Subject: [ticket number] XXX - POSSIBLE CYBER SECURITY THREAT IMPACTING AVIATION SECTOR

Message Classification: XXX

TLP: Amber

[Date]

XXX - POSSIBLE CYBER SECURITY THREAT IMPACTING AVIATION SECTOR

1. According to recent reports, a threat actor known as "USDoD" compromised the confidential information of 3,200 Airbus vendors, exposing sensitive data like names, phone numbers, and email addresses. The breach stemmed from an employee of a Turkish airline who obtained an illegal copy of Microsoft.NET framework, leading to the spread of the RedLine malware. The threat actors gained access to credentials from the infected system, using them as an initial attack vector into Airbus website. Refer to the following annexes for more details.

    - Annex A - Summary of reports about Airbus data breach with lessons to be learnt and the associated threats
    - Annex B - Information and Yara rules on the associated RedLine malware
    - Annex C - MITRE ATT&CK matrix and TTPs on the RedLine malware

2. XXX Stakeholders are strongly encouraged to put in place mitigations based on the lessons to be learnt and associated threats mentioned in Annex A.

3. Recommendation XXX

4. XXX