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

- Descriptions of TTPs used during the ColunmTK campaign
- Connections between APT41 and the infrastructure used during the ColunmTK campaign

The potential ramifications of this incident for the entire airline industry and carriers that might yet discover traces of ColunmTK in their networks are significant. To help companies detect and hunt for ColunmTK, we have provided a full list of indicators of compromise (IOCs) that we retrieved. MITRE ATT&CK, MITRE Shield, and recommendations are available at the end of this blog post.

Group-IB's Threat Intelligence team informed CERT India and Air India of its findings so that they can take the necessary steps to mitigate the threat.

Background

On May 21, Air India, India's flag carrier, published an official statement on their website about a data breach. The announcement revealed that the breach was caused by a February incident at the airline's IT service provider, which is responsible for processing customers' personally identifiable information (PII). However, that statement has since been corrected. It came to light that the cyberattack on this IT service provider affected 4,500,000 data subjects globally, including data related to Air India's customers.

To view this email as a web page, go here.

Dear Passenger,

This is to inform you that SITA PSS our data processor of the passenger service system (which is responsible for storing and processing of personal information of the passengers) had recently been subjected to a cybersecurity attack leading to personal data leak of certain passengers including yours. This incident affected around 4,500,000 data subjects in the world.

While we had received the first notification in this regard from our data processor on 25.02.2021, we would like to clarify that the identity of the affected data subjects was only provided to us by our data processor on 25.03.2021 & 5.04.2021. The present communication is an effort to apprise you of accurate state of facts as on date and to supplement our general announcement of 19th March 2021 initially made via our website.

The breach involved personal data registered between 26th August 2011 and 20th February 2021, with details that included name, date of birth, contact information, passport information, ticket information, Star Alliance and Air India frequent flyer data (but no passwords data were affected) as well as credit cards data. However, in respect of this last type of data, CVV/CVC numbers are not held by our data processor.

data. However, in respect of this last type of data, CVV/CVC numbers are not held by our data processor.

was put up for sale on an underground market at USD 3,000.

According to Group-IB's Threat Intelligence & Attribution system, the alleged database was published on a fraudulent resource known for reselling data that has been published on various data-leak websites. Because the database had never surfaced anywhere on the dark web, nor in the public domain, Group-IB researchers considered it fake and decided to instead look deeper and

discovered that the post about Air India's alleged data had nothing to do with what happened in reality. Group-IB's Threat Intelligence team soon realized that in this other attack on Air India they were dealing with a sophisticated nation-state threat actor, rather than another financially motivated cybercriminal group.