Organización de Aviación Civil Internacional
Grupo Regional de Planificación y Ejecución CAR/SAM (GREPECAS)

NOTA DE ESTUDIO

GREPECAS/22 — NE/25
02/09/24

Cuarta Reunión Conjunta GREPECAS–RASG-PA y
Vigésima segunda Reunión del Grupo Regional de Planificación y Ejecución del Caribe y Sudamérica (GREPECAS/22)
Fase Virtual (Asincrónica, en línea 13 de septiembre al 11 de octubre de 2024)
Fase Presencial (Lima, Perú, 20 al 22 de noviembre de 2024)

Cuestión 5 del Orden del Día: **Implementación de los Servicios de Navegación Aérea (ANS) CAR/SAM**
5.4 Gestión de la Información Aeronáutica (AIM)

INTERCAMBIO DE INFORMACIÓN MEDIANTE MISP (MALWARE INFORMATION SHARING PLATFORM) Y SU CONTRIBUCIÓN A LA MEJORA DE LA CIBERSEGURIDAD Y LA RESILIENCIA DE LOS SISTEMAS DE INFORMACIÓN

(Presentada por Brasil)

RESUMEN EJECUTIVO

Este documento de trabajo destaca los esfuerzos de Brasil en materia de ciberseguridad de la aviación en relación con el intercambio de información sobre ciberseguridad a través de la MISP (Malware Information Sharing Platform), en consonancia con las propuestas del Panel de Ciberseguridad de la OACI (CYSECP). Enfatiza que esta solución no requiere gastos adicionales de ciberseguridad y fomenta la colaboración entre estados, organizaciones e industria para mejorar la seguridad cibernética.

Acción:	Como se indica en la sección 6
Objetivos Estratégicos:	• Explorar y participar activamente en la iniciativa de intercambio de información sobre amenazas cibernéticas, promoviendo así el uso de MISP como una plataforma de colaboración robusta • Aumentar la resiliencia cibernética de la aviación regional para que, en el futuro, haya una integración global, en línea con las recomendaciones de la OACI
Referencias:	• Proyecto MISP. Obtenido de https://www.misp-project.org/ • Plan de Acción de Ciberseguridad (CyAP) de la OACI. Obtenido de https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx • Política Nacional de Ciberseguridad de Brasil (PNCiber). Obtenido de https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289

1. Introducción

1.1 La OACI mejora continuamente sus normas y reglamentos para hacer frente al panorama mundial de amenazas en constante cambio, en consonancia con las resoluciones del Consejo de Seguridad de las Naciones Unidas que hacen hincapié en la obligación de los Estados de salvaguardar los servicios aéreos dentro de su jurisdicción. Estas resoluciones instan a todos los Estados a colaborar con la OACI para evaluar, mejorar e implementar las normas internacionales de seguridad. El Plan de Acción de Ciberseguridad (CyAP) está formulado para perseguir eficazmente los objetivos descritos en los siete pilares de la Estrategia de Ciberseguridad de la Aviación y establecer un entorno de ciberseguridad sólido.

1.2 Las funciones principales de DECEA abarcan la supervisión del control del espacio aéreo, la protección de vuelos, los servicios de búsqueda y rescate, así como la gestión de las telecomunicaciones en la aviación civil brasileña. Además, DECEA ofrece apoyo logístico y mantiene sistemas de ciberseguridad esenciales para la ejecución de estas tareas.

2. INTERCAMBIO DE INFORMACIÓN SOBRE CIBERSEGURIDAD

2.1 Las amenazas globales son cada vez más preocupantes. Para garantizar la seguridad y la continuidad de las operaciones de vuelo, los sistemas de navegación y vigilancia aérea deben estar protegidos en sus intercambios mundiales de información. Identificar y supervisar estos sistemas es crucial para evitar que las vulnerabilidades sean explotadas, causando fallos o interrupciones del servicio. Además, la aparición de nuevos sistemas de hiperconectividad de la navegación aérea será un problema importante para 2030. En este contexto, conocer las amenazas de manera oportuna es un factor esencial para que los activos de ciberseguridad puedan proteger de manera más efectiva los sistemas que brindan servicios de aviación.

