Arkose Labs

HK Express prevents automated attacks that disrupt online ticketing platform with Arkose Labs

CASE STUDY

HKexpress

Business Problem

- Automated attacks made tickets unavailable
- Decline in ticket bookings
- Revenue losses

Solution

Platform that combines a dynamic risk engine with adaptive step-up to effectively detect attacks without misclassifying good users

Results

- Attacks stopped and ticket inventory restored
- Bookings and revenue increased immediately
- Ability to adapt to evolving attack techniques

Overview

Hong Kong Express Airways (HK Express) is a low-cost carrier providing affordable fares for scheduled air service in and out of Hong Kong since 2013. Connecting multiple destinations across Asia, the carrier introduced an online ticketing platform to enable its customers to conveniently search and book affordable fares.

The Business Problem

While digitization in the travel industry has made it convenient for customers to search and book last-minute airfares, attackers abuse online ticketing platforms to disrupt services at a significant financial loss to carriers.

Following the initial release of its online ticketing platform, HK Express began identifying anomalies in its key business metrics. The carrier witnessed a sharp increase in the number of tickets reserved (but not purchased) in-cart, which effectively made the available ticket inventory invisible to customers looking for low-cost airfares. Despite the increased volume of reservations, the number of booking transactions actually decreased significantly with noticeable impact on the carrier's revenue and customer experience.

HK Express conducted an internal investigation which revealed attackers were intentionally disrupting the online ticketing platform through automation; and programmatically channelling payments to an off-site payment redirect gateway. When an off-site gateway is used, the ticketing platform affords the customer approximately 15 minutes to complete their transaction before the inventory is returned to circulation. However, these transactions would never occur because attackers were using automation to reserve thousands of tickets repetitively. Genuine customers were consequently denied access to the full inventory of affordable tickets and were forced to make their purchase from a competing carrier.

HK Express also discovered that the attacks were particularly sophisticated in that booking transactions appeared to originate from unique users. Each request was made by a headless browser that could execute JavaScript like a human. They prevented device identification by providing a dynamic client fingerprint, as well as a dynamic network fingerprint to hinder IP identification.

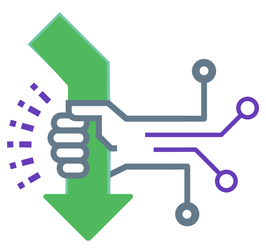
The Arkose Labs Solution

In response to the attacks, HK Express implemented a standard bot mitigation solution, but it could not remediate the abuse and booking disruptions persisted. HK Express then deployed the Arkose Labs platform which quickly neutralized attackers and their ability to exploit the online ticketing platform. Airfares were no longer invisible and customers were presented with all the available inventory to choose from.

Features of Arkose Labs that enabled HK Express to prevent attacks against the online ticket booking platform include:

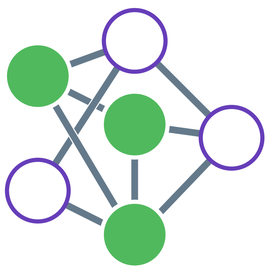
Arkose Enforce

Arkose Enforce is an adaptive step-up that presents challenges to accurately differentiate customers from attackers, thereby filtering automation away from the enterprise and controlling how incentives can be extracted through abuse



Diminishing Returns from Attacks

To subvert the tiered security of Arkose Labs and bypass Arkose Enforce at scale, attackers must invest significantly in computer vision and machine learning. This diminishes the return on investment (ROI) from abuse and discourages attackers to continue investing their resources in launching such attacks



Intelligent Analytics

The platform gets smarter by parsing real-time insights and network effects through Arkose Detect, a dynamic risk engine that invisibly analyzes traffic with continuous machine learning. Customers are challenged less because the platform learns to only target attackers and minimize false positives

The bilateral security approach offered by Arkose Labs not only enabled HK Express to protect its online ticketing platform from automated attacks, but also provided the carrier with the advantage of being adaptive to the evolving attack techniques.

"We're extremely pleased with Arkose Labs and their ability to solve a very expensive problem for us. I'd definitely recommend Arkose Labs for online abuse, fraud, or other damaging automated attacks."

- **Tommy Kok**
  Web Infrastructure, HK Express

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Schedule Demo

demo@arkoselabs.com
(800) 604-3319
arkoselabs.com