10.06.2021

Big airline heist

APT41 likely behind a third-party attack on Air India

Nikita Rostovcev

Threat Intelligence Analyst at Group-IB

UPDATE: This blog post was updated on August 12, 2021 at the request of a third party.

Executive summary

In late May, Air India reported a massive passenger data breach. The announcement was preceded by data breaches in various airline companies, including **Singapore Airlines and Malaysia Airlines**. According to the public source data, these airlines use services of the same IT service provider. The media suggested the airline industry was facing "a coordinated supply chain attack". Air India was the first carrier to reveal more details about its security breach.

The data revealed by Air India suggested that the massive data breach that affected multiple carriers was a result of the compromise of the airline's IT service provider. That announcement prompted Group-IB Threat Intelligence analysts to look closer at the attack.

Using its external threat hunting tools, Group-IB's Threat Intelligence team then discovered and attributed another previously unknown cyberattack on Air India with moderate confidence to the Chinese nation-state threat actor known as **APT41**. The campaign was codenamed **ColunmTK**.

In this blog post you will find:

- Previously unknown details about the ColunmTK campaign
- Evidence of compromised workstations and exfiltration of 200 MB of data from Air India's network