2.2 Así, la práctica de intercambio de información sobre amenazas de ciberseguridad está en perfecta alineación con la Política Nacional de Ciberseguridad de Brasil (PNCiber), establecida mediante el Decreto Nº 11.856, de 26 de diciembre de 2023, que establece como uno de sus objetivos:

- Art. 3, Inc. XI - "implementación de estrategias de colaboración para desarrollar la cooperación internacional en ciberseguridad".

2.3 En el contexto de la OACI, el intercambio de información en materia de ciberseguridad se describe en su Plan de Acción de Ciberseguridad (CyAP), segunda edición, enero de 2022. El intercambio de información se describe específicamente en el punto 3.1.1 como uno de los pilares de la Estrategia de Ciberseguridad de la Aviación de CyAP , y en el Capítulo 9.

2.4 En cumplimiento con el CyAP, Brasil ha estado cumpliendo con los plazos, que se extienden hasta 2025, para las acciones establecidas para desarrollar las capacidades de intercambio de información de ciberseguridad (Acciones CyAP 5.1 a CyAP 5.5).

3. MISP

3.1 MISP (Malware Information Sharing Platform) es una herramienta de ciberseguridad crucial para compartir información sobre amenazas. Su adopción ha crecido debido a los muchos beneficios que ofrece a las organizaciones y a los profesionales de la ciberseguridad. Las principales ventajas incluyen:

- MISP facilita la colaboración entre organizaciones, lo que permite compartir de forma segura la información sobre amenazas. Esto es crucial en un panorama en el que las amenazas cibernéticas están en constante evolución. La capacidad de compartir indicadores de compromiso e información de amenazas en tiempo real permite una defensa más sólida y efectiva.
- Al centralizar y compartir la información sobre amenazas, MISP permite a las organizaciones acceder a la inteligencia de amenazas en tiempo real. Esto acelera la detección y la respuesta a incidentes, mejorando la postura de seguridad general.
- MISP es altamente personalizable y extensible, lo que permite a las organizaciones adaptar la plataforma a sus necesidades específicas. Esto incluye la capacidad de agregar atributos personalizados, crear modelos de amenazas específicos e integrar MISP con otras herramientas de seguridad.
- MISP conecta a los usuarios con las comunidades globales de ciberseguridad, lo que permite compartir información con otros profesionales y organizaciones. Esto amplía la base de conocimientos disponible y fortalece la defensa contra amenazas a gran escala, comprendiendo las tácticas, técnicas y procedimientos (TTP) de los adversarios cibernéticos.
- MISP incorpora funciones avanzadas de control de acceso y privacidad, lo que garantiza que las organizaciones puedan compartir información de forma selectiva y segura. Esto es crucial para proteger los datos confidenciales y cumplir con las regulaciones de privacidad.

3.2 En resumen, el MISP es crucial para gestionar las amenazas cibernéticas, ya que ofrece una plataforma eficaz para el intercambio de información sobre ciberseguridad. Su adopción mejora la defensa organizacional y fortalece la ciberseguridad a nivel nacional, regional y global.

4. USO DE MISP POR DECEA

4.1 DECEA comenzó a implementar MISP en 2021 y ha estado utilizando y mejorando el uso de esta herramienta desde entonces. El refinamiento continuo del uso de MISP subraya el compromiso de DECEA de mantenerse en línea con los desafíos de ciberseguridad en evolución.

4.2 La adopción del MISP permite a la DECEA colaborar eficazmente con otras partes interesadas brasileñas, incluido el CTIR. FAB (Centro de Tratamiento de Incidentes de Red de la Fuerza Aérea Brasileña), Petrobras (Corporación Brasileña de Petróleo), ANATEL (Agencia Nacional de Telecomunicaciones) y FEBRABAN (Federación Brasileña de Bancos), en el intercambio de inteligencia de amenazas críticas. Esta colaboración no solo fortalece los mecanismos de defensa propios de DECEA, sino que también contribuye a la postura general de seguridad del Sistema Brasileño de Control del Espacio Aéreo (SISCEAB).

