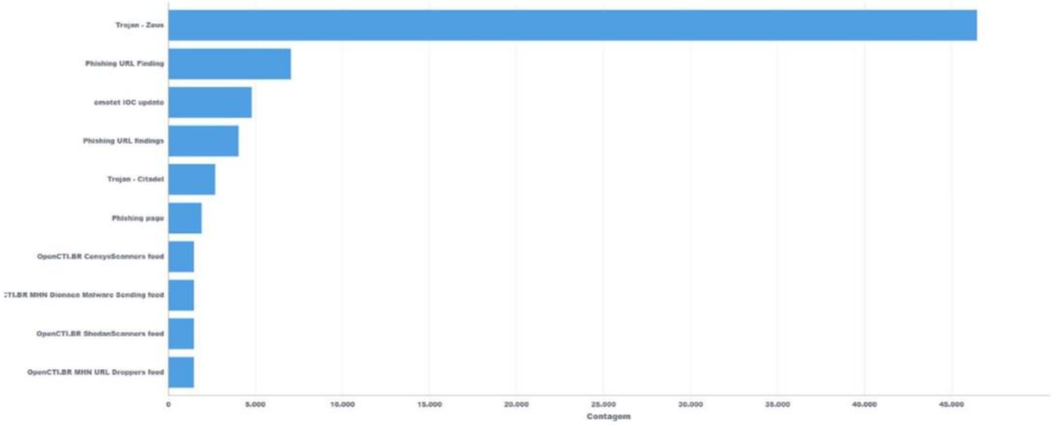

Figure 1 - Top ten types of threats received by DECEA

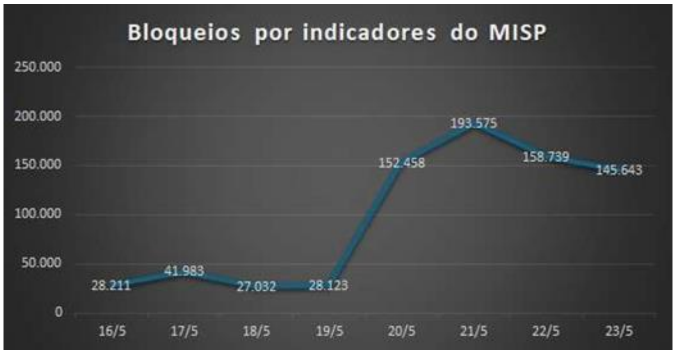

Figure 2 - Malwares blocked by MISP indicators

2.3.7 Today, MISP assists in receiving and/or notifying any confirmed or suspected adverse event related to the security of computer systems or computer networks, in order to contribute with information security in the SISCEAB.

3. CONCLUSION

3.1 In conclusion, DECEA's use of MISP significantly enhances aviation cybersecurity in Brazil. This proactive approach aligns with international standards like ICAO's Cybersecurity Action Plan (CyAP). DECEA also supports National Civil Aviation Agency of Brazil (ANAC) in using MISP to improve cyber threat information sharing in Brazilian civil aviation, leveraging MISP's capabilities for real-time intelligence sharing and adherence to open standards.

3.2 Brazil reaffirms its commitment to contribute to international aviation security, especially in cybersecurity. Its collaborative approach enhances global aviation safety. As hyper-connectivity increases the attack surface of air navigation systems, Brazil is dedicated to adopting the best strategies and technologies to protect its critical aviation infrastructure from evolving cyber threats.

3.3 Brazil intends to encourage the use of MISP among members of the Caribbean and South American (CAR/SAM) Region , to explore and actively participate in the cyber threat information exchange initiative, thus promoting the use of MISP as a robust collaboration platform. The objective is to increase the cyber resilience of regional aviation so that there is, in the future, global integration, in line with ICAO recommendations.

3.4 In light of the above, the Conference is invited to agree to the following recommendation:

Recommendation 4.2/x – Cybersecurity and information system resilience

a) note that the use case of Malware Information Sharing Platform (MISP) by Department of Airspace Control (DECEA) in Brazil as a platform for sharing cybersecurity information has been positive so far;

b) encourage Member States to adopt the MISP as a platform for sharing cybersecurity information; and

c) bring the topic of this paper to the Cybersecurity Panel (CYSECP) and create a Working Group to address the standardization of cybersecurity information sharing and the potential use of the MISP platform by the Member States.

— END —