**IRCTC train online ticketing system hacked (2020)**

A data breach incident was captured by RPF (Railway Protection Force) on IRCTC ( Indian Railway Catering and Tourism Corporation ) website. The link of this case has suspected involvement in terror financing and money laundering. The hacker was running an illegal software to get access to IRCTC portal and generate fake IDs of IRCTC. This IDs were sold to multiple agents and panels across India to generate e-tickets through the IRCTC website for customers and was earning 10-15 million (Indian Rupees) black money per month. This software was sold to roughly 20000 agents across India.

**Attack Details**

**Threat Actor:** An Indian software company has been involved in the case of data breach and generating 563 fake IDs on IRCTC website to get access to the IRCTC Portal. These IDs were able to book the tickets in less time than IRCTC normal time by eliminating login captcha, booking captcha and bank OTP

**Threat:** This attack led to data stealing of many passengers’ private information and also includes the data leak of railways private information. The accused also had access to multiple official websites of government private information in his laptop.

**Vulnerability:**

1. Credit card numbers, name addresses, and other personal information of passengers were stolen by fake IDs

2. The security of the database and the website was very poor that the hacker was having direct access to IRCTC database

**Technical Details**

**Data breach:** Between 2017 to 2020, IRCTC website and databases security was compromised and the hacker’s company was able to access private information about passenger’s and railways through a software called as ANMS to access darknet and Linux based hacking system

**Business Impacts**

**Financial:** Due to this incident, the railways faced a loss in billions. Black money of roughly 3 billion Indian rupees were generated through this company and were sent to outside India via hawala accounts and cryptocurrency. Also, after the news came out the stock price of IRCTC also saw a slight fall.

**Operational:** The PM of India told all government departments to pick personnel with a technical aptitude for the job and train them in cyber security, Indian Railways began identifying trouble-shooters to tackle online security breaches. These officials will be trained in both practical and theoretical aspects of cyber security through a course prepared by the ministry of electronics and information technology of around six to eight hours. For advanced training, officers who are technically qualified or and have a requisite aptitude for cyber security or information technology will be identified.

**Compliance:** Compliance violations can fall into sovereign such as consumer, privacy, security, financial, and data-protection compliance violations.

**Reputation:** After the news came out in media, there were some controversies about IRCTC data secrecy. Also, the stock price of IRCTC fall down by 4 Indian Rupees during that week.

**Preventative Controls**

DCS-11: *Unauthorized Access Response Training* - Prepare datacenter staff to respond to unauthorised entry or egress attempts.

DSP-17: *Sensitive Data Protection* - Define and execute protocols, procedures, and technical safeguards to safeguard sensitive data throughout its lifecycle.

TVM-07: *Vulnerability Identification* - Define, implement, and assess at least monthly processes, procedures, and technical measures for the detection of vulnerabilities on organizationally managed assets.

EKM-02: Key Generation—Employees must take good care of all access management tools, keys, passwords, and cryptosystems.

IAM-12: User ID Credentials—The organization needs to take proper steps to verify identity, restrict access and maintain adherence to industry standards and compliance.

**References**

<https://www.livemint.com/news/india/software-developer-who-hacked-irctc-train-tickets-online-caught-11579665921480.html>

<https://www.youtube.com/watch?v=0eGEvxKJj4M>

<https://railways375.rssing.com/chan-61205109/all_p42.html>

<https://www.newindianexpress.com/nation/2020/jan/22/jharkhand-based-software-developer-held-for-terror-links-2092670.html>

<https://www.hindustantimes.com/india-news/railways-troubleshooters-to-help-fight-cybersecurity-breaches/story-VAoin5KqG4Fv2oqYI8cx3H.html>