4.3 Los indicadores de amenazas y las alertas recibidas a través de MISP de otros se procesan y sirven como base para componer listas de bloqueo o para elaborar reglas de firewall. Estos indicadores proporcionan información crucial sobre las posibles amenazas de seguridad, lo que permite a las organizaciones proteger de forma proactiva sus redes y sistemas de actividades maliciosas, adelantarse a las amenazas emergentes y fortalecer su postura de ciberseguridad.

4.4 Las reglas asociadas a una amenaza están determinadas por su nivel de riesgo a lo largo del tiempo. Este nivel de riesgo para cada amenaza se actualiza continuamente en función de los indicadores recibidos a través del MISP. Al ajustar dinámicamente el nivel de riesgo asociado con cada amenaza, las organizaciones pueden asegurarse de que sus reglas de firewall sigan siendo efectivas y receptivas para

garantizar entornos más seguros. Este enfoque permite estrategias de mitigación de amenazas más adaptables y precisas, mejorando la resiliencia general de la ciberseguridad.

4.5 A modo de ejemplo, la Figura 1 muestra algunos de los diez principales tipos de amenazas, entre los más recibidos a través de MISP por DECEA, en el último año, fueron Trojan Zeus, Phishing URL Finding, emotet IOC update, Trojan Citadel y páginas de phishing.

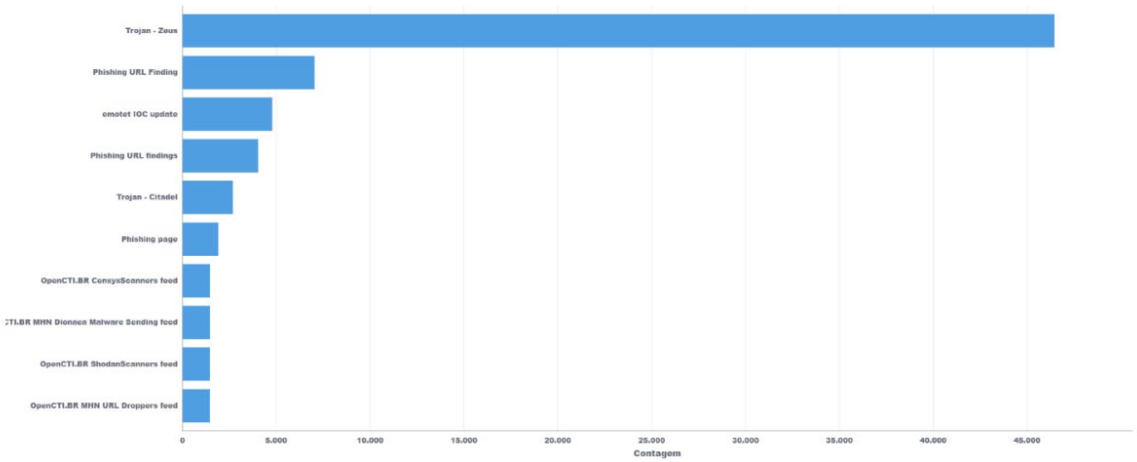

Figura 1 - Los diez tipos principales de amenazas recibidas por DECEA

4.6 La Figura 2 presenta la cantidad diaria de bloques de malware de los indicadores recibidos por la plataforma MISP durante un período de una semana. En el gráfico mostrado, se puede observar que MISP contribuye a aproximadamente 40.000.000 de bloques de malware al año.

