radware

CASE STUDY: **TRANSPORTATION**

APAC Airline Stops Bot Attacks To Prevent Competitors From Price Scraping, Hijacking Inventory and Increasing Cost Per Search

OVERVIEW

This APAC airline provides low cost domestic and international flights with hubs throughout the Pacific. Based on number of passengers flown domestically and internationally, it has become one of the largest regional airlines in APAC.

CHALLENGES

Due to its recent success, the airline's web platform and mobile APIs have become the target of cyberattacks from competitors. Their customer portal has experienced attacks including low and slow attacks, malicious behavior and bad bot signatures. Competitors would scrape prices on a periodic basis and hijack reservation inventory, reducing availability for legitimate customers. Hijacking attacks increased seat bookings with no corresponding reservation payments.

In order for the airline to advertise available flights on travel booking sites, it subscribes to a global distribution system (GDS) that charges a fee per search. The airline was being charged for false bot-initiated GDS searches, resulting in revenue loss. Distributed bot attacks impacted the portal response when real customers tried to make a ticket purchase, causing a poor user experience. The airline needed to stop the competition from impacting their business and revenue.

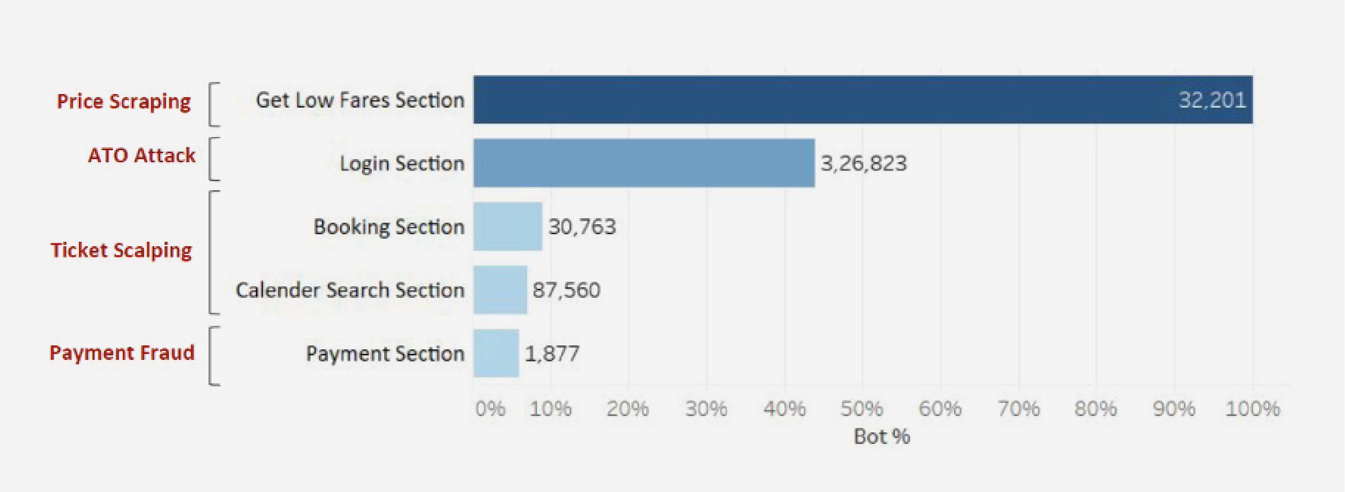


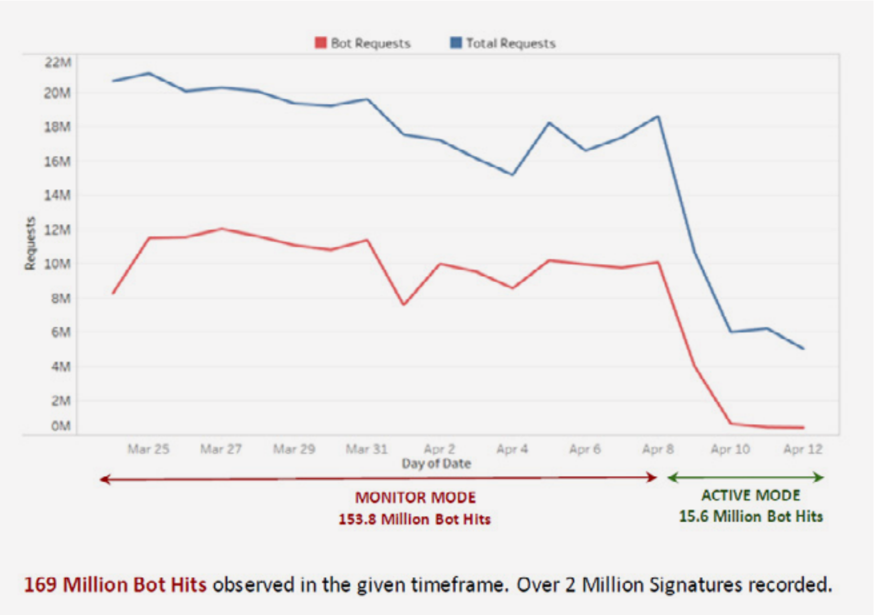
Figure 1: Overview of bot attacks by type that the airline faced

The airline was using Oracle's Dyn Web Application Security suite for application and bot protection. The WAF was approaching end of service and needed to be replaced. The Oracle bot management service used rate limiting and other basic mitigation techniques which could not defend the airline against advanced, human-like bot attacks they were experiencing. Bots were using rotating IP addresses to strike the airline's website, making it difficult to block these attacks using traditional mitigation practices. Because the Oracle solution did not have behavioral-based capabilities, the airline's mobile APIs and website were not sufficiently protected.

