国 际 民 用 航 空 组 织

工 作 文 件

AN-Conf/14-WP/136
30/6/24
第 1 号修改稿
(Revision No.1)
30/7/24

第十四次空中航行会议

2024 年 8 月 26 日至 9 月 6 日，加拿大，蒙特利尔

议程项目 **4**： 空中航行系统的超联通
4.2： 网络安全和信息系统的韧性

利用恶意软件信息共享平台（MISP）共享信息及其对提高网络安全和信息系统韧性的贡献

（由巴西提交，并获得拉丁美洲民用航空委员会（LACAC）20 个成员国[1]的支持）

第 1 号修改稿

执行摘要

本工作文件重点介绍了巴西在航空网络安全方面所做的努力，通过恶意软件信息共享平台（MISP）共享网络安全信息，这与国际民航组织网络安全专家组（CYSECP）的建议保持一致。文件强调，这一解决方案不需要额外的网络安全开支，并能促进各国、各组织和行业之间的协作以加强网络安全。

行动：请会议：

a) 注意到巴西空域管制司（DECEA）使用 MISP 作为网络安全信息共享平台的实例迄今为止效果良好；
b) 鼓励成员国采用 MISP 作为共享网络安全信息的平台；和
c) 将本文件的主题提交网络安全专家组（CYSECP），并建立一个工作组，以探讨网络安全信息共享的标准化问题以及成员国使用 MISP 平台的可能性。

1. 引言

1.1 国际民航组织不断改进其标准和法规，以应对不断变化的全球威胁，并遵守联合国安理会相关决议，其中强调各国有义务保障其管辖范围内的航空服务。这些决议敦促所有国家与国际民航组织协作，评估、加强和实施国际安全标准。《网络安全行动计划》（CyAP）的制定是为了有效地实现航空网络安全战略七大支柱中概述的各项目标，并建立一个强大的网络安全环境。

[1] 阿根廷、阿鲁巴（荷兰王国）、伯利兹、智利、哥伦比亚、哥斯达黎加、古巴、厄瓜多尔、萨尔瓦多、危地马拉、洪都拉斯、牙买加、墨西哥、尼加拉瓜、巴拿马、巴拉圭、秘鲁、多米尼加共和国、乌拉圭和委内瑞拉玻利瓦尔共和国。

1.2 DECEA 的主要职责包括监督空域管制、飞行保护、搜索和救援服务，以及管理巴西的民航电信。此外，空域管制司还提供后勤支持，并维护执行这些任务所必需的网络安全系统。

2 讨论

2.1 网络安全信息共享

2.1.1 全球威胁日益令人担忧。为确保安全和持续的飞行运行，必须保护空中航行和监视系统的全球信息交换。识别和监督这些系统对于防止漏洞被利用、造成服务故障或中断至关重要。此外，到 2030 年，因空中航行超联通而出现的新系统也将是一个重要问题。在这种情况下，及时了解威胁是一个至关重要的因素，这样网络安全资产才能更有效地保护提供航空服务的各个系统。

2.1.2 因此，交流网络安全威胁信息的做法完全符合巴西国家网络安全政策（PNCiber），该政策是通过 2023 年 12 月 26 日第 11,856 号法令制定的，其目标之一为：

— 第 3 条，XI — “实施协作战略，发展网络安全方面的国际合作”。

2.1.3 就国际民航组织而言，其《网络安全行动计划》（CyAP）（第二版，2022 年 1 月）对网络安全信息共享进行了概述。信息共享作为 CyAP 航空网络安全战略的支柱之一，在 3.1.1 项中得到了具体描述。

2.2 恶意软件信息共享平台

2.2.1 恶意软件信息共享平台（MISP）是共享威胁信息的重要网络安全工具。由于它能为组织和网络安全专业人员带来诸多益处，其利用率越来越高。主要优势包括：

a) MISP 可促进各组织之间的协作，实现威胁信息的安全共享。在网络威胁不断演变的今天，这一点至关重要。通过实时共享入侵迹象和威胁信息，可以实现更强大、更有效的防御。

b) 通过集中和共享威胁信息，MISP 使各组织能够获取实时威胁情报。这加快了对事件的检测和响应，改善了整体安全态势。

c) MISP 具有高度可定制性和可扩展性，使各组织能够根据自己的具体需求定制平台。这包括添加自定义属性、创建特定威胁模型以及将 MISP 与其他安全工具集成的功能。

d) MISP 将用户与全球网络安全社区连接起来，使用户能够与其他专业人员和组织共享信息。这扩大了现有的知识库，加强了对大规模威胁的防御，了解了网络对手的战术、技术和程序（TTPs）。

e) MISP 集成了先进的访问控制和隐私保护功能，确保各组织可以有选择性地安全共享信息。这对于保护敏感数据和遵守隐私法规至关重要。

2.2.2 总之，MISP 对于管理网络威胁至关重要，它为网络安全信息共享提供了一个有效的平台。采用该系统可在国家、地区和全球层面增强组织防御能力，加强网络安全。

2.3 空域管制司使用恶意软件信息共享平台

2.3.1 空域管制司于 2021 年开始实施 MISP，并一直在利用和加强这一工具。DECEA 不断改进对 MISP 的使用，彰显了其不断应对演变中的网络安全挑战的承诺。

2.3.2 MISP 的采用使 DECEA 能够与巴西其他利害攸关方有效合作，包括巴西空军网络事件处理中心（CTIR.FAB）、巴西石油公司（Petrobras）、国家电信局（ANATEL）和巴西银行联合会（FEBRABAN），并共享关键威胁情报。这一协作不仅加强了 DECEA 自身的防御机制，也有助于巴西空域管制系统（SISCEAB）的整体安全态势。

2.3.3 通过 MISP 从其它各处收到的威胁指标和警报经过处理后，可作为编制拦截列表或制定防火墙规则的基础。这些指标提供了对潜在安全威胁的重要洞察，使各组织能够比新威胁先行一步，主动保护其网络和系统免受恶意活动的侵害，并加强其网络安全态势。

2.3.4 与威胁相关的规则取决于随时间变化的风险水平。每个威胁的风险水平都会根据通过 MISP 收到的指标不断更新。通过动态调整与每种威胁相关的风险水平，各组织可以确保其防火墙规则保持有效和反应迅速，从而确保更安全的环境。通过这种方法，可以制定适应性更强、更精确的威胁缓解战略，提高整体网络安全复原力。

2.3.5 例如，图 1 显示了 DECEA 去年通过 MISP 收到数量最多的十大威胁类型，包括木马 Zeus、钓鱼 URL 查找、emotet IOC 更新、木马 Citadel 和钓鱼网页。

2.3.6 图 2 显示了在一周时间内每天借助 MISP 平台收到的指标而拦截的恶意软件数量。从图中可以看出，MISP 帮助我们每年拦截约 40 000 000 个恶意软件。

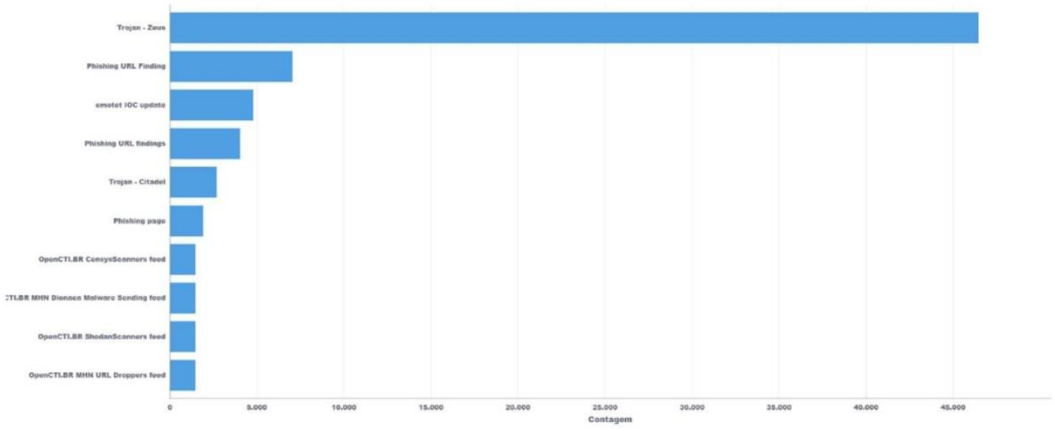

图 1 — DECEA 收到的十大威胁类型

图 2 — 通过 MISP 指标拦截的恶意软件

2.3.7 如今，MISP 协助接收和/或通知任何与计算机系统或计算机网络安全有关的已证实或可疑的不利事件，以促进巴西空域管制系统（SISCEAB）的信息安全。

3. 结论

3.1 总之，DECEA 使用 MISP 极大地增强了巴西的航空网络安全。这种积极主动的做法符合国际民航组织网络安全行动计划（CyAP）等国际标准。DECEA 还支持巴西国家民航局（ANAC）利用 MISP 实时分享情报和遵守开放标准的能力，改善巴西民航的网络威胁信息共享状况。

3.2 巴西重申其致力于促进国际航空安全，特别是网络安全。其协作办法加强了全球航空安全。超联通性增加了空中航行系统的攻击面，巴西致力于采用最佳战略和技术，保护其关键航空基础设施免受不断变化的网络威胁。

3.3 巴西希望鼓励加勒比和南美洲（CAR/SAM）地区成员使用 MISP，探索并积极参与网络威胁信息交流举措，从而更多地使用 MISP 作为一个强大的协作平台。其目标是提高地区航空的网络复原力，以便将来根据国际民航组织的建议实现全球一体化。

3.4 鉴于上述情况，请会议同意以下建议：

建议 4.2/x — 网络安全和信息系统的韧性

a) 注意到巴西空域管制司（DECEA）使用恶意软件信息共享平台（MISP）作为网络安全信息共享平台的实例迄今为止效果良好；

b) 鼓励成员国采用 MISP 作为共享网络安全信息的平台；和

c) 将本文件的主题提交网络安全专家组（CYSECP），并建立一个工作组，以探讨网络安全信息共享的标准化问题以及成员国使用 MISP 平台的可能性。

— 完 —