HUMAN

Application Protection Case Study

Top 10 U.S. Airline Stops Web Scraping and Account Takeover Attacks

This top ten airline in the United States serves more than one hundred destinations and employs over 20,000 people. The majority of its business comes through online transactions via the company website and its mobile applications. The airline receives over 6 million website visits per month, servicing millions of travelers, agencies and corporate customers each year.

Challenge

This top ten U.S. airline was barraged by bot attacks, with more than 25% of traffic to company properties coming from malicious bot networks. During peak attack periods, the ratio of bad traffic to good traffic could be as high as 20 to 1.

- Scraping bots continually checked price information and seat inventory without booking, negatively impacting the airline's look-to-book ratio.
- Automated account takeover attacks hijacked customer accounts and stole stored credit card data, airline miles, and loyalty points.
- Malicious bot traffic skewed KPIs, impeding the airline's ability to effectively price, market and analyze its online business

These attacks cost the airline money, time, and other resources, not to mention the potential for significant brand damage.

Solution

The airline deployed HUMAN Application Protection to mitigate bad bots.

Application Protection analyzes more than 2500 signals per interaction—including device and agent type, network and cloud hosting information, and on-page user behaviors—to determine which visitors are humans and which are malicious bots. The airline's team found that Application Protection dropped in smoothly and required minimal integration and configuration changes. They loved the responsiveness of the HUMAN team, including direct Slack channel access to HUMAN customer support.

Results

After the airline installed Application Protection, a botnet operator targeted the company with a massively distributed account takeover attack. The volume of website login traffic increased 30-fold, to more than 5 million requests per day. The attacker spoofed thousands of user agents and distributed the attack across tens of thousands of physical and virtual machines, utilizing more than 100,000 IP addresses. In short, the attacker used the most modern and sophisticated techniques to mask the nature of the bot requests and mimic real user behaviors.

The airline's cybersecurity team had never seen some of the techniques deployed and said that in the past they would have spent weeks or months digging out manually from the attack. This time was different. This attacker spent a lot of money and resources on this scheme, but it was no match for Application Protection. In fact, the airline's information security and ecommerce teams barely noticed the attack. Application Protection proved to be a reliable prevention solution, and, most importantly, demonstrated tangible real business value, saving the airline significant time and money while proactively protecting its brand.

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit ***www.humansecurity.com***