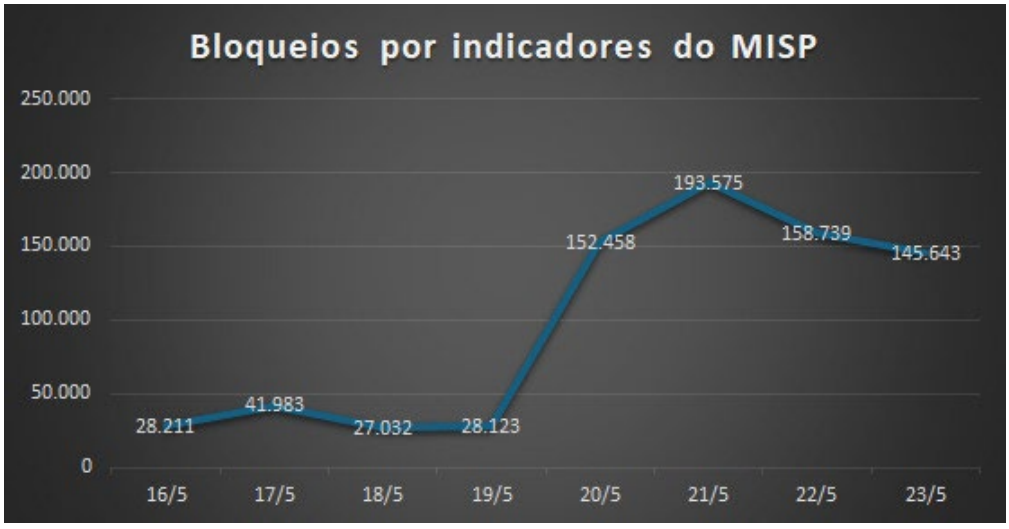

Figura 2 - Malwares bloqueados por indicadores MISP

4.7 En la actualidad, el MISP asiste en la recepción y/o notificación de cualquier evento adverso confirmado o sospechado relacionado con la seguridad de los sistemas informáticos o de las redes informáticas, con el fin de contribuir con la seguridad de la información en el SISCEAB.

5. Conclusión

5.1 En conclusión, el uso de MISP por parte de DECEA mejora significativamente la ciberseguridad de la aviación en Brasil. Este enfoque proactivo se alinea con estándares internacionales como el Plan de Acción de Ciberseguridad (CyAP) de la OACI. DECEA también apoya a ANAC en el uso de MISP para mejorar el intercambio de información sobre amenazas cibernéticas en la aviación civil brasileña, aprovechando las capacidades de MISP para el intercambio de inteligencia en tiempo real y el cumplimiento de estándares abiertos.

5.2 Brasil reafirma su compromiso de contribuir a la seguridad de la aviación internacional, especialmente en materia de ciberseguridad. Su enfoque colaborativo mejora la seguridad de la aviación mundial. Con el objetivo de aumentar la integridad de la información de los sistemas AIM para garantizar operaciones efectivas y seguras, Brasil se dedica a adoptar las mejores estrategias y tecnologías para proteger su infraestructura crítica de aviación de las amenazas cibernéticas en evolución.

5.3 Brasil tiene la intención de alentar el uso del MISP entre los miembros de la región de CAR SAM (Caribe y América del Sur), para explorar y participar activamente en la iniciativa de intercambio de información sobre amenazas cibernéticas, promoviendo así el uso del MISP como una plataforma de colaboración robusta. El objetivo es aumentar la resiliencia cibernética de la aviación regional para que en el futuro haya una integración global, en línea con las recomendaciones de la OACI.

5.4 Además, el DECEA se compromete a apoyar la implementación de MISP ofreciendo asistencia a los Estados Miembros que deseen adoptar esta plataforma, garantizando un enfoque más cohesivo y seguro para la ciberseguridad en la región.

6. Acciones sugeridas

6.1 Se invita a la reunión a:

a) Tomar nota que el uso de MISP por parte de DECEA en Brasil como plataforma para compartir información de ciberseguridad ha sido positivo hasta ahora;

b) alentar a los Estados Miembros a que adopten el PSIM como plataforma para compartir información sobre ciberseguridad; y

c) llevar el tema de este documento al Panel de Ciberseguridad (CYSECP) y crear un Grupo de Trabajo para abordar la estandarización del intercambio de información sobre ciberseguridad y el uso potencial de la plataforma MISP por parte de los Estados miembros.

— FIN —