

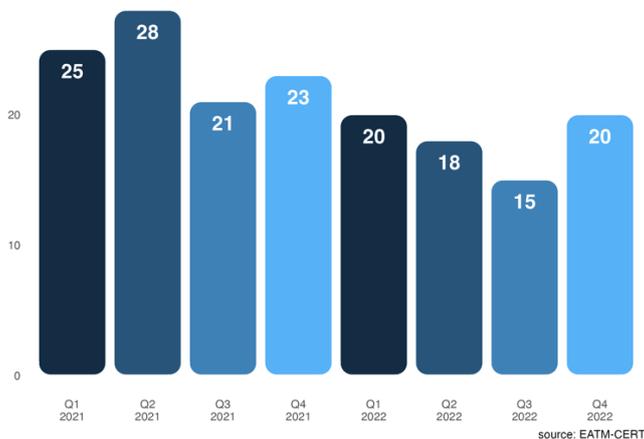
EUROCONTROL Data Snapshot

Ransomware groups target aviation's supply chain

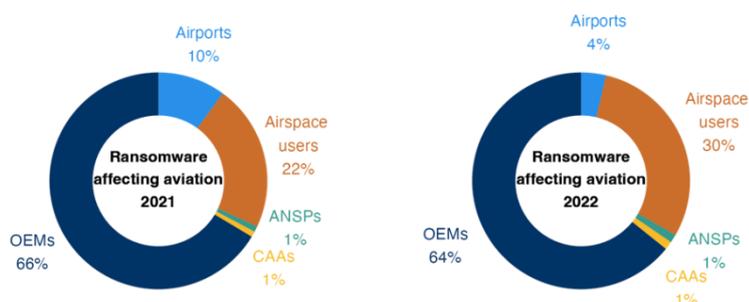


07 February 2023

Quarterly reported ransomware events in Europe affecting aviation



Worldwide share of reported ransomware events



The global air transportation system is a critical part of society. A key feature of the system is its high level of connectivity between different stakeholders and its increased digitalisation; however, the more digitalised, the more there is the risk of cyber-attacks. The challenge is to keep the system cyber-resilient – to keep risk at an acceptable level despite cyber-attacks.

This data snapshot shows the number of ransomware attacks which affected aviation in 2021 and 2022 (*ransomware is a type of malicious software designed to block access to a computer system by encrypting its files until a sum of money is paid*). The timeline on the left shows how many incidents have been reported in Europe on a quarterly basis. As can be seen on the right, the majority of incidents impacted original equipment manufacturers (OEMs).

Since 2021, we have had a clearer idea of the scale of the problem thanks to more incidents and events being shared by European aviation stakeholders with EUROCONTROL/EATM-CERT (our Computer Emergency Response Team). On the global level, similar patterns emerge; we are aware of approximately 2.5 reported ransomware attacks per week on aviation-related organisations.

Ransomware is a worrying category of cyber-attacks; cyber criminals have changed their strategy to focus on companies able to pay large sums (so-called “big game hunting” – the ransom is around 5% of the annual revenue). As shown, ransomware mostly affects the extensive aviation supply chain. This has disruptive consequences on the whole sector, beyond the company being directly affected.

Since early 2022, the conflict in Ukraine has affected the activity of some ransomware groups. As a significant number of these groups rely on Russian resources, some groups re-oriented their activities into cyber-attacks supporting Russian forces and propaganda. Thus the number of attacks in Europe dropped down to 73. However, we do expect to see an increase in ransomware incidents again in 2023.

When stakeholders subject to a ransomware incident share information about such an attack with EATM-CERT, they help improve the cyber-resilience of the overall European aviation – as EATM-CERT can inform other stakeholders about the techniques that each ransomware group systematically uses.

Technical Bits: The quarterly data is derived from the EATM-CERT data collection with a focus on Europe. The global total shares accounts also for events shared by worldwide stakeholders.

For more information on EATM-CERT, please also visit <https://www.eurocontrol.int/service/european-air-traffic-management-computer-emergency-response-team>. For an interactive map of recent events, please check out <https://www.eurocontrol.int/cybersecurity>.

Interested in EATM-CERT and cyber security in aviation? Earmark the upcoming “Aviation Capture The Flag” in Sofia on 14 & 15 June 2023.

©EUROCONTROL 2023

SUPPORTING EUROPEAN AVIATION



NETWORK MANAGER