SOLUTION

The APAC airline is a customer of Limelight Networks, a CDN service provider.   When Limelight discovered the airline's predicament, they recommended Radware's Cloud WAF Service and Bot Manager. After a successful proof of concept, the airline purchased both services.

Bot Manager detected and mitigated price scraping, account takeover, ticket scalping and payment fraud attacks against alternating IP addresses in the following months. During one extended attacked, Radware Bot Manager reduced the number of bot hits from 21 million to zero within a two-week timeframe.



169 Million Bot Hits observed in the given timeframe. Over 2 Million Signatures recorded.

Figure 2: The airline witnessed an 89% decrease in bot attacks by using Radware Bot Manager

Radware Bot Manager successfully detected attacks against the airline's "Search" API for flight pricing, and the "Low Fare" API invoked when customers looked for special deals. Bot Manager controlled these API attacks so customers were able to search and book flights with no issues.

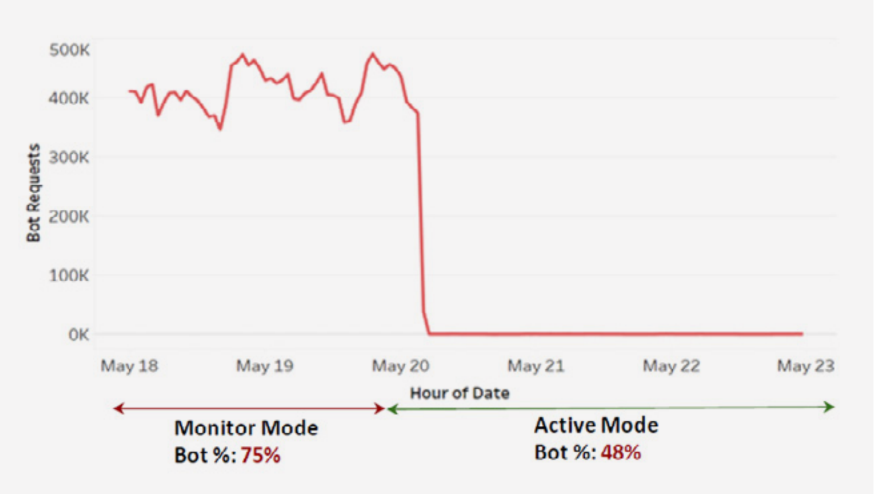


Figure 3: The airline witnessed a 91% decrease of bot attacks on "Search" APIs. Bot characteristics included Suspicious User Journey Traversal, Programmatic Accessing URL Identifier, Integrity Check Failed.

BENEFITS

Radware's Bot Manager and Cloud WAF Service protect the airline's website and mobile APIs so the company can keep inventory free for legitimate customers and provide a better online experience. Lastly, the airline is leveraging these solutions to also protect its website from compromised mobile apps on Android and iOS smartphones.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.