# Airbus supply chain hacked in a cyberespionage campaign

Reference: Memo [190927-2] – Version: 1.0
Keywords: transportation, aviation, supply chain compromise, espionage, China
Sources: Publicly available information

## Key Points

- According to Agence France Presse (AFP), Airbus has fallen victim to a sophisticated cyber-espionage campaign.
- Attackers reportedly breached IT systems of several Airbus's suppliers and, from there, penetrated Airbus's IT systems.
- Attackers have been looking after certification documentation, sensitive information related to A350 and A400M's engines as well avionics details.
- Several AFP's sources suspect Chinese hacking groups, still no formal attribution has been made.

## Summary

According to an investigation by AFP[1], in the past few months, Airbus has been the victim of a series of sophisticated cyberattacks carried out via Airbus's suppliers compromised IT networks. Several sources in the security sector suspect that the campaign could have an economic espionage motive and be originating from China.

Cyberattacks reportedly targeted the French technology consultancy Expleo, the engine maker Rolls Royce, and two French Airbus subcontractors which have not been identified.

This campaign reportedly started 12 months ago and consisted of four major attacks. The first attack was discovered in a British subsidiary of the company Assystem and at Rolls Royce. The attack against Expleo was discovered in the end of 2018, but the initial compromise was likely older. The attackers targeted the virtual private network (VPN) that connected Expleo to Airbus. Other attacks employed the same modus operandi: compromise a supplier, breach its VPN connection to Airbus, and penetrate into Airbus systems using access rights granted to suppliers.

The attackers were reportedly especially interested in technical documents related to certification. According to 3 AFP's sources, stolen information was related to the engines of the A400M military transportation aircraft. Attackers were also interested in A350's engines as well as documentation on avionics.

## Comments

More than a decade ago, China announced the development of a second airliner to boost the country's economic competitiveness, with the implicit objective to breach the long-standing duopoly that Airbus and Boeing have maintained in the commercial jet market. However, according to a report[2], the C919 program continues to be hampered by weak management and manufacturing delays, sparking concerns about its ability to gain certification in Western markets. One of the long-standing impediments constraining progress is reportedly the integration of avionics in the flight deck.

Information that attackers were looking for in the Airbus hack (technical details on avionics) are hence consistent with China's cyberespionage priorities in the commercial aviation sector.

AFP's sources have discussed the possible involvement of the China-based APT10 threat actor. Interestingly, in October and December 2018, the US Department of Justice indicted several Chinese nationals (including members of the cyber-threat group APT10), for theft of aviation trade secrets (see Memo [231218]). In 2019, CERT-EU has released memos (see Memos [190626-1], [190729-1]) related to miscellaneous APT10 activities (e.g. targeting the telecoms sector).

According to an industrial source, there is however another hacking group specialised in aerospace matters which is affiliated to the regional branch of the Chinese ministry of state security (MSS) in the province of Jiangsu (east), the JSSD. JSSD's core business is reportedly aerospace and its people understand the language and software used in the sector.

Several historical cases of Chinese cyber-espionage in the aviation sector have been presented in CERT-EU's Memo [190425-1] on cyber enabled espionage.

Other affiliations between MSS regional offices and Chinese hacking groups have been analysed in CERT-EU's Memo [190729-1].

[1] https://www.afp.com/fr/infos/334/espionnage-airbus-cible-dune-serie-de-cyberattaques-ses-sous-traitants-doc-1kn4ke1

2 https://www.ainonline.com/aviation-news/air-transport/2019-06-14/flight-deck-woes-still-hampering-c919