# BOEING CYBERATTACK: DID THEY PAY A RANSOM?



Cybercriminals have recently targeted the airline and tourism industries, with disastrous consequences. Several companies, including IATA, American Airlines, Tap Air Portugal, and Corsica Ferries, have already been attacked. Boeing is the latest cyberattack victim, with a significant amount of sensitive data being exfiltrated.

The cybercriminals behind the attack, including LockBit, threaten to release the data if Boeing does not respond promptly. VX Underground, a distributor of malware samples, source code, and research papers, has confirmed the breach.

**Boeing Cyberattack: Data Stolen by Hackers**

**It's important to note that cybercriminals do not randomly target the aviation industry.This is because the industry has a significant turnover, collects a lot of data, and works with many service providers who may not always prioritize cybersecurity.**

The large amount of data aviation companies hold makes them a very attractive target for cybercriminals. For instance, a cybercriminal group recently claimed responsibility for an attack on Boeing, threatening to publish 4 GB of data on the dark web and release 500 GB of data in the future. However, this threat was not carried out, and the name of Boeing was later removed from the list of LockBit's demands.

LockBit is a ransomware gang that became the most active in the world in 2022, phishing around 1,700 companies and collecting over 85 million euros in ransoms, according to the FBI.

**Did Boeing Pay a Ransom?**

Boeing has admitted to a cybersecurity incident affecting their production and distribution businesses. However, a spokesperson for the aircraft manufacturer emphasized that this issue has no impact on flight safety.

Boeing's name was mysteriously removed from the list of potential targets for LockBit ransomware. This removal was coupled with public recognition, implying that the American manufacturer had initiated negotiations with the cybercriminal group. As a result, LockBit removed the claim from its dark web showcase site.

According to VX Underground, the malware sample distributor, LockBit's administrative staff informed them of Boeing's removal from the list because negotiations had begun. The information dates back to November 1, 2023, when the cybercriminal group stopped communicating about the Boeing cyberattack.

It is unclear whether the American manufacturer paid the ransom demanded by LockBit, which logically would have been a substantial amount, given that Boeing has a turnover of $66 billion and employs 150,000 people. Additionally, the small group behind the ransom may have faced pressure from the American administration. **It is worth noting that Boeing is one of the largest private military companies in the world.**

With all the breaches and attacks, especially when an organization hosts many sensitive data records, organizations must plan for ransomware encryption events. Additionally, theft and extortion-demand situations of data leakage should be prepared for in resilience efforts, as we often see both being used against victims.

Date: 2023-11-06

Article link: