Ransomware paralyses European aircraft supplier

Reference: Memo [190617-1] – Version: 1.0
Keywords: Ransomware, ASCO, aircraft, aviation, supplier
Sources: publicly available information

Key Points

- Belgium-based airplane parts and aviation structuring business ASCO Industries has been hit by a cyber-attack.
- ASCO confirmed that the breach was allegedly related to a piece of ransomware.
- The company provides components to Airbus, Boeing, Bombardier Aerospace, and Lockheed Martin.
- About 1,000 people (70 percent of employees in Belgium) were sent home on unpaid leave, in Zaventem.
- According to media, production was shut down in Belgium and other countries (Canada, Germany, USA, Brazil, and France).

Summary

By mid-June, Belgium-based airplane parts and aviation structuring business ASCO Industries has shuttered its production plants after falling victim of a potential ransomware attack. The perpetrators of the attack have still not been identified.

ASCO is originally a Belgian company with offices and production plants not only in Zaventem (Belgium) but also in Canada, Germany, USA, Brazil, and France. The enterprise provides components to Airbus, Boeing, Bombardier Aerospace, and Lockheed Martin.

According to public media, ASCO shut down a large part of its Headquarters in Zaventem, as well as operations in other countries, following a security breach. Due to technical unemployment, about 1,000 people (70 percent of their employees in Belgium) were sent home, on unpaid leave until the company resumes operations.

Immediately following the attack, ASCO was quoted to have hired internal and external experts who are currently investigating the incident. The company also reported to the authorities, and informed the media that there currently is no evidence of the theft of information and that the attackers were unidentified at this stage.

Although ASCO confirmed that the breach was related to ransomware, however they were still unable to categorise the ransomware family involved so far.

According to key stats, compiled by safeatlast, ransomware is behind 56% of malware attacks and 95% of ransomware profits went through the cryptocurrency trading platform BTC-e.

Comments

CERT-EU believes that the potential ransomware compromise of ASCO highlights the possible downstream risks and consequences of cyber-attacks on third-party manufacturers in complex supply chains such as aircraft manufacturing.

The company manufactures parts for the F-35 fighter jet, Airbus A400M military aircraft, Ariane space launch rockets and commercial aircrafts from Boeing and Airbus. Although ransomware attacks are usually about money, in the case of a company, with connections in the defence sector, like ASCO, it could also be a decoy for an espionage campaign.

When it comes to ransomware, organisations are advised to be well prepared and have an incident response plan in place to help limit the potential damages, not only to production but also to customer trust and brand reputation. In these cases, prevention is always better than a cure: there is a possibility that the cyber criminals who orchestrated a ransom-attack would not restore data / systems or be stopped by the authorities before being able to do so. Therefore, instead of paying the ransom, victims should consider involving law enforcement as well as external forensic experts.

Several important organizations have been hit by ransomware over the past year, including Eurofins Scientific, COSCO, Norsk Hydro (MEMO-190320-1), a cloud service provider (MEMO-190103-1), the UK Police Federation, the local administration of Baltimore (MEMO-190604-2). The aviation sector was also a target with organisations such as Aebi Schmidt, Mitsubishi Canada Aerospace, in the US, the Louisville Regional Airport Authority and the Cleveland Hopkins Airport. Popular ransomware targeting the aviation sector recently are Ryuk and LockerGoga.